XenServer

XenServer 8

Contents

Acerca de XenServer 8 5

Novedades 7

Novedades del canal de acceso anticipado 17

Novedades de canales normales 25

Problemas resueltos 33

Problemas conocidos 36

Elementos retirados 40

Inicio rápido 50

Requisitos del sistema 75

Límites de configuración 80

Controladores de hardware 85

Compatibilidad con sistemas operativos invitados 86

Requisitos de conectividad 90

Información técnica general 98

Preguntas frecuentes técnicas 106

Descripción general del sistema de licencias 125

Preguntas frecuentes sobre licencias 129

Instalación 136

Otros casos de instalación 146

Actualización desde la Actualización acumulativa 1 de Citrix Hypervisor 8.2 167

Actualice los hosts de XenServer 179

Aplicar actualizaciones mediante XenCenter 181

Versión actual de XenCenter 196

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Uso de XenServer con productos Citrix **196**

Escenarios de actualización para XenServer y Citrix Virtual Apps and Desktops **199**

IntelliCache **217**

PVS-Accelerator **222**

Hosts y grupos de recursos **231**

Verificación de certificados **254**

Agrupaciones en clúster **259**

Solucionar problemas de grupos agrupados **267**

Administrar usuarios **274**

Control de acceso basado en roles **283**

Funciones y permisos de RBAC **285**

Usar RBAC con la CLI **297**

Redes **302**

Administrar redes **322**

Solucionar problemas de redes **347**

Almacenamiento **352**

Crear un repositorio de almacenamiento **358**

Almacenamiento en bloques GFS2 compartido con aprovisionamiento fino **378**

Administrar repositorios de almacenamiento **391**

Rutas múltiples de almacenamiento **404**

Almacenamiento en caché de lectura **411**

Descripción general de gráficos **415**

Preparar el host para gráficos **419**

Crear máquinas virtuales habilitadas para vGPU **427**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Uso de memoria **432**

Supervise y administre su implementación **435**

Supervisa el uso de la CPU **481**

Administrar máquinas virtuales **485**

VM de Windows **494**

Herramientas de máquinas virtuales de XenServer para Windows **507**

Máquinas virtuales Linux **529**

Memoria de VM **543**

Migrar máquinas virtuales **550**

Importación y exportación de máquinas virtuales **556**

Eliminar máquinas virtuales **572**

vApps **574**

Notas avanzadas para máquinas virtuales **578**

Habilitar VNC para máquinas virtuales Linux **588**

Solucionar problemas de VM **601**

Alta disponibilidad **609**

Copia de seguridad y recuperación ante desastres **617**

Habilitar recuperación ante desastres **621**

vApps **627**

Realizar copias de seguridad y restaurar hosts y máquinas virtuales **628**

Instantáneas de VM **634**

Hacer frente a los fallos de las **641**

Balance de carga **645**

Novedades del equilibrio de carga de trabajo **648**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Comience con el equilibrio de carga de trabajo **650**

Tareas básicas de equilibrio de carga **663**

Configurar el comportamiento del equilibrio de carga **681**

Administrar el equilibrio de carga **713**

Certificados para el equilibrio de carga **746**

Solucionar problemas de equilibrio de carga de **755**

XenServer Conversion Manager **762**

Novedades de XenServer Conversion Manager **766**

Introducción a XenServer Conversion Manager **767**

Solución de problemas de XenServer Conversion Manager **780**

Interfaz de la línea de comandos **781**

Solución de problemas **922**

Asistencia **925**

Avisos legales de terceros **930**

Licencias y atribución de código abierto de XenServer **930**

Reglamentación de datos **936**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Acerca de XenServer 8

April 10, 2024

XenServer es una plataforma de virtualización que permite a las organizaciones crear y administrar infraestructuras de servidores virtualizados. Está diseñado para optimizar la entrega de máquinas virtuales Windows y Linux, proporcionando una solución sólida y escalable para la virtualización de centros de datos.

XenServer ofrece funciones como la migración en vivo, capacidades de clonación e instantáneas y la agrupación de recursos, lo que permite una administración eficiente de las cargas de trabajo virtualizadas. Proporciona un entorno seguro y de alto rendimiento para ejecutar aplicaciones y servicios, lo que lo convierte en una opción adecuada para las empresas que buscan optimizar su infraestructura de servidores.

Cloud Software Group (CSG) hace hincapié en la integración de XenServer con los productos Citrix, creando una solución integral de virtualización y entrega de aplicaciones. Nuestro objetivo es mejorar la flexibilidad, la agilidad y la rentabilidad de las operaciones de TI mediante una administración centralizada y un uso eficiente de los recursos. En general, XenServer se posiciona como una solución de virtualización fiable para las empresas que buscan una plataforma potente y versátil para sus entornos de servidores.

Obtenga XenServer 8 aquí.

> **Nota:**
>
> Si anteriormente usaba XenServer 8 como versión Technical Preview, aplique el conjunto de actualizaciones más reciente para pasar sin problemas a la versión compatible con producción.
>
> Si usa una licencia de Citrix Virtual Apps and Desktops con XenServer, debe cambiarla a una licencia de XenServer Premium Edition. Para obtener más información, consulte https://xenserver.com/buy. Los clientes actuales de Citrix Virtual Apps and Desktops pueden solicitar participar en nuestra promoción y recibir hasta 10 000 licencias de socket de XenServer Premium Edition de forma gratuita. Más información.

¿XenServer 8 es para mí?

XenServer 8 es la versión más reciente de XenServer. Sustituye a la actualización acumulativa 1 de Citrix Hypervisor 8.2 e incluye muchas funciones nuevas. Para obtener más información acerca de estas funciones, consulte Novedades.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Por qué elegir XenServer 8?

- Quiere probar las funciones más recientes de XenServer y puede actualizar sus hosts y grupos con regularidad.

  Un cambio notable entre Citrix Hypervisor 8.2 CU 1 y XenServer 8 es el cambio para ofrecer funciones y correcciones de forma continua mediante nuestro mecanismo de actualizaciones frecuentes. Para obtener más información, consulte Actualizar los hosts de XenServer.

- Quiere usar máquinas virtuales Windows 11 en su entorno.

  XenServer 8 es compatible con VM y vTPM de Windows 11. Para obtener más información, consulte Máquinas virtuales de Windows.

- Es usuario de Citrix Virtual Apps and Desktops y quiere ejecutar sus cargas de trabajo en un hipervisor que contenga muchas funciones optimizadas para su entorno.

  Para obtener más información sobre estas funciones, consulte Uso de XenServer con productos Citrix.

  Para saber qué versiones de Citrix Virtual Apps and Desktops (MCS) y Citrix Provisioning (PVS) son compatibles con XenServer 8, consulte Hipervisores compatibles con Citrix Virtual Apps and Desktops (MCS) y Citrix Provisioning (PVS).

  También puede beneficiarse de una promoción por tiempo limitado que ofrece licencias de XenServer gratuitas para los clientes de Citrix. Más información.

En cualquiera de estos casos, XenServer 8 es para usted. Consíguelo aquí.

XenCenter

XenServer 8 requiere la versión más reciente de XenCenter, que tiene un número de versión con el formato "XenCenter aaaa.x.x". Las versiones anteriores de XenCenter, como XenCenter 8.2.x, no son compatibles con XenServer 8.

- Descargue la versión más reciente de XenCenter
- Consulte la documentación

XenCenter aaaa.x.x es totalmente compatible con XenServer 8. XenCenter aaaa.x.x aún no se admite para uso en producción con Citrix Hypervisor 8.2 CU1.

Actualizaciones frecuentes a lo largo del ciclo de vida de XenServer 8

Con XenServer 8, las actualizaciones frecuentes están disponibles en XenCenter, lo que le permite beneficiarse de un proceso de publicación más eficiente que ofrece nuevas funciones y correcciones

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de errores a un ritmo más rápido de lo que era posible anteriormente. Esta función le permite utilizar el modelo de actualización frecuente para administrar las actualizaciones de sus grupos y hosts de XenServer.

Durante su ciclo de vida, XenServer 8 proporciona un flujo de actualizaciones frecuentes y fáciles de aplicar, que le permiten usar nuevas funciones y corregir errores lo antes posible. Debe aplicar todas las actualizaciones disponibles de forma periódica. Como resultado, el comportamiento y el conjunto de funciones de XenServer 8 pueden cambiar.

Introducción

Pasos para usar XenServer 8:

1. Obtenga XenServer 8 en la página de descargas de XenServer.
2. Instale la versión más reciente de XenCenter.
3. Instale o actualice a XenServer 8.
4. Aplique actualizaciones mediante XenCenter.

---

layout: doc
description: Discover the features added in the latest version of XenServer.—

Novedades

Nuestro objetivo es ofrecer nuevas funciones y actualizaciones de productos a los clientes de XenServer 8 tan pronto como estén listas. Las nuevas versiones añaden valor al producto y no hay motivo para retrasar el momento de actualizar. A través del flujo de versiones de XenServer 8, entregamos actualizaciones de forma incremental en oleadas para garantizar la calidad del producto y maximizar la disponibilidad.

> **Nota:**
>
> Si anteriormente usaba XenServer 8 como versión Technical Preview, aplique el conjunto de actualizaciones más reciente para pasar sin problemas a la versión compatible con producción.
>
> Si usa una licencia de Citrix Virtual Apps and Desktops con XenServer, debe cambiarla a una licencia de XenServer Premium Edition. Para obtener más información, consulte https://xenserver.com/buy. Los clientes actuales de Citrix Virtual Apps and Desktops pueden solicitar participar en nuestra promoción y recibir hasta 10 000 licencias de socket de XenServer Premium Edition

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> de forma gratuita. Más información.

XenServer está de vuelta

Una vez más, lanzamos nuestro producto bajo la marca XenServer. Para obtener más información, consulte el sitio web de XenServer.

Como parte de este cambio, cambiarán algunos de los otros nombres y términos que se utilizan en nuestro producto y en nuestra documentación:

Término antiguo	Nuevo término	Notas
Citrix Hypervisor	XenServer	
Formato de versión de XenServer `major_version.minor_version`	Formato de versión de XenServer `major_version`	El formato de la versión de XenServer ha cambiado para mostrar solo la versión principal. Mientras que las versiones anteriores se numeraban como "XenServer 7.6", "Citrix Hypervisor 8.2", etc., esta versión y las versiones futuras muestran solo la versión principal, por ejemplo, "XenServer 8". XenServer 8 se basa en la misma plataforma que Citrix Hypervisor 8.2 CU1 y, por lo tanto, comparte la misma versión principal. Sin embargo, XenServer 8 es la versión más reciente del producto y contiene las funciones y correcciones más recientes.
XenCenter x.xx	XenCenter aaaa.x.x	El formato de la versión de XenCenter ha cambiado para ser independiente de la versión de XenServer. El nuevo formato de versión de XenCenter es. `year.major_version.minor_version`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Término antiguo	Nuevo término	Notas
Citrix VM Tools (anteriormente XenServer PV Tools)	Herramientas de máquinas virtuales de XenServer	
Maestro de agrupación	Coordinador de agrupaciones	El host principal de un grupo ahora se denomina coordinador del grupo en la documentación y en XenCenter. El término anterior todavía se utiliza en algunos comandos de la CLI xe y en la API de administración.
Esclavo de agrupación	Soporte de agrupación	Los hosts subordinados de un grupo ahora se denominan anfitriones auxiliares del grupo o anfitriones auxiliares en la documentación y en XenCenter. El término anterior todavía se utiliza en algunos comandos de la CLI xe y en la API de administración.
Contraseña maestra	Contraseña principal	
Express Edition	Edición de prueba	

Actualizaciones frecuentes y fáciles de aplicar

En XenServer 8, la forma en que publicamos las actualizaciones ha cambiado. Las actualizaciones frecuentes están disponibles, lo que le permite beneficiarse de un proceso de lanzamiento más eficiente que ofrece nuevas funciones y correcciones de errores a un ritmo más rápido de lo que era posible anteriormente. Use XenCenter o la CLI xe para aplicar estas actualizaciones a los hosts y grupos de XenServer en el momento que más le convenga. Para obtener más información, consulte Actualizar los hosts de XenServer.

1. Ponemos a su disposición actualizaciones frecuentes para XenServer 8 en nuestra CDN segura.
2. En XenCenter, compruebe cuándo hay actualizaciones disponibles para su grupo.
3. Con XenCenter o la CLI xe, inicie el proceso de aplicación de actualizaciones a su grupo de XenServer.

Para obtener más información, consulte Aplicar actualizaciones mediante XenCenter o Aplicar actualizaciones mediante la CLI xe.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para obtener una lista de las actualizaciones más recientes disponibles para sus grupos de acceso anticipado o normal, consulta las páginas siguientes:

- Novedades del canal de acceso anticipado
- Novedades de canales normales

Estas páginas no muestran todos los cambios en los canales de acceso anticipado y normal, solo un subconjunto. Para ver el conjunto completo de cambios disponibles, consulte la información de la vista Actualizaciones de **XenCenter**.

Compatibilidad con Windows 11 y vTPM

Windows 11 ahora es compatible con XenServer.

Esta función también incluye soporte para VTPM. Puede crear y adjuntar un vTPM a una máquina virtual de Windows 10 o Windows 11. Para obtener más información, consulte Máquinas virtuales de Windows.

El vTPM proporciona una API compatible con TPM 2.0 a las aplicaciones de la máquina virtual. No se admite TPM 1.2.

Cambios en las licencias

El comportamiento de las licencias en XenServer 8 es diferente al de las versiones anteriores de Citrix Hypervisor y XenServer. Cambiamos los requisitos para los clientes de Citrix, agregamos una nueva edición y pusimos algunas funciones a disposición de todos.

Para obtener más información, consulte Licencias.

Citrix Virtual Apps and Desktops y Citrix DaaS

En XenServer 8, debe tener una licencia Premium Edition para ejecutar las cargas de trabajo en un grupo o host de XenServer. Se trata de un cambio con respecto a las versiones anteriores de Citrix Hypervisor o XenServer, que le permitían usar la licencia Citrix Virtual Apps and Desktops o Citrix DaaS para obtener derecho gratuito a XenServer.

Para obtener más información sobre cómo obtener una licencia de XenServer, consulte https://xenserver.com/buy.

Si ya usa XenServer o Citrix Hypervisor para alojar sus cargas de trabajo de Citrix Virtual Apps and Desktops, puede solicitar la participación en nuestra promoción y recibir hasta 10 000 licencias de socket de XenServer Premium Edition de forma gratuita. Más información.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para saber qué versiones de Citrix Virtual Apps and Desktops (MCS) y Citrix Provisioning (PVS) son compatibles con XenServer 8, consulte Hipervisores compatibles con Citrix Virtual Apps and Desktops (MCS) y Citrix Provisioning (PVS).

Edición de prueba

Ahora puede probar XenServer 8 de forma gratuita con la versión de prueba. La Edición de prueba le permite probar las funciones de la Edición Premium, pero en un grupo de tamaño restringido de hasta 3 hosts. Para obtener más información sobre las diferentes ediciones de XenServer, consulte Ediciones de XenServer.

Cambios en las funciones

Las siguientes funciones, que en versiones anteriores estaban restringidas a los clientes de la edición Premium, ahora también están disponibles en la edición Standard:

- Actualizaciones automatizadas de los controladores de máquinas virtuales de Windows
- Actualizaciones automatizadas del agente de administración
- Aplicación de parches en vivo
- XenServer Conversion Manager

Supervisar los recursos del host y del dom0 con NRPE

> **Nota:**
>
> La función NRPE está disponible para los clientes de XenServer Premium o Trial Edition. Para obtener más información sobre las licencias de XenServer, consulte Licencias. Para actualizar o comprar una licencia de XenServer, visite el sitio web de XenServer.

En XenServer 8, puede usar cualquier herramienta de supervisión de terceros compatible con Nagios Remote Plugin Executor (NRPE) para supervisar los recursos de host y dom0, como Nagios Core. XenServer integra NRPE en dom0, lo que le permite capturar varias métricas de host y dom0. Para obtener más información, consulte Supervisar los recursos de host y dom0 con NRPE.

Supervisar los recursos de host y dom0 con SNMP

> **Nota:**
>
> La función SNMP está disponible para los clientes de XenServer Premium o Trial Edition. Para

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> obtener más información sobre las licencias de XenServer, consulte Licencias. Para actualizar o comprar una licencia de XenServer, visite el sitio web de XenServer.

Ahora puede usar SNMP y cualquier NMS de su elección para supervisar de forma remota los recursos que consume XenServer. Con esta función, también puede configurar capturas para supervisar los hosts de XenServer. Las capturas son mensajes iniciados por el agente que alertan al NMS de que se ha producido un evento específico en XenServer. Para obtener más información, consulte Supervisión de los recursos de host y dom0 con SNMP.

XFS local

Ahora puede usar dispositivos de almacenamiento local con bloques físicos de 4 KB sin necesidad de un tamaño de bloque lógico de 512 bytes mediante el nuevo tipo de SR local de aprovisionamiento delgado: XFS. Para obtener más información, consulte XFS local.

Cambios en la compatibilidad con el sistema operativo invitado

Para ver la lista completa de sistemas operativos invitados compatibles en XenServer 8, consulte Compatibilidad con sistemas operativos invitados.

Agregada

XenServer 8 ahora admite los siguientes huéspedes nuevos:

- Debian Bullseye 11 (64 bits)
- Ubuntu 22.04 (64 bits)
- Windows 11 (64 bits)

Eliminado

XenServer 8 ya no admite los siguientes invitados:

- Debian Jessie 8 (32 bits)
- Debian Jessie 8 (64 bits)
- Debian Stretch 9 (32 bits)
- Debian Stretch 9 (64 bits)
- Ubuntu 16.04 (32-bits)
- Ubuntu 16.04 (64 bits)
- CoreOS
- SUSE Linux Enterprise Desktop 12 SP3, 12 SP4 (64 bits)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- SUSE Linux Enterprise Desktop 15 SP3 (64 bits)
- SUSE Linux Enterprise Server 12 SP3 (64 bits)
- CentOS 8 (64 bits)
- Windows 10 (32 bits)

Elementos retirados

Los siguientes invitados están en desuso en XenServer 8:

- Ubuntu 18.04 (64 bits)
- SUSE Linux Enterprise Desktop 12 SP4 (64 bits)

XenServer Conversion Manager 8.3.1

XenServer Conversion Manager 8.3.1, la versión más reciente del dispositivo virtual XenServer Conversion Manager, le permite convertir máquinas virtuales en paralelo, lo que le permite migrar todo su entorno de VMware a XenServer de forma rápida y eficiente. Puede convertir hasta 10 máquinas virtuales VMware ESXi/vCenter al mismo tiempo.

Para obtener más información sobre cómo usar XenServer Conversion Manager, consulte XenServer-Conversion Manager.

Mejoras en GFS2

Se han eliminado algunas restricciones sobre el uso de SR de GFS2 con Citrix Machine Creation Services.

- Ahora puede usar máquinas virtuales de clonación completa de MCS con SR de GFS2.
- Ahora puede utilizar varios SR de GFS2 en el mismo catálogo de MCS.

Para obtener más información sobre el uso de los SR de GFS2, consulte Almacenamiento en bloques GFS2 compartido con aprovisionamiento fino.

Verificación de certificados

La función de verificación de certificados garantiza que todos los puntos finales de comunicación TLS de la red de administración verifiquen los certificados utilizados para identificar a sus pares antes de transmitir datos confidenciales.

La verificación de certificados está habilitada de forma predeterminada en las instalaciones nuevas de XenServer 8 y versiones posteriores. Si actualiza desde una versión anterior de XenServer o Citrix

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hypervisor, la verificación de certificados no se habilita automáticamente y debe habilitarla. XenCenter le pedirá que habilite la verificación de certificados la próxima vez que se conecte al grupo actualizado.

Para obtener más información, consulte Verificación de certificados.

Restringir el uso del puerto 80

Para mejorar la seguridad, XenServer 8 ahora le permite cerrar el puerto TCP 80 en la interfaz de administración y usar exclusivamente HTTPS a través del puerto 443 para comunicarse con XenServer. Sin embargo, antes de cerrar el puerto 80, compruebe si todos sus clientes de API (en particular Citrix Virtual Apps and Desktops) pueden usar HTTPS a través del puerto 443.

De forma predeterminada, el puerto 80 sigue abierto. Sin embargo, todas las conexiones internas para la migración de máquinas virtuales ahora usan HTTPS a través del puerto 443 de forma predeterminada.

Para obtener más información acerca de cómo cerrar el puerto 80, consulte Restringir el uso del puerto 80.

Compresión del flujo de migración

La función de compresión del flujo de migración le permite acelerar la transferencia de memoria en redes lentas cuando se migra en vivo una máquina virtual al comprimir el flujo de datos entre los hosts. Habilítelo desde XenCenter o la CLI xe. Para obtener más información, consulte Propiedades de la agrupación: Opciones avanzadas y Parámetros de la agrupación.

Winbind reemplaza a PBIS

Winbind reemplazó a PBIS para autenticar a los usuarios de Active Directory (AD) con el servidor de AD y para cifrar las comunicaciones con el servidor de AD. Este reemplazo se produce automáticamente cuando se actualiza. En el improbable caso de que la autenticación externa no funcione después de actualizar a XenServer 8, abandone el dominio AD y vuelva a unirse a él.

Hay algunas pequeñas diferencias de comportamiento como resultado de este cambio:

- Al usar el comando `xe pool-enable-external-auth` para unirse a un dominio, ahora el parámetro `config:disable_modules` se ignora. Este parámetro es específico de PBIS.
- Para el comando `xe pool-enable-external-auth`, el parámetro `config:ou` ahora admite uno de los siguientes formatos al especificar una unidad organizativa de varias capas: `config:ou=a/b/c` o `config:ou=c,ou=b,ou=a`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Winbind actualiza automáticamente la contraseña de la cuenta de la máquina cada 14 días o según lo especifique la opción `winbind_machine_pwd_timeout`de configuración.
- Winbind no admite los siguientes casos:
  - Espacio al principio o al final de un nombre de usuario o grupo de dominios de dominio.
  - Nombres de usuario de dominio que contengan 64 caracteres o más.
  - Nombres de usuario de dominio que incluyen cualquiera de los caracteres especiales +<>” =/%@:,; ‘
  - Nombres de grupos de dominios que incluyen cualquiera de los caracteres especiales,; ‘

Para obtener más información, consulte Winbind.

Acelerador PVS integrado

En versiones anteriores de XenServer o Citrix Hypervisor, el PVS-Accelerator se proporcionaba como paquete complementario. El PVS-Accelerator ahora está incluido en la instalación básica de XenServer. Por lo demás, el comportamiento del PVS-Accelerator no cambia y debe configurarlo antes de usarlo.

Para obtener más información sobre el PVS-Accelerator, consulte PVS-Accelerator.

Arranque de red una máquina virtual a través de IPv6

Ahora puede arrancar en red una máquina virtual a través de una red IPv6. Esta función solo es compatible con las máquinas virtuales UEFI, no con las máquinas virtuales de BIOS.

Funciones eliminadas

Las siguientes funciones ya no se admiten en XenServer:

- Diseño de partición heredado
- Comprobación de estado
- Measured Boot Supplemental Pack
- Dispositivo virtual Linux de demostración

> **Nota:**
>
> Windows conserva los registros del servicio Health Check para solucionar problemas. Para eliminar estos registros, elimínelos manualmente de `%SystemRoot%\System32\Winevt\Logs` la máquina Windows que ejecute XenCenter.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cambios en componentes de terceros

PuTTY ya no viene incluido en XenCenter. Para lanzar una consola SSH en un host de XenServer mediante XenCenter, debe instalar una herramienta de consola SSH externa y asegurarse de que XenCenter esté configurado para usarla. Para obtener más información, consulte Configurar XenCenter para usar unaconsola SSH externa.

Los siguientes binarios de Broadcom ya no se incluyen en la instalación de XenServer:

- elxocmcore
- elxocmcorelibs
- hbaapiwrapper

Para descargar estos binarios desde la página de descargas de Broadcom Emulex, siga estos pasos:

1. Vaya a la sección **Software y herramientas de administración**.
2. Descargue el **kit de aplicaciones principales (CLI) de Emulex HBA Manager para Citrix XenServer**.

Los siguientes binarios de línea de comandos de Marvell ya no se incluyen en la instalación de XenServer:

- CLI de QConvergeConsole para Citrix (QCC)
- QCS

Para descargar QCC desde la página de descargas de Marvell QLogic, siga estos pasos:

1. Seleccione la ficha **Adaptadores**.
2. En el panel izquierdo, elige el tipo de adaptador.
3. En el panel central, elija el modelo de su adaptador.
4. En el panel derecho, elija **Citrix Hypervisor.**
5. Haga clic en **Ir**. Se le redirigirá a una página con las descargas disponibles.
6. Descargue la **CLI de QConvergeConsole para Citrix (**QCC).

Para instalar esta aplicación, siga las instrucciones de la Guía del usuario de la utilidad de línea de comandos de QConvergeConsole.

Notas de compatibilidad

XenServer 8 es compatible con los siguientes componentes:

- La versión más reciente de XenServer VM Tools para Windows
- La última versión de XenServer VM Tools para Linux
- La versión más reciente del dispositivo virtual Equilibrio de carga de trabajo

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- La última versión del dispositivo virtual XenServer Conversion Manager

Estos componentes están disponibles en la página de descargas de XenServer.

---

layout: doc
description: Changes that are available in the Early Access update channel that have not yet progressed to the Normal update channel.—

Novedades del canal de acceso anticipado

Las siguientes funciones, funciones de vista previa, mejoras y correcciones de errores están disponibles en el canal de actualizaciones de acceso anticipado. Es posible que algunas de las últimas entradas de la lista no estén disponibles todavía en el canal Normal. En este artículo no se enumeran todos los cambios en el canal de acceso anticipado, solo un subconjunto. Para ver el conjunto completo de cambios disponibles, consulte la información de la vista Actualizaciones de **XenCenter**.

25 de marzo de 2024

Estas actualizaciones incluyen las siguientes mejoras:

- Reduzca el uso de la CPU inactiva de QEMU.
- Actualice el controlador Cisco enic a 4.5.0.7.
- Actualice el controlador Cisco fnic a 2.0.0.90.

18 de marzo de 2024

Estas actualizaciones solucionan el siguiente problema:

- Tras actualizar desde Citrix Hypervisor 8.2 CU1, los servicios de mantenimiento en segundo plano para los SR de GFS2 no se inician correctamente.

14 de marzo de 2024

Estas actualizaciones solucionan los siguientes problemas:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si el coordinador del grupo no se está ejecutando o la pila de herramientas se está reiniciando, es posible que se produzcan errores en las operaciones de vTPM realizadas por el usuario o por Windows en segundo plano.
- Corrija los nombres de algunos tipos de SR en xsconsole.
- Cambios de código iniciales que pueden reducir las notificaciones de falsos positivos para el CVE-2023-38545.

Estas actualizaciones incluyen las siguientes mejoras:

- Cambios de código iniciales que pueden reducir las notificaciones de falsos positivos para el CVE-2023-28486.

12 de marzo de 2024

Estas actualizaciones incluyen los siguientes cambios en XenServer:

- Si usa la versión preliminar de XenServer 8 con una licencia de Citrix Virtual Apps and Desktops, esta licencia es obsoleta y ya no es compatible con XenServer 8.

  Para ejecutar una carga de trabajo de Citrix Virtual Apps and Desktops en un grupo de XenServer 8, debe obtener una licencia de XenServer Premium Edition para todos los hosts del grupo. Para obtener más información, visite el sitio web de XenServer.

Estas actualizaciones solucionan el siguiente problema:

- XSA-452 CVE-2023-28746

  Para obtener más información, consulte el boletín de seguridad: https://support.citrix.com/article/CTX616982.

Estas actualizaciones incluyen las siguientes mejoras:

- Actualice la versión de microcódigo Intel IPU 2024.1.

06 de marzo de 2024

> **Nota:**
>
> Antes de aplicar estas actualizaciones, actualice XenCenter a la versión 2024.1.0 o posterior. La versión más reciente de XenCenter está disponible en https://xenserver.com/downloads.

Estas actualizaciones contienen la siguiente función:

- La etiqueta de "vista previa"se ha eliminado de la plantilla de Windows 11. Este sistema operativo invitado está listo para ser totalmente compatible cuando XenServer 8 pase de una versión preliminar a una versión totalmente compatible en producción.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Estas actualizaciones solucionan los siguientes problemas:

- Al recopilar estadísticas de rendimiento de hosts e invitados, los archivos RRD recopilados a menudo no están actualizados.
- En los clústeres de XenServer 8 con SR de GFS2, al recopilar las bases de datos de XenServer, no se recopila la base de datos del demonio del clúster.
- Al recopilar un informe de estado del servidor, si solicita un archivo completo de informes de errores y se supera el límite de tamaño de archivo de una base de datos para xcp-rrdd-plugins, los archivos de registro de xcp-rrdd-plugin no se recopilan.
- Al recopilar un informe de estado del servidor, si usa el inicio de sesión por SSH:
  - El modo interactivo en el que se confirman los archivos individuales para su recopilación no funciona sin la intervención de un usuario específico.
  - Al descargar datos RRD sin comprimir con un método obsoleto, no se recopilan los RRD de máquina virtual.
- CVE-2023-45230: Desbordamiento de búfer en el cliente DHCPv6 mediante una opción de ID de servidor largo.
- CVE-2023-45231: Lectura fuera de límites al gestionar un mensaje de redirección ND con opciones truncadas.
- CVE-2023-45232: Bucle infinito al analizar opciones desconocidas en el encabezado Opciones de destino.
- CVE-2023-45233: Bucle infinito al analizar una opción PadN en el encabezado Opciones de destino.
- CVE-2023-45234: Desbordamiento de búfer al procesar servidores DNS en un mensaje de anuncio de DHCPv6.
- CVE-2023-45235: Desbordamiento de búfer al gestionar la opción de ID de servidor desde un mensaje de anuncio de proxy DHCPv6.
- Un problema con el uso de vTPM mientras se reinicia la pila de herramientas.
- El estado de los enlaces de NIC no se refleja correctamente.

Estas actualizaciones incluyen las siguientes mejoras:

- Mejoras en la forma de aplicar las actualizaciones de software a los hosts y grupos de XenServer. Para obtener más información, consulte Aplicar actualizaciones.
- Actualice la configuración de rutas múltiples usada para PURE FlashArray SAN para que coincida con las recomendaciones del proveedor.
- Mejora en los mensajes de error cuando los tipos de SR de archivos son de solo lectura.
- Mejoras en el rastreo distribuido.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

28 de febrero de 2024

Estas actualizaciones solucionan los siguientes problemas:

- XSA-451 CVE-2023-46841.
- Un problema de migración con máquinas virtuales en las que anteriormente se veía CMP_LEGACY.

21 de febrero de 2024

Estas actualizaciones contienen la siguiente función nueva:

- Supervise los recursos de host y dom0 con SNMP. Esta función se puede utilizar a partir de la próxima versión de XenCenter. Para obtener más información, consulte Supervisión de los recursos de host y dom0 con SNMP.

Estas actualizaciones solucionan los siguientes problemas:

- Si intenta habilitar SR-IOV en una NIC Intel E810 en XenCenter, la VF asignada a una máquina virtual no funciona una vez que se inicia la máquina virtual.

Estas actualizaciones incluyen las siguientes mejoras:

- Actualice Xen de 4.13 a 4.17.
- Varias mejoras en las operaciones de rutas de datos de GFS2.

12 de febrero de 2024

Estas actualizaciones incluyen la siguiente función nueva:

- Agregue un nuevo check (`check_multipath`) al servicio NRPE para permitir la supervisión del estado de rutas múltiples.

Estas actualizaciones solucionan los siguientes problemas:

- Cuando hay grupos de portales de destino independientes dentro del IQN, XenServer no puede iniciar sesión en todos los portales iSCSI.
- Al crear un recurso compartido ISO SR para pequeñas y medianas empresas, ya no es necesario proporcionar credenciales al conectarse a un servidor para pequeñas y medianas empresas que permita el acceso de invitados.
- Es posible que parte de la pila de herramientas deje de ejecutarse inesperadamente.
- No puede importar una máquina virtual Windows 11 suspendida que se haya exportado como XVA con conservación del estado de energía.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Cuando una máquina virtual con vTPM se inicia o se migra rápidamente de un grupo a otro, puede producirse una condición de carrera.
- Las operaciones `pool-eject` que se ejecutan en paralelo pueden provocar errores de verificación de TLS.
- Se han corregido varios problemas de baja probabilidad con los SR de GFS2.

Estas actualizaciones incluyen las siguientes mejoras:

- Actualice el controlador fastlinq de Qlogic a 8.74.0.2.
- Mejoras en el rastreo distribuido.

29 de enero de 2024

Estas actualizaciones incluyen las siguientes mejoras:

- Soporte para arranque UEFI y arranque seguro para sistemas operativos invitados Linux. Para obtener más información, consulte Arranque UEFI de invitado y Arranque seguro.
- Proporcione información más detallada sobre los certificados TLS SHA256 y SHA1 de un host de XenServer en la vista de la consola del host de XenCenter.

23 de enero de 2024

Estas actualizaciones incluyen correcciones de seguridad. Para obtener más información, consulte el boletín de seguridad https://support.citrix.com/article/CTX587605.

15 de enero de 2024

Estas actualizaciones incluyen las siguientes mejoras:

- Actualice XenServer VM Tools para Linux a la versión 8.4.0-1, disponible para descargar desde la página de descargas de XenServer. A partir de esta versión, puede usar el script `install.sh` para desinstalar XenServer VM Tools para Linux. Para obtener más información, consulte Desinstalar XenServer VM Tools para Linux.
- Asegúrese de que el mensaje de bienvenida de XenServer aparezca siempre al conectarse a una consola host de XenServer y de que el mensaje esté correctamente empaquetado en líneas.

4 de enero de 2024

Estas actualizaciones solucionan los siguientes problemas:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- A veces, después de migrar una máquina virtual de un grupo a otro, las alertas de la máquina virtual no se copian correctamente al grupo de destino ni se eliminan del grupo de origen.
- A veces, la base de datos del grupo no se restaura desde el registro de redo (parte de la función de alta disponibilidad).

Estas actualizaciones incluyen las siguientes mejoras:

- Actualice el controlador Smartpqi de Microsemi a 2.1.26_030.
- Actualiza el microcódigo de AMD a la versión 2023-12-05.
- Mejoras en el rastreo distribuido.

11 de diciembre de 2023

Estas actualizaciones solucionan los siguientes problemas:

- Al usar rutas múltiples con el firmware v7.x de la serie PS de Dell EqualLogic, es posible que se produzcan errores en el protocolo iSCSI.

27 de noviembre de 2023

Estas actualizaciones solucionan los siguientes problemas:

- A veces, el registro de repetición (parte de la función de alta disponibilidad) no reproduce todas las escrituras de la base de datos.
- Al ejecutar el `vdi-copy` comando para copiar una VDI a una SR, XenServer no informa correctamente del progreso de la operación.
- En XenCenter, personalizar una plantilla y, a continuación, exportarla y volver a importarla puede provocar que la plantilla no se importe.

Estas actualizaciones incluyen las siguientes mejoras:

- Agregue un controlador para Dell PERC12 (versión del controlador: mpi3mr 8.1.4.0.0).
- Mejoras generales de la API.
- Se ha eliminado la etiqueta «vista previa» del soporte de vTPM. Esto significa que vTPM estará listo para ser totalmente compatible cuando XenServer 8 pase de la versión preliminar a la versión totalmente compatible en producción.

15 de noviembre de 2023

Estas actualizaciones incluyen las siguientes mejoras:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- La etiqueta “vista previa”se ha eliminado de la plantilla de Ubuntu 22.04. Este sistema operativo invitado está listo para ser totalmente compatible cuando XenServer 8 pase de una versión preliminar a una versión totalmente compatible en producción.

14 de noviembre de 2023

Estas actualizaciones incluyen correcciones de seguridad. Para obtener más información, consulte el boletín de seguridad https://support.citrix.com/article/CTX583037/.

6 de noviembre de 2023

Estas actualizaciones incluyen las siguientes mejoras:

- Mejoras generales del SDK y tiempos de inicio de sesión de la API mejorados.
- Actualice Open vSwitch a la v2.17.7.

3 de noviembre de 2023

Estas actualizaciones incluyen mejoras y correcciones generales.

25 de octubre de 2023

Estas actualizaciones solucionan los siguientes problemas:

- La implementación de Windows mediante el arranque PXE y Configuration Manager puede provocar que Windows se bloquee.
- Si la sincronización horaria está inhabilitada, las máquinas virtuales de Windows no devuelven la hora correcta.

Estas actualizaciones incluyen las siguientes mejoras:

- Las máquinas virtuales Windows del modo de arranque UEFI ahora muestran el logotipo de Windows durante el arranque en lugar del logotipo de Tianocore.

18 de octubre de 2023

Estas actualizaciones incluyen mejoras y correcciones generales.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

11 de octubre de 2023

Compatibilidad con los siguientes sistemas operativos invitados:

- Debian Bookworm 12
- Rocky Linux 9
- CentOS Stream 9

> **Nota:**
>
> Los clientes que quieran utilizar estos sistemas operativos invitados también deben instalar XenServer VM Tools for Linux v8.3.1-1 o posterior, que se puede descargar desde la página de descargas de productos de XenServer.

Estas actualizaciones incluyen las siguientes mejoras:

- Actualice el controlador Mellanox mlnx_en a 5.9-0.5.5.0.

10 de octubre de 2023

Estas actualizaciones incluyen correcciones de seguridad. Para obtener más información, consulte el boletín de seguridad https://support.citrix.com/article/CTX575089/.

2 de octubre de 2023

Estas actualizaciones incluyen las siguientes mejoras:

- Soporte para el sistema operativo Red Hat Enterprise Linux 9. Consulte las notas de lanzamiento de Red Hat Enterprise Linux 9 para obtener más información técnica.

> **Nota:**
>
> Los clientes que quieran utilizar este sistema operativo invitado también deben instalar Citrix VM Tools para Linux v8.3.1-1 o posterior, que se puede descargar desde la página de descargas de productos de XenServer.

18 de septiembre de 2023

Estas actualizaciones incluyen mejoras y correcciones generales.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

11 de septiembre de 2023

Estas actualizaciones incluyen las siguientes mejoras:

- Habilite el equilibrio de interrupciones para los dispositivos PCI Fibre Channel (FC). Esto mejora el rendimiento de los SR de HBA FC rápidos, especialmente si se utilizan rutas múltiples.
- Solución para la errata #1474 de AMD. Inhabilite el C6 después de 1000 días de funcionamiento en los sistemas AMD Zen2 para evitar un bloqueo de aproximadamente 1044 días.

31 de agosto de 2023

Estas actualizaciones solucionan los siguientes problemas:

- Las métricas de rendimiento no están disponibles para los SR de GFS2 y los discos en estos SR.
- No puede realizar instantáneas ni comprobar una máquina virtual suspendida si esa máquina virtual tiene un vTPM conectado.
- Si un host de XenServer se bloquea o se cierra abruptamente, es posible que no se puedan iniciar más máquinas virtuales de Windows 11 o migrar más máquinas virtuales de Windows 11 a ese host.
- Si, cuando se conectan los SR iSCSI, no están disponibles todas las rutas posibles (por ejemplo, un puerto remoto de un controlador fuera de línea está inactivo), al SR no se le agregarán sesiones iSCSI adicionales cuando se vuelva a acceder a esos puertos remotos.

Estas actualizaciones incluyen las siguientes mejoras:

- Actualice el controlador Intel ice a la versión 1.11.17.1.
- Mejoras de rendimiento para GFS2.

---

layout: doc
description: Changes that are available in the Normal update channel after having progressed from the Early Access update channel.—

Novedades de canales normales

Las actualizaciones pasan del canal de actualizaciones de acceso anticipado a Normal con una cadencia regular. Las siguientes funciones, funciones de vista previa, mejoras y correcciones de errores están disponibles en el canal de actualizaciones normal. En este artículo no se enumeran todos los cambios en el canal Normal, solo un subconjunto. Para ver el conjunto completo de cambios disponibles, consulte la información de la vista Actualizaciones de **XenCenter**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

19 de marzo de 2024

Estas actualizaciones solucionan los siguientes problemas:

- Corrija los nombres de algunos tipos de SR en xsconsole.
- Cambios de código iniciales que pueden reducir las notificaciones de falsos positivos para el CVE-2023-38545.

Estas actualizaciones incluyen las siguientes mejoras:

- Cambios de código iniciales que pueden reducir las notificaciones de falsos positivos para el CVE-2023-28486.

18 de marzo de 2024

Estas actualizaciones solucionan los siguientes problemas:

- Si el coordinador del grupo no se está ejecutando o la pila de herramientas se está reiniciando, es posible que se produzcan errores en las operaciones de vTPM realizadas por el usuario o por Windows en segundo plano.
- Tras actualizar desde Citrix Hypervisor 8.2 CU1, los servicios de mantenimiento en segundo plano para los SR de GFS2 no se inician correctamente.

12 de marzo de 2024

Estas actualizaciones incluyen los siguientes cambios en XenServer:

- Si usa la versión preliminar de XenServer 8 con una licencia de Citrix Virtual Apps and Desktops, esta licencia es obsoleta y ya no es compatible con XenServer 8.

  Para ejecutar una carga de trabajo de Citrix Virtual Apps and Desktops en un grupo de XenServer 8, debe obtener una licencia de XenServer Premium Edition para todos los hosts del grupo. Para obtener más información, visite el sitio web de XenServer.

Estas actualizaciones solucionan el siguiente problema:

- XSA-452 CVE-2023-28746

  Para obtener más información, consulte el boletín de seguridad: https://support.citrix.com/article/CTX616982.

Estas actualizaciones incluyen las siguientes mejoras:

- Actualice la versión de microcódigo Intel IPU 2024.1.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

07 de marzo de 2024

> **Nota:**
>
> Antes de aplicar estas actualizaciones, actualice XenCenter a la versión 2024.1.0 o posterior. La versión más reciente de XenCenter está disponible en https://xenserver.com/downloads.

Estas actualizaciones contienen la siguiente función:

- La etiqueta de "vista previa"se ha eliminado de la plantilla de Windows 11. Este sistema operativo invitado está listo para ser totalmente compatible cuando XenServer 8 pase de una versión preliminar a una versión totalmente compatible en producción.

Estas actualizaciones solucionan los siguientes problemas:

- Al recopilar estadísticas de rendimiento de hosts e invitados, los archivos RRD recopilados a menudo no están actualizados.
- En los clústeres de XenServer 8 con SR de GFS2, al recopilar las bases de datos de XenServer, no se recopila la base de datos del demonio del clúster.
- Al recopilar un informe de estado del servidor, si solicita un archivo completo de informes de errores y se supera el límite de tamaño de archivo de una base de datos para xcp-rrdd-plugins, los archivos de registro de xcp-rrdd-plugin no se recopilan.
- Al recopilar un informe de estado del servidor, si usa el inicio de sesión por SSH:
  - El modo interactivo en el que se confirman los archivos individuales para su recopilación no funciona sin la intervención de un usuario específico.
  - Al descargar datos RRD sin comprimir con un método obsoleto, no se recopilan los RRD de máquina virtual.
- CVE-2023-45230: Desbordamiento de búfer en el cliente DHCPv6 mediante una opción de ID de servidor largo.
- CVE-2023-45231: Lectura fuera de límites al gestionar un mensaje de redirección ND con opciones truncadas.
- CVE-2023-45232: Bucle infinito al analizar opciones desconocidas en el encabezado Opciones de destino.
- CVE-2023-45233: Bucle infinito al analizar una opción PadN en el encabezado Opciones de destino.
- CVE-2023-45234: Desbordamiento de búfer al procesar servidores DNS en un mensaje de anuncio de DHCPv6.
- CVE-2023-45235: Desbordamiento de búfer al gestionar la opción de ID de servidor desde un mensaje de anuncio de proxy DHCPv6.
- Un problema con el uso de vTPM mientras se reinicia la pila de herramientas.
- El estado de los enlaces de NIC no se refleja correctamente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Estas actualizaciones incluyen las siguientes mejoras:

- Mejoras en la forma de aplicar las actualizaciones de software a los hosts y grupos de XenServer. Para obtener más información, consulte Aplicar actualizaciones.
- Actualice la configuración de rutas múltiples usada para PURE FlashArray SAN para que coincida con las recomendaciones del proveedor.
- Mejore los mensajes de error cuando los tipos de SR de archivos son de solo lectura.
- Mejoras en el rastreo distribuido.

28 de febrero de 2024

Estas actualizaciones contienen la siguiente función nueva:

- Supervise los recursos de host y dom0 con SNMP. Esta función se puede utilizar a partir de la próxima versión de XenCenter.

Estas actualizaciones solucionan los siguientes problemas:

- Si intenta habilitar SR-IOV en una NIC Intel E810 en XenCenter, la VF asignada a una máquina virtual no funciona una vez que se inicia la máquina virtual.
- XSA-451 CVE-2023-46841.
- Un problema de migración con máquinas virtuales en las que anteriormente se veía CMP_LEGACY.

Estas actualizaciones incluyen las siguientes mejoras:

- Actualice Xen de 4.13 a 4.17.
- Varias mejoras en las operaciones de rutas de datos de GFS2.

15 de febrero de 2024

Estas actualizaciones incluyen la siguiente función nueva:

- Agregue un nuevo check (`check_multipath`) al servicio NRPE para permitir la supervisión del estado de rutas múltiples.

Estas actualizaciones solucionan los siguientes problemas:

- Cuando hay grupos de portales de destino independientes dentro del IQN, XenServer no puede iniciar sesión en todos los portales iSCSI.
- Al crear un recurso compartido ISO SR para pequeñas y medianas empresas, ya no es necesario proporcionar credenciales al conectarse a un servidor para pequeñas y medianas empresas que permita el acceso de invitados.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Es posible que parte de la pila de herramientas deje de ejecutarse inesperadamente.
- No puede importar una máquina virtual Windows 11 suspendida que se haya exportado como XVA con conservación del estado de energía.
- Cuando una máquina virtual con vTPM se inicia o se migra rápidamente de un grupo a otro, puede producirse una condición de carrera.
- Las operaciones `pool-eject` que se ejecutan en paralelo pueden provocar errores de verificación de TLS.
- Se han corregido varios problemas de baja probabilidad con los SR de GFS2.

Estas actualizaciones incluyen las siguientes mejoras:

- Actualice el controlador fastlinq de Qlogic a 8.74.0.2.
- Mejoras en el rastreo distribuido.

01 de febrero de 2024

Estas actualizaciones incluyen las siguientes mejoras:

- Soporte para arranque UEFI y arranque seguro para sistemas operativos invitados Linux. Para obtener más información, consulte Arranque UEFI de invitado y Arranque seguro.
- Proporcione información más detallada sobre los certificados TLS SHA256 y SHA1 de un host de XenServer en la vista de la consola del host de XenCenter.

23 de enero de 2024

Estas actualizaciones incluyen correcciones de seguridad. Para obtener más información, consulte el boletín de seguridad https://support.citrix.com/article/CTX587605.

18 de enero de 2024

Estas actualizaciones incluyen las siguientes mejoras:

- Actualice XenServer VM Tools para Linux a la versión 8.4.0-1, disponible para descargar desde la página de descargas de XenServer. A partir de esta versión, puede usar el script `install.sh` para desinstalar XenServer VM Tools para Linux. Para obtener más información, consulte Desinstalar XenServer VM Tools para Linux.
- Asegúrese de que el mensaje de bienvenida de XenServer aparezca siempre al conectarse a una consola host de XenServer y de que el mensaje esté correctamente empaquetado en líneas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8 de enero de 2024

Estas actualizaciones solucionan los siguientes problemas:

- A veces, después de migrar una máquina virtual de un grupo a otro, las alertas de la máquina virtual no se copian correctamente al grupo de destino ni se eliminan del grupo de origen.
- A veces, la base de datos del grupo no se restaura desde el registro de redo (parte de la función de alta disponibilidad).

Estas actualizaciones incluyen las siguientes mejoras:

- Actualice el controlador Smartpqi de Microsemi a 2.1.26_030.
- Actualiza el microcódigo de AMD a la versión 2023-12-05.
- Mejoras en el rastreo distribuido.

14 de diciembre de 2023

Estas actualizaciones solucionan los siguientes problemas:

- Al usar rutas múltiples con el firmware v7.x de la serie PS de Dell EqualLogic, es posible que se produzcan errores en el protocolo iSCSI.

30 de noviembre de 2023

Estas actualizaciones solucionan los siguientes problemas:

- A veces, el registro de repetición (parte de la función de alta disponibilidad) no reproduce todas las escrituras de la base de datos.
- Al ejecutar el `vdi-copy` comando para copiar una VDI a una SR, XenServer no informa correctamente del progreso de la operación.
- En XenCenter, personalizar una plantilla y, a continuación, exportarla y volver a importarla puede provocar que la plantilla no se importe.

Estas actualizaciones incluyen las siguientes mejoras:

- Agregue un controlador para Dell PERC12 (versión del controlador: mpi3mr 8.1.4.0.0).
- Mejoras generales de la API.
- Se ha eliminado la etiqueta «vista previa» del soporte de vTPM. Esto significa que vTPM estará listo para ser totalmente compatible cuando XenServer 8 pase de la versión preliminar a la versión totalmente compatible en producción.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

22 de noviembre de 2023

Estas actualizaciones incluyen las siguientes mejoras:

- La etiqueta "vista previa"se ha eliminado de la plantilla de Ubuntu 22.04. Este sistema operativo invitado está listo para ser totalmente compatible cuando XenServer 8 pase de una versión preliminar a una versión totalmente compatible en producción.

15 de noviembre de 2023

Estas actualizaciones incluyen las siguientes mejoras:

- Mejoras generales del SDK y tiempos de inicio de sesión de la API mejorados.
- Actualice Open vSwitch a la v2.17.7.

14 de noviembre de 2023

Estas actualizaciones incluyen correcciones de seguridad. Para obtener más información, consulte el boletín de seguridad https://support.citrix.com/article/CTX583037/.

6 de noviembre de 2023

Estas actualizaciones solucionan los siguientes problemas:

- La implementación de Windows mediante el arranque PXE y Configuration Manager puede provocar que Windows se bloquee.
- Si la sincronización horaria está inhabilitada, las máquinas virtuales de Windows no devuelven la hora correcta.

Estas actualizaciones incluyen las siguientes mejoras:

- Las máquinas virtuales Windows del modo de arranque UEFI ahora muestran el logotipo de Windows durante el arranque en lugar del logotipo de Tianocore.

23 de octubre de 2023

Estas actualizaciones incluyen mejoras y correcciones generales.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

16 de octubre de 2023

Estas actualizaciones incluyen soporte para los siguientes sistemas operativos invitados:

- Debian Bookworm 12
- Rocky Linux 9
- CentOS Stream 9

> **Nota:**
>
> Los clientes que quieran utilizar estos sistemas operativos invitados también deben instalar XenServer VM Tools for Linux v8.3.1-1 o posterior, que se puede descargar desde la página de descargas de productos de XenServer.

Estas actualizaciones incluyen las siguientes mejoras:

- Actualice el controlador Mellanox mlnx_en a 5.9-0.5.5.0.

10 de octubre de 2023

Estas actualizaciones incluyen correcciones de seguridad. Para obtener más información, consulte el boletín de seguridad https://support.citrix.com/article/CTX575089/.

5 de octubre de 2023

Estas actualizaciones incluyen soporte para el sistema operativo Red Hat Enterprise Linux 9. Consulte las notas de lanzamiento de Red Hat Enterprise Linux 9 para obtener más información técnica.

> **Nota:**
>
> Los clientes que quieran utilizar este sistema operativo invitado también deben instalar Citrix VM Tools para Linux v8.3.1-1 o posterior, que se puede descargar desde la página de descargas de productos de XenServer.

21 de septiembre de 2023

Estas actualizaciones incluyen mejoras y correcciones generales.

14 de septiembre de 2023

Estas actualizaciones incluyen las siguientes mejoras:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Habilite el equilibrio de interrupciones para los dispositivos PCI Fibre Channel (FC). Esto mejora el rendimiento de los SR de HBA FC rápidos, especialmente si se utilizan rutas múltiples.
- Solución para la errata #1474 de AMD. Inhabilite el C6 después de 1000 días de funcionamiento en los sistemas AMD Zen2 para evitar un bloqueo de aproximadamente 1044 días.

4 de septiembre de 2023

Estas actualizaciones solucionan los siguientes problemas:

- Las métricas de rendimiento no están disponibles para los SR de GFS2 y los discos en estos SR.
- No puede realizar instantáneas ni comprobar una máquina virtual suspendida si esa máquina virtual tiene un vTPM conectado.
- Si un host de XenServer se bloquea o se cierra abruptamente, es posible que no se puedan iniciar más máquinas virtuales de Windows 11 o migrar más máquinas virtuales de Windows 11 a ese host.
- Si, cuando se conectan los SR iSCSI, no están disponibles todas las rutas posibles (por ejemplo, un puerto remoto de un controlador fuera de línea está inactivo), al SR no se le agregarán sesiones iSCSI adicionales cuando se vuelva a acceder a esos puertos remotos.

Estas actualizaciones incluyen las siguientes mejoras:

- Actualice el controlador Intel ice a la versión 1.11.17.1.
- Mejoras de rendimiento para GFS2.

---

layout: doc
description: This release of XenServer contains a number of fixes to issues that were present in previous releases.—

Problemas resueltos

Se han corregido los siguientes problemas en XenServer 8. Además de estos problemas resueltos, se publican correcciones adicionales en los canales de actualización normal y de acceso anticipado.

General

- Reiniciar la máquina virtual no tiene el mismo efecto que apagarla y, a continuación, iniciarla. (CA-188042)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si un usuario de Active Directory hereda la función de administrador de grupo de un grupo de AD que tiene espacios en su nombre, el usuario no puede iniciar sesión en XenServer 8 a través de SSH. (CA-363207)
- En los grupos agrupados, una interrupción de la red puede provocar los siguientes problemas: incapacidad de volver a conectarse al almacenamiento de GFS2 tras el reinicio del host, incapacidad de agregar o eliminar hosts de un grupo, dificultades para administrar el grupo. (XSI-1386)

Gráficos

- En el hardware con tarjetas gráficas NVIDIA A16/A2, las máquinas virtuales con vGPU a veces no pueden migrar y se produce el error interno "Gpumon_interface.Gpumon_error([S(Internal_error);S((Failure "No vGPU available"))])". (CA-374118)

Invitados

Invitados de Windows

- Cuando se inician las máquinas virtuales Windows con arranque UEFI, muestran el logotipo de TianoCore. (CP-30146)
- En una VM Windows, a veces la dirección IP de una VIF de SR-IOV no está visible en XenCenter. (CA-340227)
- En una VM Windows con más de 8 vCPU, es posible que el escalado del lado de recepción no funcione porque el controlador xenvif no puede configurar la tabla de direccionamiento indirecto. (CA-355277)
- Si un host de XenServer se bloquea o se cierra abruptamente, es posible que no se puedan iniciar más máquinas virtuales de Windows 11 o migrar más máquinas virtuales de Windows 11 a ese host. (CA-37592)

Invitados de Linux

- Las herramientas de máquina virtual de XenServer para Linux pueden proporcionar un valor incorrecto para la memoria libre de la máquina virtual superior al valor correcto. (CA-352996)

Almacenamiento

- Al conectar un LVM SR iSCSI con objetivos multiobjetivo y comodín a un host, la operación de conexión puede fallar si no responden todos los destinos. (CA-375968)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si un SR de GFS2 tiene menos de 500 MB de espacio, al intentar eliminar los discos almacenados en este SR, la operación puede fallar. (CA-379589)
- Al intentar reparar una conexión a un NFS v3 SR de solo lectura, la operación puede fallar en el primer intento con el error "SM ha lanzado una excepción genérica de Python". Para solucionar este problema, vuelva a intentar la operación de reparación. Este problema se debe a una operación de escritura en el intento de reparación inicial. (XSI-1374)

Actualizaciones

- Mientras la actualización de instalación está en curso en un miembro del grupo, es posible que aparezca el error "No se pudo realizar la operación porque se están obteniendo las actualizaciones". ". Para resolver este error, puede volver a intentar la operación. (CA-381215)

Balance de carga

- Para un dispositivo virtual de equilibrio de carga de trabajo versión 8.2.2 y posteriores que no use LVM, no puede ampliar el espacio disponible en disco. (CA-358817)
- En XenCenter, el intervalo de fechas que se muestra en el informe de auditoría del grupo de equilibrio de carga de trabajo es incorrecto. (CA-357115)
- Durante la ventana de mantenimiento del equilibrio de carga de trabajo, el equilibrio de carga de trabajo no puede proporcionar recomendaciones de ubicación Cuando se produce esta situación, aparece el error: "La detección de grupos 4010 no se ha completado. Mediante el algoritmo original". La ventana de mantenimiento del equilibrio de carga de trabajo dura menos de 20 minutos y, de forma predeterminada, se programa a medianoche. (CA-359926)

XenCenter

Para obtener información sobre los problemas conocidos y resueltos en XenCenter, consulte Novedades de XenCenter.

---

layout: doc
description: These known issues are present in XenServer 8. Workarounds are available for some of the issues.—

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problemas conocidos

Este artículo contiene avisos y problemas menores de la versión XenServer 8, así como cualquier solución alternativa que pueda aplicar.

General

- Al intentar usar la consola en serie para conectarse a un host de XenServer, es posible que la consola en serie se niegue a aceptar la entrada del teclado. Si espera hasta que la consola se actualice dos veces, la consola acepta la entrada del teclado. (CA-311613)
- Cuando el almacenamiento en caché de lectura está habilitado, es más lento leer desde la instantánea principal que desde la hoja. (CP-32853)
- Cuando intenta iniciar sesión en la consola dom0 con una contraseña incorrecta, recibe el siguiente mensaje de error: `When trying to update a password, this return status indicates that the value provided as the current password is not correct.` Este mensaje de error se espera aunque esté relacionado con un cambio de contraseña, no con un inicio de sesión. Intente iniciar sesión con la contraseña correcta. (CA-356441)
- Si un host XenServer se apaga inesperadamente y se reinicia, cuando intenta recuperar máquinas virtuales que tenían un vTPM conectado, es posible que el vTPM no aparezca en la máquina virtual. (CA-37928)

Gráficos

- Cuando NVIDIA T4 se agrega en modo de transferencia a una VM en algún hardware de servidor específico, es posible que esa VM no se encienda. (CA-360450)

Invitados

- Si intenta migrar en vivo una máquina virtual con el control dinámico de memoria habilitado a un host de destino donde los recursos, como la memoria, son muy limitados, la migración a veces puede fallar. (CA-380607)

Invitados de Windows

- Para máquinas virtuales de Windows 10 unidas a un dominio (1903 y posteriores) con FireEye Agent instalado, las conexiones RDP repetidas y correctas pueden provocar que la máquina vir-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

tual se congele con un uso del 100% de la CPU en `ntoskrnl.exe`. Realice un reinicio completo en la VM para recuperarse de este estado. (CA-323760)

- Al crear una máquina virtual UEFI, la instalación de Windows requiere presionar una tecla para iniciarse. Si no presiona una tecla durante el período requerido, la consola de VM cambia al shell UEFI.

  Para evitar este problema, puede reiniciar el proceso de instalación de una de las siguientes maneras:

  - En la consola UEFI, escriba los siguientes comandos.

    ```
    EFI:
    EFI\BOOT\BOOTX64
    ```

  - Reinicie la VM

  Cuando se reinicie el proceso de instalación, observe la consola de la VM para ver el mensaje de instalación. Cuando aparezca el mensaje, presiona cualquier tecla. (CA-333694)

- Al intentar actualizar una VM con Windows 10 de 1909 a 20H2 o posterior, es posible que la actualización falle y aparezca una pantalla azul que muestre el error: DISPOSITIVO DE ARRANQUE INACCESIBLE. (XSI-1075)

  Para reducir las probabilidades de que se produzca este error, puede seguir los siguientes pasos antes de intentar actualizar:

  1. Actualice las herramientas de máquina virtual de XenServer para Windows de su máquina virtual a la versión más reciente.
  2. Cree una instantánea de la VM.
  3. En el registro de VM, elimine los siguientes valores de la clave HKEY_LOCAL_MACHINE\SYSTEM\CurrentC ActiveDeviceID, ActiveInstanceID y ActiveLocationInformation

- Al crear una máquina virtual Windows a partir de una plantilla que está configurada para no actualizar automáticamente sus controladores, la máquina virtual creada está configurada incorrectamente para actualizar sus controladores. Para solucionar este problema, ejecute el siguiente comando: `xe pool-param-set policy-no-vendor-device=true uuid =<pool-uuid>`. Este comando garantiza que las máquinas virtuales futuras creadas a partir de la plantilla estén configuradas correctamente para que no actualicen automáticamente los controladores. Las máquinas virtuales que se generaron anteriormente a partir de la plantilla no se modifican. (CA-371529)

- Las operaciones de vTPM realizadas por el usuario o por Windows en segundo plano pueden fallar en las siguientes situaciones:

  - Si la pila de herramientas o el host de XenServer se bloquean antes de que la operación se sincronice con el disco. Se ignoran los errores al escribir en el disco.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

En el caso de este tipo de error, el vTPM devuelve un error al sistema operativo. Windows registra estos errores en el registro de eventos del sistema.

- Si tiene Bitlocker habilitado en una máquina virtual Windows e intenta suspenderla o reanudarla, la máquina virtual a veces puede fallar. (CA-368791)

  Además, Bitlocker no es compatible con máquinas virtuales que tengan un vTPM adjunto.

Invitados de Linux

- No puede usar la función de control dinámico de memoria (DMC) en las máquinas virtuales Red Hat Enterprise Linux 8, Red Hat Enterprise Linux 9, Rocky Linux 8, Rocky Linux 9 o CentOS Stream 9, ya que estos sistemas operativos no admiten la expansión de memoria con el hipervisor Xen. (CA-378797)
- En algunas máquinas virtuales Linux, especialmente en los sistemas ocupados con E/S de disco pendientes, los intentos de suspender o migrar en vivo la máquina virtual pueden fallar. Para solucionar este problema, intenta aumentar el valor de `/sys/power/pm_freeze_timeout`, por ejemplo, a 300000. Si esta solución alternativa no funciona correctamente, puede actualizar el núcleo Linux de la máquina virtual a la versión más reciente. (CP-41455)
- Si instala Debian 10 (Buster) mediante el arranque de red PXE, no agregue`console=tty0` los parámetros de arranque. Este parámetro puede provocar problemas con el proceso de instalación. Use solo `console=hvc0` en los parámetros de arranque. (CA-329015)
- Debido a un problema conocido en algunos sistemas operativos SUSE Linux, si intenta activar un volcado automático en una máquina virtual SUSE Linux con 32 o más vCPU, la operación falla y la máquina virtual no se reinicia automáticamente. Este problema afecta a los siguientes sistemas operativos: SUSE Linux Enterprise Server 15 SP1, 15 SP2, 15 SP3 y 15 SP4. (CA-375759)

Instalación

- Al actualizar o instalar XenServer 8 desde una ISO ubicada en un servidor IIS, la instalación o la actualización pueden fallar e impedir que los hosts se reinicien. La consola remota muestra el error de GRUB: "Archivo '/boot/grub/i3860pc/normal.mod'no encontrado. Entrar en modo de rescate". Este problema se debe a que la configuración de IIS hace que falten los archivos del paquete. Para evitar este problema, asegúrese de que se permite el doble escape en IIS antes de extraer la ISO de instalación en él. (XSI-1063)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Internacionalización

- Los caracteres que no son ASCII, por ejemplo, los caracteres con acentos, no se pueden usar en la consola host. (CA-40845)
- En una máquina virtual Windows con XenServer VM Tools for Windows instalado, es posible que no se pueda copiar y pegar caracteres de doble byte si se utiliza la consola de escritorio predeterminada de XenCenter. Los caracteres pegados aparecen como signos de interrogación (?).

  Para evitar este problema, puede usar la consola de escritorio remoto en su lugar. (CA-281807)

Almacenamiento

- Si crea una nueva instalación de XenServer en un host con un SR de XFS local en un dispositivo NVMe, el almacenamiento local no se conecta al arrancar. La acción falla y aparece el error: "Raised Server_error(SR_BACKEND_FAILURE, [FileNotFoundError; [Errno 2] No such file or directory: '/sys/block/nvme0n/queue/scheduler'])".

  Si aparece este problema, contacte con nosotros en feedback@xenserver.com. Estamos trabajando activamente en una solución que se entregará en una actualización futura. Asegúrese de configurar su grupo para recibir las actualizaciones más recientes.
- Si usa SR de GFS2 y tiene dos hosts en su grupo agrupado, su clúster puede perder quórum y límite durante una actualización. Para evitar esta situación, agregue o elimine un host del clúster. Asegúrese de tener uno o tres hosts en su grupo durante el proceso de actualización. (CA-313222)
- Si usa una SR de GFS2 y su red de clústeres está en una VLAN que no es de administración, no puede agregar ni eliminar hosts a su agrupación en clústeres. (XSI-1604)
- Después de eliminar un LUN de HBA de una SAN, es posible que vea mensajes de registro y errores de E/S al consultar la información del volumen lógico. Para solucionar este problema, reinicie el host de XenServer. (XSI-984)
- No puede establecer ni cambiar el nombre del tmpfs SR utilizado por el PVS-Accelerator. Cuando `type` es `tmpfs`, el comando `xe sr-create` ignora el valor establecido para `name-label` y, en su lugar, utiliza un valor fijo. Si intenta ejecutar el comando `xe sr-param-set` para cambiar el nombre de tmpfs SR, recibirá el error SCRIPT_MISSING.
- No puede ejecutar más de 200 máquinas virtuales habilitadas para PVS-Accelerator en un host de XenServer. (CP-39386)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Terceros

- Una limitación en los clientes SSH recientes significa que SSH no funciona para nombres de usuario que contienen alguno de los siguientes caracteres: `{ } [] | &`. Asegúrese de que sus nombres de usuario y nombres de servidores de Active Directory no contengan ninguno de estos caracteres.

XenCenter

Para obtener información sobre los problemas conocidos y resueltos en XenCenter, consulte Novedades de XenCenter.

Elementos retirados

April 10, 2024

Los anuncios de este artículo le avisan con antelación sobre las plataformas, los productos y las funciones que se van a eliminar gradualmente para que pueda tomar decisiones empresariales oportunas. Supervisamos el uso y los comentarios de los clientes para determinar cuándo se retiran. Estos anuncios están sujetos a cambios en las versiones posteriores y es posible que no contengan todas las funciones o funciones retiradas.

Para obtener información detallada sobre el ciclo de vida útil de los productos, consulte el artículo Product Lifecycle Support Policy.

Elementos eliminados y obsoletos

En la siguiente tabla se muestran las plataformas, los productos y las funciones que están en desuso o que se han eliminado.

Los elementos *retirados* no se eliminan inmediatamente. Seguimos admitiéndolos en la versión actual, pero se eliminarán en una versión futura.

Los elementos*eliminados* se eliminan o ya no se admiten en XenServer.

Las fechas en **negrita** indican cambios en esta versión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Elemento	Retirada anunciada en	Eliminado en	Alternativa
Derecho de uso de XenServer para clientes de Citrix Virtual Apps and Desktops	**XenServer 8**	**XenServer 8**	Obtenga una licencia de Premium Edition en https://xenserver.com/buy.
Modo de arranque de BIOS para hosts de XenServer	**XenServer 8**		En su lugar, instale sus hosts con el modo de arranque UEFI.
Conexiones de XenCenter a hosts de XenServer de la versión 7.x y anteriores.	**XenCenter 2023.3.1**	**XenCenter 2023.3.1**	Actualice los hosts de XenServer que no son compatibles.
Dispositivo virtual Linux de demostración	**XenServer 8**	**XenServer 8**	
Soporte para Windows 10 de 32 bits	**XenServer 8**	**XenServer 8**	
Soporte para Debian Bullseye 11 de 32 bits	8.2 CU1	**XenServer 8**	
Compatibilidad con Bromium Secure Platform en máquinas virtuales de Windows	8.2 CU1	8.2 CU1	
Comprobación de estado	XenCenter 8.2.6	XenCenter 8.2.7	
Carga de informes de estado del servidor a Citrix Insight Services (CIS) desde XenCenter	XenCenter 8.2.6	XenCenter 8.2.7	Sube sus informes de estado manualmente a través del sitio web del CIS.
PuTTY instalado con XenCenter	XenCenter 8.2.6	**XenCenter 2023.3.1**	En las versiones futuras de XenCenter, debe instalar su propia instancia de PuTTY u OpenSSH en el sistema en el que esté instalado XenCenter.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Elemento	Retirada anunciada en	Eliminado en	Alternativa
Localización de XenCenter al japonés y al chino simplificado	XenCenter 8.2.6	**XenCenter 2023.3.1**	
Canal de fibra por Ethernet (FCoE) de software	8.2 CU1		
AMD MxGPU	8.2 CU1	**XenServer 8**	
Intel GVT-g	8.2 CU1		
Paquete complementario de PVS-Accelerator por separado	8.2 CU1	**XenServer 8**	Estas capacidades ahora están incluidas en el producto principal.
Soporte para los siguientes sistemas operativos Linux: CoreOS, Ubuntu 16.04, Debian Jessie 8, Debian Stretch 9, SUSE Linux Enterprise Server 12 SP3, SUSE Linux Enterprise Desktop 12 SP3, CentOS 8	8.2 CU1	8.2 CU1	Actualice sus máquinas virtuales a una versión posterior de su sistema operativo cuando esté disponible.
Soporte para los siguientes sistemas operativos Linux: Ubuntu 18.04, SUSE Linux Enterprise Server 12 SP4, SUSE Linux Enterprise Desktop 12 SP4	8.2 CU1	8.2 CU1	Actualice sus máquinas virtuales a una versión posterior de su sistema operativo cuando esté disponible.
Compatibilidad con Windows Server 2012 R2	8.2 CU1	**XenServer 8**	Actualice sus máquinas virtuales a una versión posterior de su sistema operativo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Elemento	Retirada anunciada en	Eliminado en	Alternativa
Compatibilidad con Windows Server 2012 y Windows 8.1	8.2 CU1	8.2 CU1	Actualice sus máquinas virtuales a una versión posterior de su sistema operativo.
Transferencia de VM	8.2 CU1	8.2 CU1 (XenCenter 8.2.3)	Use la versión más reciente de XenCenter. Desde XenCenter 8.2.3, el mecanismo utilizado para la importación/exportación de OVF/OVA y la importación de imágenes de un solo disco se ha simplificado y estas operaciones ahora se realizan sin usar la máquina virtual de transferencia.
Measured Boot Supplemental Pack	8.2 CU1	8.2 CU1	
Paquete complementario de administración de contenedores	8.2	8.2	
Compatibilidad con Lights-Out (iLO) Hewlett-Packard Integrated Lights-Out	8.2	8.2	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Elemento	Retirada anunciada en	Eliminado en	Alternativa
Compatibilidad con los siguientes procesadores heredados: `Xeon E3/5/7 family - Sandy Bridge`,`Xeon E3/5/7 v2 family - Ivy Bridge`	8.2	8.2	
El `guest-tools.iso` archivo incluido en la ISO de instalación de XenServer	8.2	8.2	Descargue XenServer VM Tools para Windows o Linux desde la página de descargas de XenServer.
Compatibilidad con Windows 7, Windows Server 2008 SP2 y Windows Server 2008 R2 SP1	8.2	8.2	Actualice sus máquinas virtuales a una versión posterior de su sistema operativo.
Modo SSL heredado y soporte para el protocolo TLS 1.0/1.1	8.2	8.2	
Redes privadas entre servidores	8.2	8.2	
Los siguientes comandos de registro de la CLI de xe: `diagnostic-db-log`, `log-set-output`, `log-get-keys`, `log-get`, `log-reopen`	8.2	**XenServer 8**	
vSwitch Controller (consulte las notas)	8.1	8.2	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Elemento	Retirada anunciada en	Eliminado en	Alternativa
Diseños de partición heredados: Diseño de partición DOS, diseño de partición GPT antiguo. Tenga en cuenta que este cambio también elimina la compatibilidad con servidores con menos de 46 GB de espacio en disco principal.	8.1	**XenServer 8**	
Instantáneas en modo inactivo y de VSS	8.1	8.1	
Compatibilidad con Ubuntu 14.04	8.1	8.1	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Elemento	Retirada anunciada en	Eliminado en	Alternativa
Soporte para todas las VM paravirtualizadas (PV), incluidas las siguientes: Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, CentOS 5, CentOS 6, Oracle Enterprise Linux 5, Oracle Enterprise Linux 6, Scientific Linux 6, NeoKylin Linux Advanced Server 6.2, Debian Wheezy 7, SUSE Linux Enterprise Server 11 SP3, SUSE Servidor empresarial Linux 11 SP4, SUSE Linux Enterprise Server 12, SUSE Linux Enterprise Server 12 SP1, SUSE Linux Enterprise Server 12 SP2, SUSE Linux Enterprise Desktop 11 SP3, SUSE Linux Enterprise Desktop 12, SUSE Linux Enterprise Desktop 12 SP1, SUSE Linux Enterprise Desktop 12 SP2	8.1	8.1	Actualice sus máquinas virtuales a una versión posterior de su sistema operativo antes de pasarlas a la última versión de XenServer.
Controladores heredados: `qla4xxx`, `qla3xxx`, `netxen_nic`, `qlge`, `qlcnic`	8.0		

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Elemento	Retirada anunciada en	Eliminado en	Alternativa
El instalador de XenCenter se incluye con el medio de instalación de XenServer.	8.0	8.0	En su lugar, descargue el instalador de XenCenter desde la página Descargas.
Conexiones de XenCenter a hosts de XenServer de la versión 6.x y anteriores.	8.0	8.0	Actualice los hosts de XenServer que no son compatibles.
Soporte para la integración de Nutanix.	8.0	8.0	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Elemento	Retirada anunciada en	Eliminado en	Alternativa
Compatibilidad con los siguientes procesadores heredados: Opteron 13xx Budapest, Opteron 23xx/83xx Barcelona, Opteron 23xx/83xx Shanghai, Opteron 24xx/84xx Istanbul, Opteron 41xx Lisbon, Opteron 61xx Magny Cours, Xeon 53xx Clovertown, Xeon 54xx Harpertown, Xeon 55xx Nehalem, Xeon 56xx Westmere-EP, Xeon 65xx/75xx Nehalem-EX, Xeon 73xx Tigerton, Xeon 74xx Dunnington	8.0	8.0	Para obtener información sobre los procesadores compatibles, consulte la Lista de compatibilidad de hardware

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Elemento	Retirada anunciada en	Eliminado en	Alternativa
Compatibilidad con `qemu-trad`. Ya no es posible usar `qemu-trad` al configurar `platform -devicemodel= qemu-trad`. Todas las máquinas virtuales creadas con el perfil de dispositivo `qemu-trad` se actualizan automáticamente al perfil `qemu-upstream-compat`.	8.0	8.0	
Compatibilidad con las siguientes plantillas invitadas: Debian 6 Squeeze, Ubuntu 12.04, Windows heredado, Asianux Server 4.2, 4.4 y 4.5, NeoKylin Linux Security OS 5, Linx Linux 6, Linx Linux 8, GreatTurbo Enterprise Server 12, Yinhe Kylin 4	8.0	8.0	
Controladores de Windows heredados de la ISO de Citrix VM Tools	8.0	8.0	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Notas

Comprobación de estado

Windows conserva los registros del servicio Health Check para solucionar problemas. Para eliminar estos registros, elimínelos manualmente de `%SystemRoot%\System32\Winevt\Logs`la máquina Windows que ejecute XenCenter.

Control de memoria dinámico (DMC)

Esta función figuraba anteriormente como obsoleta. El aviso de obsolescencia se retiró el 30 de enero de 2023. Las versiones futuras de XenServer admiten DMC.

Desconexión de la controladora vSwitch

Ya no se admite vSwitch Controller. Desconecte el vSwitch Controller del grupo antes de intentar actualizar o actualizar a la versión más reciente de XenServer.

1. En la interfaz de usuario del controlador vSwitch, vaya a la ficha **Visibilidad y control**.
2. Busque el grupo que quiere desconectar en la tabla **Todos los grupos de recursos**. Los grupos de la tabla se enumeran con la dirección IP del coordinador del grupo.
3. Haga clic en el icono de engranaje y seleccione **Eliminar grupo**.
4. Haga clic en **Eliminar** para confirmar.

Después de la actualización o actualización, se producen los siguientes cambios de configuración:

- Las redes privadas entre servidores vuelven a ser redes privadas de un solo servidor.
- Los ajustes de calidad de servicio realizados a través de la consola DVSC ya no se aplican. Los límites de velocidad de red ya no se aplican.
- Se eliminan las reglas de listas ACL. Se permite todo el tráfico de las VM.
- La duplicación de puertos (RSPAN) está inhabilitada.

Después de la actualización o actualización, si encuentra algún estado sobrante sobre vSwitch Controller en el grupo, borre el estado con el siguiente comando de la CLI: `xe pool-set-vswitch-controller address=`

Inicio rápido

April 10, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

En este artículo se explica cómo instalar y configurar XenServer (anteriormente Citrix Hypervisor) y su interfaz gráfica de usuario basada en Windows, XenCenter. Después de la instalación, le lleva a través de la creación de máquinas virtuales (VM) de Windows y, a continuación, la creación de plantillas de VM personalizadas que puede usar para crear varias máquinas virtuales similares rápidamente. Por último, en este artículo se muestra cómo crear un grupo de hosts, que proporciona la base para migrar máquinas virtuales en ejecución entre hosts mediante la migración en vivo.

Centrándose en los casos más básicos, este artículo tiene como objetivo configurarlo rápidamente.

Este artículo está dirigido principalmente a los nuevos usuarios de XenServer y XenCenter. Está destinado a aquellos usuarios que desean administrar XenServer mediante XenCenter. Para obtener información sobre cómo administrar XenServer mediante los comandos xe
basados en Linux a través de la interfaz de línea de comandos de XenServer (conocida como CLI xe), consulte Interfaz de línea de comandos.

Terminología y abreviaturas

- *Servidor*: un equipo físico que ejecuta XenServer.
- *Host*: una instalación de XenServer que aloja máquinas virtuales (VM).
- *Máquina virtual (VM)*: Un equipo compuesto enteramente por software que puede ejecutar su propio sistema operativo y aplicaciones como si fuera un equipo físico. Una VM se comporta exactamente como un equipo físico y contiene su propia CPU, RAM, disco duro y NIC virtuales (basados en software).
- *Grupo*: una única entidad administrada que une varios hosts de XenServer y sus máquinas virtuales.
- *Coordinador de grupo* (anteriormente *maestro de grupo*): anfitrión principal de un grupo que proporciona un único punto de contacto para todos los anfitriones del grupo y enruta la comunicación a otros miembros del grupo según sea necesario.
- *Repositorio de almacenamiento (SR)*: un contenedor de almacenamiento en el que se almacenan los discos virtuales.

Componentes principales

XenServer

XenServer es una plataforma de virtualización de servidores completa, con todas las capacidades necesarias para crear y administrar una infraestructura virtual. XenServer está optimizado para servidores virtuales Windows y Linux.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

XenServer se ejecuta directamente en el hardware del servidor sin necesidad de un sistema operativo subyacente, lo que se traduce en un sistema eficiente y escalable. XenServer extrae los elementos de la máquina física (como discos duros, recursos y puertos) y los asigna a las máquinas virtuales (VM) que se ejecutan en ella.

XenServer le permite crear máquinas virtuales, tomar instantáneas de discos de máquinas virtuales y administrar cargas de trabajo de máquinas virtuales.

XenCenter

XenCenter es una interfaz de usuario gráfica basada en Windows. XenCenter le permite administrar los hosts, los grupos y el almacenamiento compartido de XenServer. Use XenCenter para implementar, administrar y supervisar máquinas virtuales desde su máquina de escritorio Windows.

La *ayuda en línea* de XenCenter también es un recurso excelente para comenzar a usar XenCenter. Presione F1 en cualquier momento para acceder a la información sensible al contexto.

Instalación de XenServer y XenCenter

En esta sección, configurará una instalación mínima de XenServer.

Lo que aprenderás

Aprenderás a:

- Instale XenServer en un único servidor físico
- Instalar XenCenter en un equipo Windows
- Conexión de XenCenter y XenServer para formar la infraestructura para crear y ejecutar máquinas virtuales (VM)

Requisitos

Para empezar, necesitas los siguientes elementos:

- Un equipo físico para ser el host de XenServer
- Un equipo Windows para ejecutar la aplicación XenCenter
- Archivos de instalación para XenServer y XenCenter

El equipo host de XenServer se dedica exclusivamente a la tarea de ejecutar XenServer y alojar máquinas virtuales, y no se utiliza para otras aplicaciones. El equipo que ejecuta XenCenter puede ser cualquier equipo Windows de uso general que satisfaga los requisitos de hardware. También

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

puede usar este equipo para ejecutar otras aplicaciones. Para obtener más información, consulte Requisitos del sistema.

Puede descargar los archivos de instalación desde XenServer Downloads.

Instalar el host de XenServer

Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.

Todos los servidores tienen al menos una dirección IP asociada a ellos. Para configurar una dirección IP estática para el host (en lugar de usar DHCP), tenga a mano la dirección IP estática antes de iniciar este procedimiento.

> **Sugerencia:**
>
> Presione **F12** para avanzar rápidamente a la siguiente pantalla del instalador. Para obtener ayuda general, presione **F1**.

Para instalar el host de XenServer:

1. Grabe los archivos de instalación de XenServer en un CD o cree un USB de arranque.

   > **Nota:**
   >
   > Para obtener información sobre el uso de HTTP, FTP o NFS como fuente de instalación, consulte Instalar XenServer.

2. Haga una copia de seguridad de los datos que quiere conservar. La instalación de XenServer sobrescribe los datos de los discos duros que seleccione para usar en la instalación.
3. Inserte los medios de instalación en el sistema.
4. Reinicie el sistema.
5. Arranque desde el medio de instalación local (si es necesario, consulte la documentación del proveedor de hardware para obtener información sobre cómo cambiar el orden de arranque).
6. Tras los mensajes de arranque iniciales y la pantalla de **bienvenida a XenServer** , seleccione la distribución del teclado para la instalación.
7. Cuando aparezca la pantalla de **bienvenida a XenServer Setup** , seleccione **Aceptar**.
8. Lea y acepte el EULA de XenServer.

   > **Nota:**
   >
   > Si ve una advertencia sobre **el hardware del sistema**, asegúrese de que la función de virtualización de hardware esté habilitada en el firmware del sistema.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

9. Seleccione **Aceptar** para realizar una instalación limpia.
10. Si tiene varios discos duros, elija un disco principal para la instalación. Seleccione **Aceptar**.

    Elija los discos que quiere utilizar para el almacenamiento de máquinas virtuales. Elija **Aceptar**.
11. Seleccione **Medios locales** como fuente de instalación.
12. Seleccione **Omitir verificación** y, a continuación, seleccione **Aceptar**.

    > **Nota:**
    >
    > Si tiene problemas durante la instalación, verifique el origen de la instalación.

13. Cree y confirme una contraseña raíz, que la aplicación XenCenter utiliza para conectarse al host de XenServer.
14. Configure la interfaz de administración que se utilizará para conectarse a XenCenter.

    Si el equipo tiene varias NIC, seleccione la NIC que quiere usar para el tráfico de administración (normalmente la primera NIC).
15. Configure la dirección IP de la NIC de administración con una dirección IP estática o use DHCP.
16. Especifique el nombre de host y la configuración de DNS de forma manual o automática a través de DHCP.

    Si configura el DNS manualmente, introduzca las direcciones IP de sus servidores DNS principal (obligatorio), secundario (opcional) y terciario (opcional) en los campos proporcionados.
17. Seleccione su zona horaria.
18. Especifique cómo quiere que el host determine la hora local: mediante NTP o la entrada manual de la hora. Elija **Aceptar**.

    - Si usa NTP, puede especificar si DHCP establece el servidor horario. Como alternativa, puede introducir al menos un nombre de host NTP o una dirección IP en los siguientes campos.
    - Si seleccionó establecer la fecha y la hora manualmente, se le solicitará que lo haga.
19. Seleccione **Instalar XenServer**.

    Se inicia el proceso de instalación. Esto puede tardar unos minutos.
20. La siguiente pantalla le pregunta si quiere instalar paquetes adicionales. Elige **No** para continuar.
21. En la pantalla **Instalación completa**, expulse el medio de instalación y, a continuación, seleccione **Aceptar** para reiniciar el host.

    Una vez reiniciado el host, XenServer **muestra**xsconsole, una consola de configuración del sistema.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Anote la dirección IP que se muestra. Esta dirección IP se utiliza cuando se conecta XenCenter al host.

Instale XenCenter

XenCenter normalmente se instala en el sistema local. Puede descargar el instalador de XenCenter desde la página de descargas de XenServer.

Para instalar XenCenter:

1. Descargue o transfiera el instalador de XenCenter al equipo en el que quiere ejecutar XenCenter.
2. Haga doble clic en el archivo `.msi` de instalación para comenzar la instalación.
3. Siga el asistente de configuración, que le permite modificar la carpeta de destino predeterminada y, a continuación, instalar XenCenter.

Conectar XenCenter al host XenServer

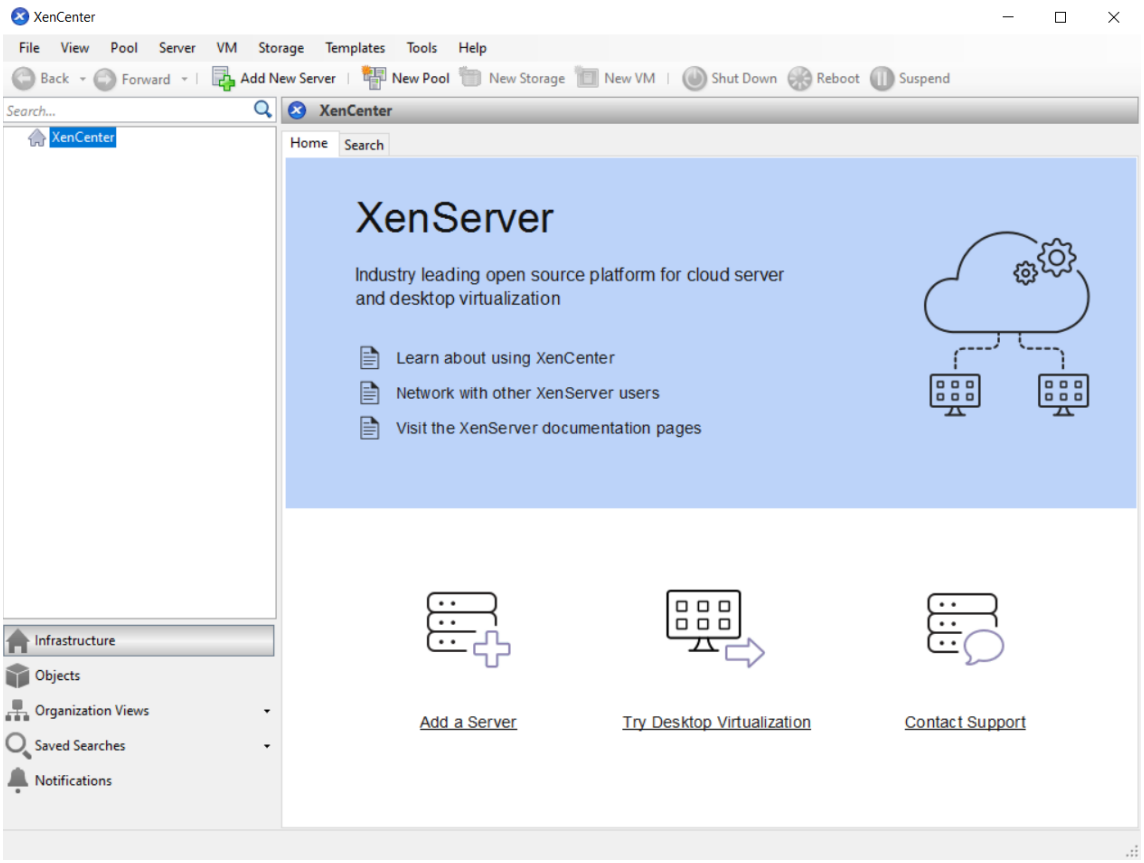
Este procedimiento le permite agregar un host a XenCenter.

Para conectar XenCenter al host de XenServer:

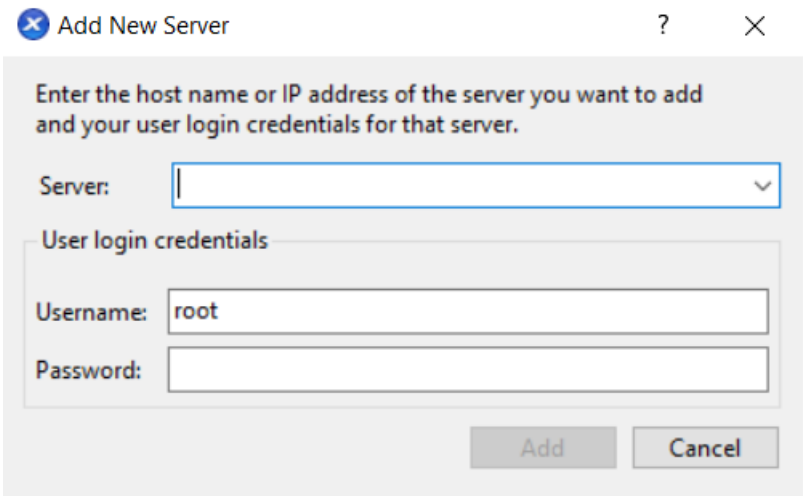
1. Inicie XenCenter.

   El programa se abre en la ficha **Inicio**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Haga clic en el icono **Agregar nuevo servidor** para abrir el cuadro de diálogo **Agregar nuevo servidor**.



3. En el campo **Servidor**, introduzca la dirección IP del host. Introduzca el nombre de usuario raíz y la contraseña que configuró durante la instalación de XenServer. Elige **Add**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> La primera vez que agregue un host, aparecerá el cuadro de diálogo **Guardar y restaurar el estado de la conexión**. Este cuadro de diálogo le permite establecer sus preferencias para almacenar la información de conexión del host y restaurar automáticamente las conexiones del host.

Licencia XenServer

Puede usar XenServer sin licencia (edición de prueba). La Edición de prueba le permite probar las funciones de la Edición Premium, pero en un grupo de tamaño restringido de hasta 3 hosts.

Si utiliza XenServer para ejecutar las cargas de trabajo de Citrix Virtual Apps and Desktops, debe tener una licencia Premium Edition. Para obtener más información sobre cómo obtener una licencia de XenServer, consulte https://xenserver.com/buy. Los clientes actuales de Citrix Virtual Apps and Desktops pueden solicitar participar en nuestra promoción y recibir hasta 10 000 licencias de socket de XenServer Premium Edition de forma gratuita. Más información.

Si tiene una licencia de XenServer, aplíquela ahora. Para obtener más información, consulte Licencias.

Crear un grupo de hosts de XenServer

Un grupo de recursos está compuesto por varias instalaciones host de XenServer, unidas entre sí como una sola entidad administrada.

Los grupos de recursos le permiten ver varios hosts y su almacenamiento compartido conectado como un único recurso unificado. Puede implementar máquinas virtuales de manera flexible en todo el grupo de recursos en función de las necesidades de recursos y las prioridades empresariales. Un grupo puede contener hasta 64 hosts que ejecuten la misma versión del software XenServer, con el mismo nivel de parche y con hardware ampliamente compatible.

Se designa a un anfitrión de la agrupación como *coordinador de la agrupación*. El coordinador de la agrupación proporciona un único punto de contacto para toda la agrupación y enruta la comunicación a otros miembros de la agrupación según sea necesario. Cada miembro de un grupo de recursos contiene toda la información necesaria para asumir el papel de coordinador del grupo si es necesario. El coordinador del grupo es el primer host que aparece para el grupo en el panel Recursos de XenCenter. Para encontrar la dirección IP del coordinador del grupo, seleccione el coordinador del grupo y haga clic en la ficha **Buscar**.

En un grupo con almacenamiento compartido, puede iniciar las máquinas virtuales en *cualquier* miembro del grupo que tenga suficiente memoria y mover las máquinas virtuales de un host a otro de forma dinámica. Las VM se mueven mientras se ejecutan y con un tiempo de inactividad mínimo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si un host XenServer individual sufre un error de hardware, puede reiniciar las máquinas virtuales con errores en otro host del mismo grupo.

Si la función de alta disponibilidad está habilitada, las máquinas virtuales protegidas se mueven *automáticamente* si se produce un error en un host. En un grupo habilitado para HA, se nomina automáticamente un nuevo coordinador de grupos si el coordinador de grupos se cierra.

> **Nota:**
>
> Para obtener una descripción de la tecnología de grupos heterogéneos, consulte Hosts y grupos de recursos.

Lo que aprenderás

Aprenderás a:

- Crea un grupo de anfitriones
- Configurar una red para el grupo
- Vincular tarjetas NIC
- Configurar almacenamiento compartido para la agrupación

Si bien XenServer admite muchas soluciones de almacenamiento compartido, esta sección se centra en dos tipos comunes: NFS e iSCSI.

Requisitos

Para crear un grupo con almacenamiento compartido, necesita los siguientes elementos:

- Un segundo host de XenServer, con un tipo de procesador similar.
  Conecte este host a la aplicación XenCenter.
- Un repositorio de almacenamiento para almacenamiento basado en IP

Para empezar rápidamente, esta sección se centra en la creación de grupos *homogéneos*. Dentro de un grupo homogéneo, todos los hosts deben tener procesadores compatibles y ejecutar la misma versión de XenServer, con el mismo tipo de licencia de producto de XenServer. Para obtener una lista completa de los requisitos de grupos homogéneos, consulte Requisitos del sistema.

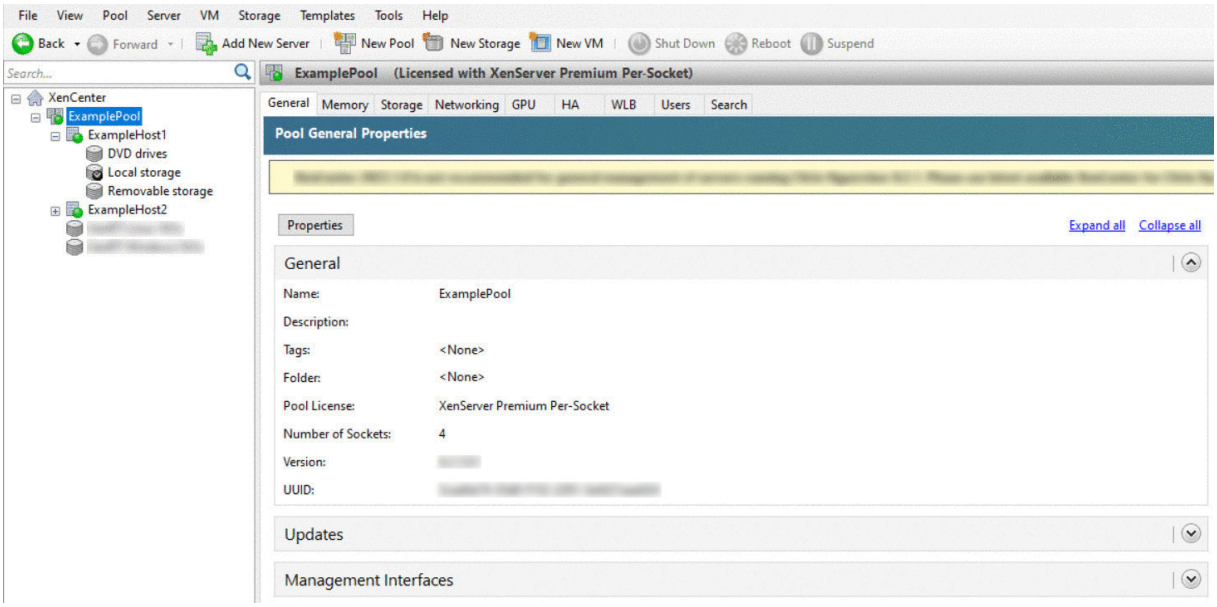
Crear un grupo

Para crear un grupo:

1. En la barra de herramientas, haga clic en el botón **Nuevo grupo**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Introduzca un nombre y una descripción opcional para el nuevo grupo.
3. Nomine al coordinador de la agrupación seleccionando un anfitrión de la lista de **coordinadores**.
4. Seleccione el segundo anfitrión para colocarlo en el nuevo grupo en la lista de **miembros adicionales**.
5. Haga clic en **Crear grupo**.
   La nueva agrupación aparece en el panel **Recursos**.



Configurar redes para la agrupación

Al instalar XenServer, se crea una conexión de red, normalmente en la primera NIC del grupo en la que se especificó una dirección IP (durante la instalación de XenServer).

Sin embargo, es posible que deba conectar su grupo a las VLAN y a otras redes físicas. Para hacerlo, debe agregar estas redes al grupo. Puede configurar XenServer para conectar cada NIC a una red física y a varias VLAN.

Antes de crear redes, asegúrese de que el cableado coincida con cada host del grupo. Conecte las NIC de cada host a las mismas redes físicas que las NIC correspondientes de los demás miembros del grupo.

> **Nota:**
>
> Si las NIC no estaban conectadas a las NIC del host cuando instaló XenServer:
>
> - Conecte las NIC

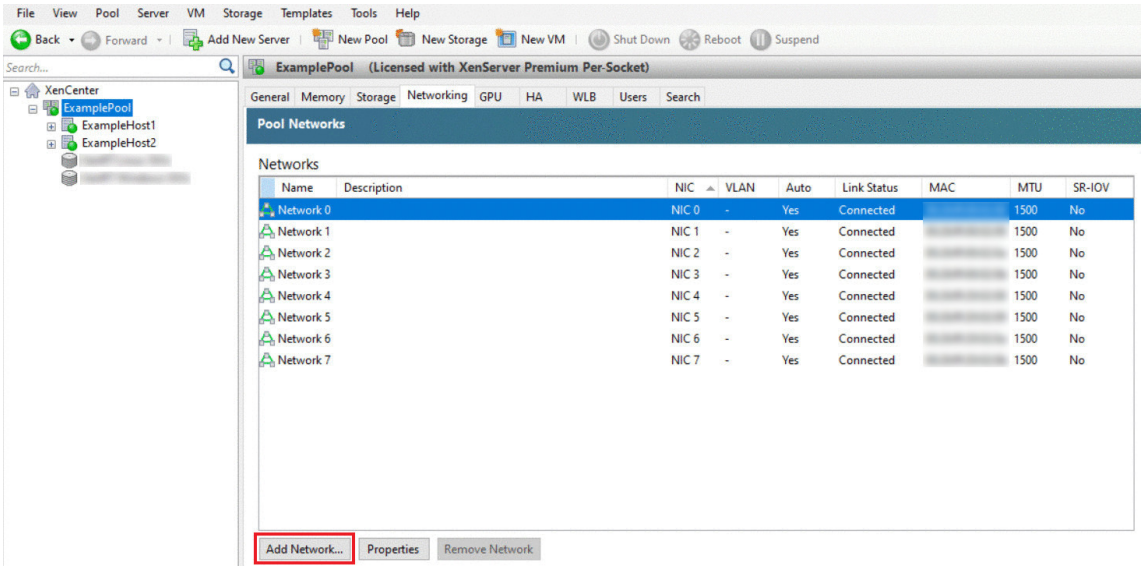
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - En XenCenter, seleccione la ficha **NIC de <su host>**.
> - Haga clic en **Volver a escanear** para que aparezcan

Para obtener información adicional sobre la configuración de redes de XenServer, consulte Redes y Acerca de las redes deXenServer.

Para agregar una red a XenServer:

1. En el panel **Recursos** de XenCenter, seleccione el grupo.
2. Haga clic en la ficha **Redes**.
3. Haga clic en **Agregar red**.



4. En la página **Seleccionar tipo**, seleccione **Red externa** y haga clic en **Siguiente**.
5. En la página **Nombre**, introduzca un nombre significativo para la red y una descripción.
6. En la página **Configuración de red**, especifique lo siguiente:

   - **NIC:** seleccione la NIC que quiere que XenServer utilice para enviar y recibir datos de la red.
   - **VLAN:** Si la red es una VLAN, introduzca el identificador de VLAN (o “etiqueta”).
   - **MTU:** Si la red utiliza tramas gigantes, introduzca un valor para la Unidad de transmisión máxima (MTU) entre 1500 y 9216. De lo contrario, deje la casilla MTU en su valor predeterminado de 1500.

   Si configura muchas máquinas virtuales para que usen esta red, puede seleccionar la casilla **Agregar automáticamente esta red a las nuevas máquinas virtuales**. Esta opción agrega la red de forma predeterminada.

7. Haga clic en **Finalizar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

NIC de unión

La unión de NIC puede hacer que su host sea más resistente mediante el uso de dos o más NIC físicas como si se tratara de un único canal de alto rendimiento. Esta sección solo proporciona una breve descripción general de la vinculación, también conocida como formación de *equipos NIC*. Antes de configurar las uniones para su uso en un entorno de producción, recomendamos leer información más detallada sobre las uniones. Para obtener más información, consulte Redes.

XenServer admite los siguientes modos de enlace: activo/activo, activo/pasivo (activo/reserva) y LACP. Activo/activo proporciona equilibrio de carga y redundancia para el tráfico basado en VM. Para otros tipos de tráfico (almacenamiento y administración), activo/activo no puede equilibrar la carga del tráfico. Como resultado, el LACP o las rutas múltiples son la mejor opción para el tráfico de almacenamiento. Para obtener información sobre las rutas múltiples, consulte Almacenamiento. Para obtener más información sobre la vinculación, consulte Redes.

Las opciones de LACP no están visibles ni disponibles a menos que configure vSwitch como la pila de red. Del mismo modo, los conmutadores deben admitir el estándar IEEE 802.3ad. El conmutador debe contener un grupo LAG independiente configurado para cada enlace LACP en el host. Para obtener más información sobre la creación de grupos de LAG, consulte Redes.

Para unir NIC:

1. Asegúrese de que las NIC que quiere vincular entre sí no estén en uso: apague las máquinas virtuales con interfaces de red virtual mediante estas NIC antes de crear el enlace. Una vez creado el enlace, vuelva a conectar las interfaces de red virtual a una red apropiada.
2. Seleccione el host en el panel **Recursos**, abra la ficha **NIC** y haga clic en **Crear enlace**.
3. Seleccione las NIC que quiere unir. Para seleccionar una NIC, seleccione su casilla de verificación en la lista. Se pueden seleccionar hasta cuatro NIC en esta lista. Desmarque la casilla de verificación para anular la selección de una NIC. Para mantener una red flexible y segura, puede unir dos, tres o cuatro NIC cuando vSwitch es la pila de red. Sin embargo, solo puede unir dos NIC cuando el puente de Linux es la pila de red.
4. En el modo **Bond**, elija el tipo de vínculo:

    - Seleccione **Activo-activo** para configurar un enlace activo-activo. El tráfico se equilibra entre las NIC enlazadas. Si se produce un error en una NIC del enlace, el tráfico de red del host se enruta automáticamente a través de la segunda NIC.
    - Seleccione **Activo-pasivo** para configurar un enlace activo-pasivo. El tráfico pasa solo por una de las NIC enlazadas. En este modo, la segunda NIC solo se activa si la NIC activa falla, por ejemplo, si pierde la conectividad de red.
    - Seleccione **LACP con equilibrio de carga basado en la dirección MAC de origen** para configurar un enlace LACP. La NIC saliente se selecciona en función de la dirección MAC

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de la VM desde la que se originó el tráfico. Use esta opción para equilibrar el tráfico en un entorno en el que tenga varias máquinas virtuales en el mismo host. Esta opción no es adecuada si hay menos interfaces virtuales (VIF) que NIC: Ya que el equilibrio de carga no es óptimo porque el tráfico no se puede dividir entre NIC.

- Seleccione **LACP con equilibrio de carga basado en IP y puerto de origen y destino** para configurar un enlace LACP. La dirección IP de origen, el número de puerto de origen, la dirección IP de destino y el número de puerto de destino se utilizan para asignar el tráfico a través de las NIC. Use esta opción para equilibrar el tráfico de las máquinas virtuales en un entorno en el que la cantidad de NIC supera la cantidad de VIF.

  > **Nota:**
  >
  > La unión LACP solo está disponible para vSwitch, mientras que los modos de unión activo-activo y activo-pasivo están disponibles para el puente vSwitch y Linux. Para obtener información sobre las pilas de redes, consulte Redes.

5. Para usar tramas gigantes, establezca la Unidad de transmisión máxima (MTU) en un valor entre 1500 y 9216.
6. Para que la nueva red enlazada se agregue automáticamente a cualquier máquina virtual nueva creada con el asistente para nueva máquina virtual, seleccione la casilla de verificación.
7. Haga clic en **Crear** para crear el enlace NIC y cerrar el cuadro de diálogo.

   XenCenter mueve automáticamente las interfaces secundarias y de administración de las NIC enlazadas secundarias a la interfaz de unión cuando se crea la nueva unión. Un anfitrión con su interfaz de administración en un bono no puede unirse a un grupo. Antes de que el host pueda unirse a un grupo, debe volver a configurar la interfaz de administración y volver a moverla a una NIC física.

Configuración del almacenamiento compartido para el grupo

Para conectar los hosts de un grupo a una matriz de almacenamiento remoto, cree un XenServer SR. El RA es el contenedor de almacenamiento donde se almacenan los discos virtuales de una VM. Los SR son objetos persistentes en disco que existen de forma independiente de XenServer. Los SR pueden existir en diferentes tipos de dispositivos de almacenamiento físico, tanto internos como externos. Estos tipos incluyen dispositivos de disco local y almacenamiento en red compartido.

Puede configurar un XenServer SR para distintos tipos de almacenamiento, entre los que se incluyen:

- NFS
- iSCSI de software

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- HBA de hardware
- SMB
- Canal de fibra
- Software FCoE (obsoleto)

En esta sección se explica cómo configurar dos tipos de SR compartidos para un grupo de hosts: NFS e iSCSI. Antes de crear un SR, configure el arreglo de almacenamiento NFS o iSCSI. La configuración varía según el tipo de solución de almacenamiento que utilice. Para obtener más información, consulte la documentación del proveedor. Por lo general, antes de empezar, complete la siguiente configuración de la solución de almacenamiento:

- **SR iSCSI**: Debe haber creado un volumen y un LUN en el arreglo de almacenamiento.
- **NFS SR**: Debe haber creado el volumen en el dispositivo de almacenamiento.
- **HBA de hardware**: Debe haber realizado la configuración requerida para exponer el LUN antes de ejecutar el asistente Nuevo repositorio de almacenamiento
- **Software FCoE SR**: debe haber completado manualmente la configuración requerida para exponer un LUN al host. Esta configuración incluye la configuración de la estructura FCoE y la asignación de LUN al nombre mundial público (PWWN) de su SAN.

Si está creando un SR para almacenamiento basado en IP (iSCSI o NFS), puede configurar una de las siguientes opciones como red de almacenamiento: La NIC que administra el tráfico de administración o una NIC nueva para el tráfico de almacenamiento. Para configurar una NIC diferente para el tráfico de almacenamiento, asigne una dirección IP a una NIC mediante la creación de una *interfaz de administración*.

Al crear una interfaz de administración, debe asignarle una dirección IP que cumpla con los siguientes criterios:

- La dirección IP se encuentra en la misma subred que la controladora de almacenamiento, si corresponde
- La dirección IP se encuentra en una subred diferente a la dirección IP que especificó al instalar XenServer
- La dirección IP no se encuentra en la misma subred que cualquier otra interfaz de administración.

Para asignar una dirección IP a una NIC:

1. Asegúrese de que la NIC esté en una subred independiente o de que la redirección esté configurada para adaptarse a la topología de su red. Esta configuración fuerza el tráfico deseado a través de la NIC seleccionada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. En el panel **Recursos** de XenCenter, seleccione el grupo (o el host independiente). Haga clic en la ficha **Redes** y, a continuación, haga clic en el botón **Configurar**.
3. En el cuadro de diálogo **Configurar dirección IP**, en el panel izquierdo, haga clic en **Agregar dirección IP**.
4. Dé a la nueva interfaz un nombre significativo (por ejemplo, *yourstoragearray_network*). Seleccione la **red** asociada a la NIC que utiliza para el tráfico de almacenamiento.
5. Haga clic en **Usar esta configuración de red**. Introduzca una dirección IP estática que quiera configurar en la NIC, la máscara de subred y la puerta de enlace. Haga clic en **Aceptar**. La dirección IP debe estar en la misma subred que la controladora de almacenamiento a la que está conectada la NIC.

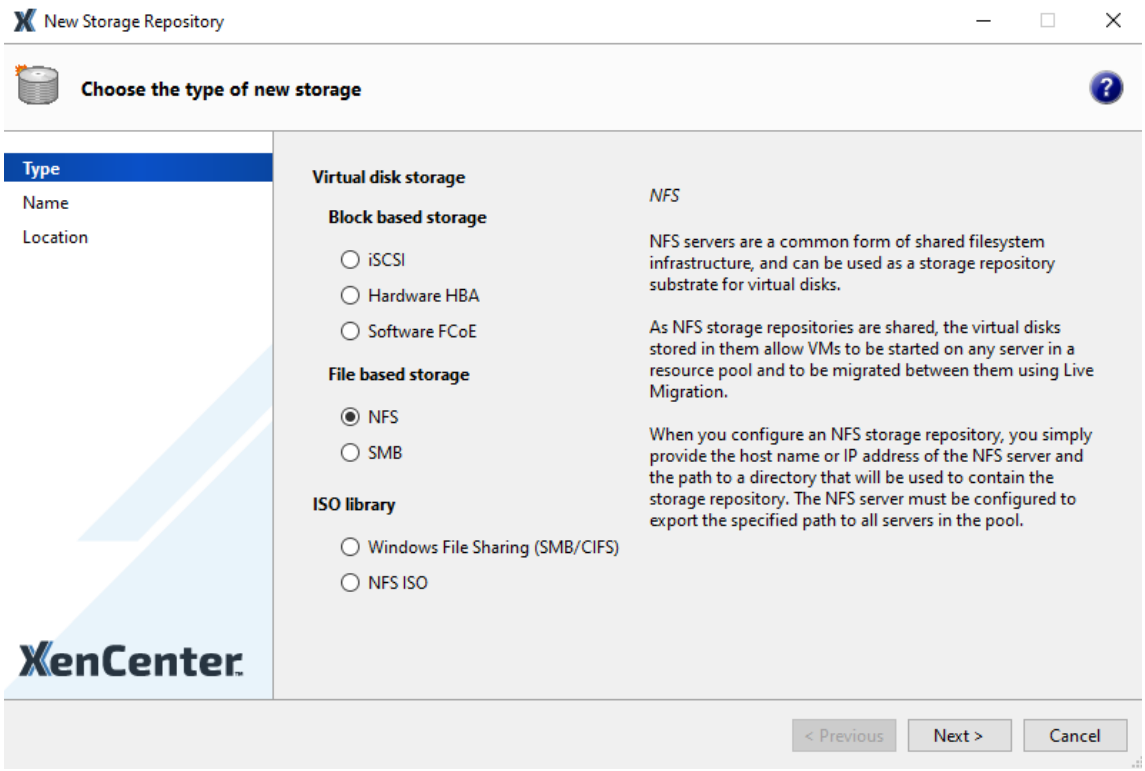
> **Nota:**
>
> Siempre que asigne una dirección IP a una NIC, debe estar en una subred diferente a la de cualquier otra NIC con direcciones IP en el grupo. Esto incluye la interfaz de administración principal.

Para crear un nuevo repositorio de almacenamiento NFS o iSCSI compartido:

1. En el panel **Recursos**, seleccione el grupo. En la barra de herramientas, haga clic en el botón **Nuevo almacenamiento**.

   Se abre el asistente **Nuevo repositorio de almacenamiento**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. En Almacenamiento en disco virtual, elija NFS o iSCSI como tipo de almacenamiento. Haga clic en Next para continuar.
3. Si elige NFS:

   a) Introduzca un nombre para la nueva SR y el nombre del recurso compartido en el que se encuentra. Haga clic en **Escanear** para que el asistente busque SR de NFS existentes en la ubicación especificada.

   > **Nota:**
   >
   > El host NFS debe configurarse para exportar la ruta especificada a todos los hosts XenServer del grupo.

   b) Haga clic en **Finalizar**.

   El nuevo RA aparece en el panel **Recursos**, dentro del grupo.

4. Si elige iSCSI:

   a) Introduzca un nombre para el nuevo SR y, a continuación, la dirección IP o el nombre DNS del destino iSCSI.

   > **Nota:**
   >
   > El destino de almacenamiento iSCSI debe configurarse para permitir que todos los

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> hosts XenServer del grupo tengan acceso a uno o más LUN.

b) Si ha configurado el destino iSCSI para que utilice la autenticación CHAP, introduzca el nombre de usuario y la contraseña.

c) Haga clic en el botón **Analizar host de destino** y, a continuación, elija el IQN de destino iSCSI de la lista IQN de destino.

> **Advertencia:**
>
> El destino iSCSI y todos los hosts del grupo deben tener IQN *únicos*.

d) Haga clic en **LUN de destino** y, a continuación, seleccione el LUN en el que quiere crear el RA en la lista LUN de destino.

> **Advertencia:**
>
> Cada repositorio de almacenamiento iSCSI individual debe estar contenido en su totalidad en un único LUN y no puede abarcar más de un LUN. Todos los datos presentes en el LUN elegido se destruyen.

e) Haga clic en **Finalizar**.

El nuevo RA aparece en el panel **Recursos**, dentro del grupo.

La nueva SR compartida ahora se convierte en la SR predeterminada para el grupo.

Creación de máquinas virtuales

A través de XenCenter, puede crear máquinas virtuales de varias maneras, de acuerdo con sus necesidades. Ya sea que implemente máquinas virtuales individuales con configuraciones distintas o grupos de varias máquinas virtuales similares, XenCenter lo pone en marcha en solo unos pocos pasos.

XenServer también proporciona una forma sencilla de convertir lotes de máquinas virtuales de VMware. Para obtener más información, consulte Conversion Manager.

Esta sección se centra en algunos métodos para crear máquinas virtuales de Windows. Para comenzar rápidamente, los procedimientos utilizan la configuración más sencilla de XenServer: un único host XenServer con almacenamiento local (después de conectar XenCenter al host XenServer, el almacenamiento se configura automáticamente en el disco local del host).

En esta sección también se muestra cómo usar la migración en vivo para migrar máquinas virtuales en vivo entre los hosts del grupo.

Después de explicar cómo crear y personalizar su nueva VM, en esta sección se demuestra cómo convertir esa VM existente en una plantilla de VM. Una plantilla de VM conserva su personalización para

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

que siempre pueda usarla para crear VM con las mismas especificaciones (o similares). También reduce el tiempo que lleva crear varias VM.

También puede crear una plantilla de VM a partir de una instantánea de una VM existente. Una instantánea es un registro de una máquina virtual en ejecución en un momento determinado. Guarda la información de almacenamiento, configuración y redes de la VM original, lo que la hace útil para realizar copias de seguridad. Las instantáneas proporcionan una forma rápida de crear plantillas de VM. En esta sección se demuestra cómo tomar una instantánea de una máquina virtual existente y, a continuación, cómo convertir esa instantánea en una plantilla de máquina virtual. Por último, en esta sección se describe cómo crear máquinas virtuales a partir de una plantilla de VM.

Lo que aprenderás

Aprenderás a:

- Crear una VM con Windows 10
- Instalación de XenServer VM Tools para Windows
- Migre una máquina virtual en ejecución entre los hosts del grupo
- Crear una plantilla de VM
- Crear una VM a partir de una plantilla de VM

Requisitos

Para crear un grupo con almacenamiento compartido, necesita los siguientes elementos:

- El grupo de XenServer que configuró
- XenCenter
- Archivos de instalación para Windows 10 VM
- Archivos de instalación de XenServer VM Tools para Windows

Crear una VM con Windows 10

> **Nota:**
>
> El siguiente procedimiento proporciona un ejemplo de cómo crear una máquina virtual con Windows 10. Los valores predeterminados pueden variar en función del sistema operativo que elija.

Para crear una VM Windows:

1. En la barra de herramientas, haga clic en el botón **Nueva VM** para abrir el asistente Nueva VM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El asistente para nueva VM le permite configurar la nueva VM, ajustando varios parámetros para la CPU, el almacenamiento y los recursos de red.

2. Seleccione una plantilla de VM y haga clic en **Siguiente**.

   Cada plantilla contiene la información de configuración para crear una VM con un sistema operativo (SO) invitado específico y con un almacenamiento óptimo. Esta lista refleja las plantillas que XenServer admite actualmente.

   > **Nota:**
   >
   > Si el sistema operativo que va a instalar en su nueva máquina virtual solo es compatible con el hardware original, marque la casilla **Copiar cadenas de BIOS del host a la máquina virtual**. Por ejemplo, use esta opción para un CD de instalación de SO que se haya empaquetado con un equipo específico.
   >
   > Después de iniciar una VM por primera vez, no puede cambiar sus cadenas de BIOS. Asegúrese de que las cadenas del BIOS sean correctas antes de iniciar la VM por primera vez.

3. Introduzca un nombre y una descripción opcional de la nueva VM.
4. Elija el origen del medio del sistema operativo que quiere instalar en la nueva máquina virtual.

   La instalación desde un CD/DVD es la opción más sencilla para empezar. Elija la opción de fuente de instalación predeterminada (unidad de DVD), inserte el disco en la unidad de DVD del host de XenServer y elija **Siguiente para continuar**.

   XenServer también le permite extraer los medios de instalación del sistema operativo de una variedad de fuentes, incluida una biblioteca ISO preexistente.

   Para adjuntar una biblioteca ISO preexistente, haga clic en **Nueva biblioteca ISO** e indique la ubicación y el tipo de biblioteca ISO. A continuación, puede elegir el medio ISO del sistema operativo específico de la lista.

5. La máquina virtual se ejecuta en el host instalado. Seleccione **Siguiente** para continuar.
6. Asigne recursos de memoria y procesador.

   Cada sistema operativo tiene requisitos de configuración diferentes que se reflejan en las plantillas. Si es necesario, puede optar por modificar los valores predeterminados. Haga clic en **Next** para continuar.

7. Asigne una unidad de procesamiento de gráficos (GPU).

   El asistente para **nueva VM** le pide que asigne una GPU dedicada o GPU virtuales a la VM. Esta opción permite que la VM utilice la potencia de procesamiento de la GPU. Proporciona un mejor soporte para aplicaciones gráficas profesionales en 3D de alta gama, como aplicaciones CAD, GIS e imágenes médicas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> La virtualización de GPU está disponible para los clientes de XenServer Premium Edition.

8. Configure el almacenamiento para la nueva VM.

   Haga clic en **Siguiente** para seleccionar la asignación y la configuración predeterminadas, o bien puede que quiera:

   a) Cambie el nombre, la descripción o el tamaño del disco virtual haciendo clic en **Modificar**.

   b) Para agregar un disco virtual nuevo, seleccione **Agregar**.

   > **Nota:**
   >
   > Al crear un grupo de hosts de XenServer, puede configurar el almacenamiento compartido en este momento al crear una máquina virtual.

9. Configure las redes en la nueva VM.

   Haga clic en **Siguiente** para seleccionar la NIC y las configuraciones predeterminadas, incluida una dirección MAC única creada automáticamente para cada NIC, o puede:

   a) Cambie la red física, la dirección MAC o la prioridad de calidad de servicio (QoS) del disco virtual haciendo clic en **Modificar**.

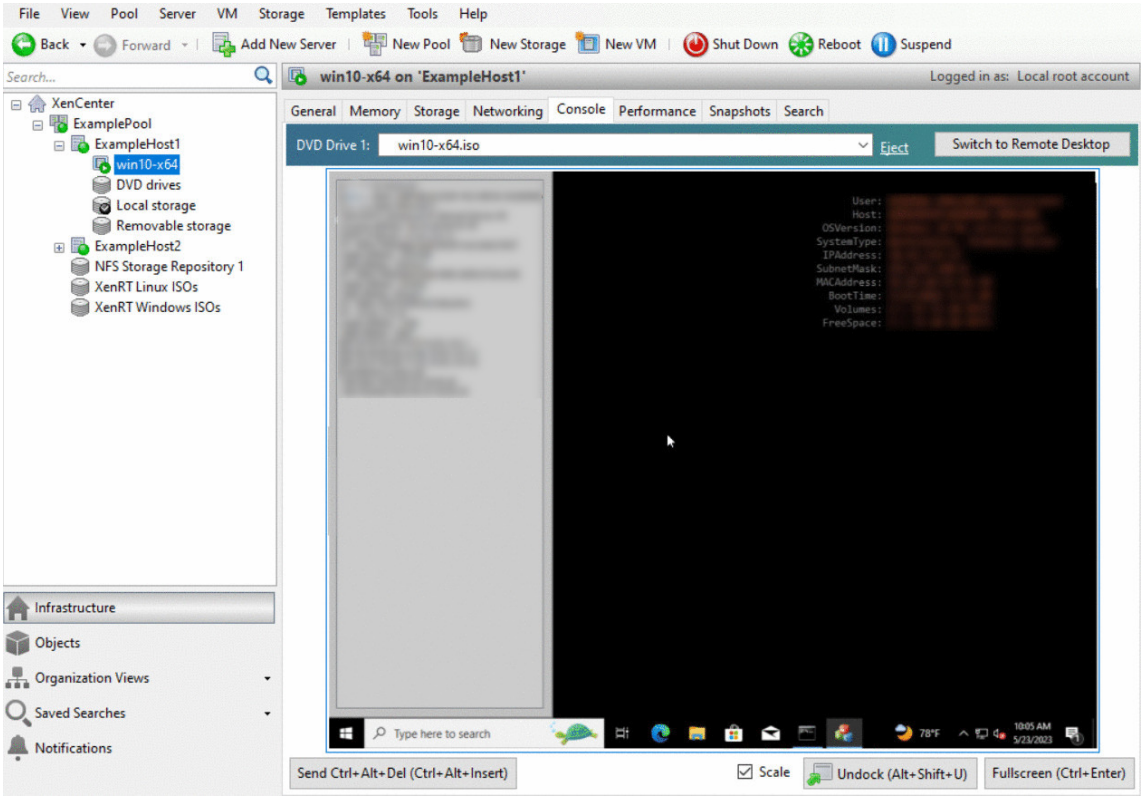
   b) Agregue una nueva interfaz de red virtual seleccionando **Agregar**.

      XenServer usa la interfaz de red virtual para conectarse a la red física del host. Asegúrese de seleccionar la red que se corresponda con la red que requiere la máquina virtual. Para agregar una red física, consulte Configuración de redes para el grupo.

10. Revise la configuración y, a continuación, haga clic en **Crear ahora** para crear la VM y volver a la ficha **Buscar**.

    Aparece un icono para la nueva VM debajo del host en el panel **Recursos**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



En el panel **Recursos**, seleccione la VM y, a continuación, haga clic en la ficha **Consola** para ver la consola de VM.

11. Siga las pantallas de instalación del sistema operativo y haga sus selecciones.
12. Una vez completada la instalación del sistema operativo y reiniciada la máquina virtual, instale XenServer VM Tools para Windows.

Instalación de XenServer VM Tools para Windows

Las herramientas de máquinas virtuales de XenServer para Windows proporcionan servicios de E/S de alto rendimiento sin la sobrecarga de la emulación de dispositivos tradicional. XenServer VM Tools para Windows consta de controladores de E/S (también conocidos como controladores paravirtualizados o controladores PV) y el agente de administración. Las herramientas de máquina virtual de XenServer para Windows deben estar instaladas en cada máquina virtual de Windows para que la máquina virtual tenga una configuración totalmente compatible. Una VM Windows funciona sin ellas, pero el rendimiento se ve obstaculizado. Las herramientas de máquinas virtuales de XenServer para Windows también permiten ciertas funciones y características, como el cierre limpio, el reinicio, la suspensión y la migración en vivo de las máquinas virtuales.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Advertencia:**
>
> Instale XenServer VM Tools para Windows para cada máquina virtual de Windows. *No se admite la ejecución de máquinas virtuales de Windows sin XenServer VM Tools para Windows.*
>
> Se recomienda realizar una instantánea de la máquina virtual antes de instalar o actualizar XenServer VM Tools.

Para instalar XenServer VM Tools para Windows:

1. Descargue el archivo XenServer VM Tools para Windows en su máquina virtual Windows. Obtenga este archivo en la página de descargas de XenServer .
2. Ejecute el `managementagentx64.msi` archivo para iniciar la instalación de XenServer VM Tools.
3. Siga las instrucciones del instalador.
4. Reinicie la VM cuando se le pida que complete el proceso de instalación.

> **Nota:**
>
> Los controladores de E/S se instalan automáticamente en una máquina virtual de Windows que puede recibir actualizaciones de Windows Update. Sin embargo, le recomendamos que instale el paquete XenServer VM Tools for Windows para instalar el agente de administración y mantener una configuración compatible. Las siguientes funciones solo están disponibles para los clientes de XenServer Premium Edition:
>
> - Posibilidad de recibir controladores de E/S de Windows Update
> - Actualización automática del agente de gestión

Una vez que haya instalado XenServer VM Tools para Windows, puede personalizar su máquina virtual instalando aplicaciones y realizando cualquier otra configuración. Si quiere crear varias VM con especificaciones similares, puede hacerlo rápidamente creando una plantilla a partir de la VM existente. Use esa plantilla para crear máquinas virtuales. Para obtener más información, consulte Creación de plantillas de VM.

Migre las máquinas virtuales en ejecución entre los hosts de un grupo

Mediante la migración en vivo, puede mover una máquina virtual en ejecución de un host a otro del mismo grupo y prácticamente sin interrupción del servicio. El lugar al que decide migrar una VM depende de cómo configure la VM y el grupo.

Para migrar una VM en ejecución:

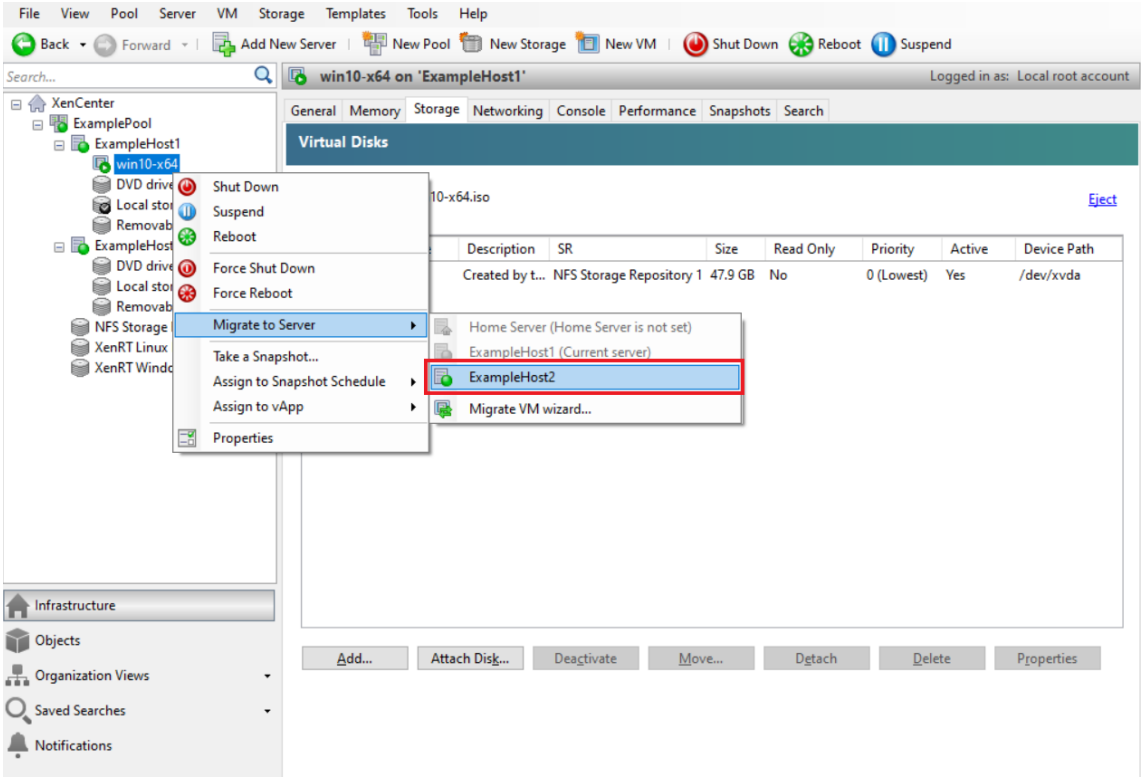
1. En el panel **Recursos**, seleccione la máquina virtual que quiere mover.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Asegúrese de que la máquina virtual que migra no tenga almacenamiento local.

2. Haga clic con el botón secundario en el icono de la máquina virtual, seleccione **Migrar al servidor**, a continuación, seleccione el nuevo host de la máquina virtual.

> **Sugerencia:**
>
> También puede arrastrar la máquina virtual al host de destino.



3. La máquina virtual migrada se muestra debajo del nuevo host en el panel **Recursos**.

Crear plantillas de VM

Hay varias formas de crear una plantilla de VM a partir de una VM de Windows existente, cada una con sus ventajas individuales. Esta sección se centra en dos métodos: convertir una VM existente en una plantilla y crear una plantilla a partir de una instantánea de una VM. En ambos casos, la plantilla de VM conserva la configuración personalizada de la VM o la instantánea de VM original. La plantilla se puede usar para crear máquinas virtuales nuevas y similares rápidamente. En esta sección se demuestra cómo crear nuevas VM a partir de estas plantillas.

Antes de crear una plantilla a partir de una instantánea de VM o VM existente, le recomendamos que ejecute la utilidad de Windows `Sysprep` en la VM original. En general, la ejecución `Sysprep` prepara

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

un sistema operativo para la clonación y restauración de discos. Las instalaciones del sistema operativo Windows incluyen muchos elementos únicos por instalación (incluidos identificadores de seguridad y nombres de equipos). Estos elementos deben seguir siendo únicos y no copiarse en máquinas virtuales nuevas. Si se copian, es probable que surjan confusión y problemas. La ejecución `Sysprep` evita estos problemas al permitir la generación de elementos nuevos y únicos para las nuevas VM.

> **Nota:**
>
> La ejecución de `Sysprep` puede no ser tan necesaria para las implementaciones básicas o los entornos de prueba como lo es para los entornos de producción.

Para obtener más información al respecto `Sysprep`, consulte la documentación de Windows. El procedimiento detallado para ejecutar esta utilidad puede variar según la versión de Windows instalada.

Crear una plantilla de VM a partir de una VM existente Para crear una plantilla de VM a partir de una VM existente:

> **Advertencia:**
>
> Cuando creas una plantilla a partir de una VM existente, la nueva plantilla reemplaza a la VM original. La VM ya no existe.

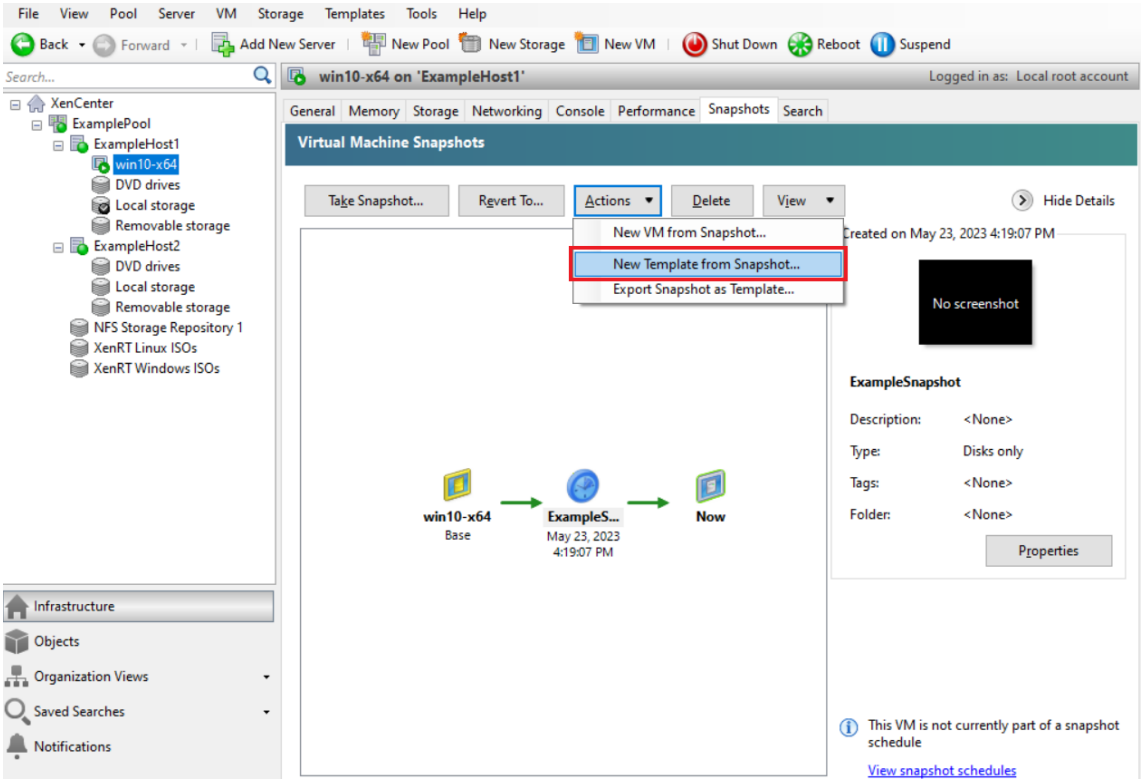
1. Apague la VM que quiere convertir.
2. En el panel **Recursos**, haga clic con el botón secundario en la máquina virtual y seleccione **Convertir en plantilla**.
3. Haga clic en **Convertir** para confirmar.

   Una vez que crea la plantilla, la nueva plantilla de VM aparece en el panel **Recursos**, en sustitución de la VM existente.

Crear una plantilla de VM a partir de una instantánea de VM Para crear una plantilla a partir de una instantánea de una VM:

1. En el panel **Recursos**, seleccione la VM. Haga clic en la ficha **Instantáneas** y, a continuación, en **Tomar instantánea**.
2. Introduzca un nombre y una descripción opcional de la nueva instantánea. Haga clic en **Tomar instantánea**.
3. Cuando finalice la instantánea y aparezca el icono en la ficha **Instantáneas**, seleccione el icono de la nueva instantánea. En la lista **Acciones**, elija **Nueva plantilla de instantánea**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Introduzca un nombre para la plantilla y, a continuación, haga clic en **Crear**.

Crear máquinas virtuales a partir de una plantilla de VM

Para crear una VM a partir de una plantilla de VM personalizada:

1. En el panel **Recursos** de XenCenter, haga clic con el botón secundario en la plantilla y seleccione Asistente para **nuevas máquinas virtuales**.

   Se abre el asistente para **máquinas virtuales nuevas**.

2. Siga el asistente para **máquinas virtuales nuevas** para crear una máquina virtual a partir de la plantilla seleccionada.

   > **Nota:**
   >
   > Cuando el asistente le pida una fuente de medios de instalación de SO, seleccione la predeterminada y continúe.

   La nueva VM aparece en el panel **Recursos**.

Si utiliza una plantilla creada a partir de una máquina virtual existente, también puede elegir seleccionar **Creación rápida**. Esta opción no lo lleva a través del asistente para **nuevas máquinas virtuales**. En su lugar, esta opción crea y aprovisiona instantáneamente una nueva VM con todos los ajustes de configuración especificados en su plantilla.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Requisitos del sistema

February 23, 2024

XenServer requiere al menos dos equipos físicos x86 independientes: uno para ser el host de XenServer y el otro para ejecutar la aplicación XenCenter o la interfaz de línea de comandos (CLI) de XenServer. El equipo host de XenServer se dedica exclusivamente a la tarea de ejecutar XenServer y alojar máquinas virtuales, y no se utiliza para otras aplicaciones.

> **Advertencia:**
>
> XenServer solo admite controladores y paquetes adicionales que proporcionemos y que se instalen directamente en el dominio de control del host. No se admiten los controladores proporcionados por sitios web de terceros, incluidos los controladores con el mismo nombre o número de versión que los que proporcionamos nosotros.
>
> Se admiten las siguientes excepciones:
>
> - Software suministrado como paquete complementario y respaldado explícitamente por nosotros.
> - Controladores que proporciona NVIDIA para habilitar la compatibilidad con vGPU. Para obtener más información, consulta NVIDIA vGPU.
>
>   Other drivers provided by NVIDIA, for example, the Mellanox drivers, are not supported with XenServer unless distributed by us.

Para ejecutar XenCenter, use cualquier sistema Windows de uso general que satisfaga los requisitos de hardware. Este sistema Windows se puede usar para ejecutar otras aplicaciones.

Al instalar XenCenter en este sistema, también se instala la CLI de XenServer. Se puede instalar una CLI de XenServer remota e independiente en cualquier distribución de Linux basada en RPM. Para obtener más información, consulte Interfaz de línea de comandos.

Requisitos del sistema host de XenServer

Aunque XenServer suele implementarse en hardware de tipo servidor, XenServer también es compatible con muchos modelos de estaciones de trabajo y portátiles. Para obtener más información, consulte la Lista de compatibilidad de hardware (HCL).

En la siguiente sección se describen las especificaciones de hardware recomendadas para XenServer.

El host XenServer debe ser una máquina de clase servidor x86 de 64 bits dedicada al alojamiento de máquinas virtuales. XenServer crea una partición Linux optimizada y reforzada con un núcleo com-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

patible con Xen. Este núcleo controla la interacción entre los dispositivos virtualizados que ven las VM y el hardware físico.

XenServer puede usar:

- Hasta 6 TB de RAM
- Hasta 16 NIC físicas
- Hasta 448 procesadores lógicos por host.

> **Nota:**
>
> La cantidad máxima de procesadores lógicos admitidos varía según la CPU. Para obtener más información, consulte la Lista de compatibilidad de hardware (HCL).

Los requisitos del sistema para el host XenServer son:

CPUs

Se recomienda una o más CPU x86 de 64 bits, 1,5 GHz como mínimo, CPU multinúcleo de 2 GHz o más rápida.

Para admitir máquinas virtuales que ejecuten Windows o versiones más recientes de Linux, necesita un sistema basado en Intel VT o AMD-V x86 de 64 bits con una o más CPU.

> **Nota:**
>
> Asegúrese de habilitar el soporte de hardware para la virtualización en el host de XenServer. La compatibilidad con la virtualización es una opción en el firmware del sistema. Es posible que su hardware tenga deshabilitada la compatibilidad con la virtualización. Para obtener más información, consulte la documentación del servidor.

Para admitir máquinas virtuales que ejecuten Linux paravirtualizado compatible, necesita un sistema estándar basado en x86 de 64 bits con una o más CPU.

RAM

2 GB como mínimo, se recomiendan 4 GB o más

Espacio en disco

- Almacenamiento con conexión local con 46 GB de espacio en disco como mínimo, se recomiendan 70 GB de espacio en disco

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- SAN a través de HBA (no a través de software) cuando se instala con arranque de múltiples rutas desde SAN.

Para obtener una lista detallada de las soluciones de almacenamiento compatibles, consulte la Lista de compatibilidad de hardware (HCL).

Red

NIC de 100 Mbit/s o más rápida. Se recomiendan NIC de 1, 10 Gb o más para transferencias de datos de exportación/importación y migración en vivo de VM más rápidas.

Le recomendamos que utilice varias NIC para obtener redundancia. La configuración de las NIC varía según el tipo de almacenamiento. Para obtener más información, consulte la documentación del proveedor.

XenServer requiere una red IPv4 para el tráfico de administración y almacenamiento.

> **Notas:**
>
> - Asegúrese de que la configuración de hora de su servidor esté establecida en la hora actual en UTC.
> - En algunos casos de soporte, se requiere acceso a la consola serie para fines de depuración. Al configurar XenServer, se recomienda configurar el acceso a la consola en serie. Para los hosts que no tienen un puerto serie físico o donde la infraestructura física adecuada no está disponible, investigue si puede configurar un dispositivo de administración integrado. Por ejemplo, DRAC de Dell. Para obtener más información sobre cómo configurar el acceso a la consola en serie, consulte CTX228930: Cómo configurar el acceso a la consola en serie en XenServer 7.0 y versiones posteriores.

requisitos del sistema de XenCenter

XenCenter tiene los siguientes requisitos del sistema:

- **Sistema operativo:**
  - Windows 10
  - Windows 11
  - Windows Server 2016
  - Windows Server 2019
- **.NET Framework:** versión 4.8
- **Velocidad de la CPU:** 750 MHz como mínimo, se recomienda 1 GHz o más rápido
- **RAM:** 1 GB como mínimo, se recomiendan 2 GB o más

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Espacio en disco:** 100 MB como mínimo
- **Red:** NIC de 100 Mbit/s o más rápida
- **Resolución de pantalla:** 1024x768 píxeles, mínimo

Si quiere que XenCenter pueda iniciar una consola SSH externa que se conecte al servidor, instale una de las siguientes aplicaciones en el sistema:

- PuTTY
- OpenSSH (instalado de forma predeterminada en algunos sistemas operativos Windows)

Para obtener más información, consulte Configurar XenCenter para usar unaconsola SSH externa.

Sistemas operativos invitados compatibles

Para obtener una lista de los sistemas operativos de VM compatibles, consulte Compatibilidad con sistemas operativos invitados.

Requisitos del grupo

Una agrupación de recursos es un agregado homogéneo o heterogéneo de uno o más hosts, hasta un máximo de 64. Antes de crear un grupo o unir un host a un grupo existente, asegúrese de que todos los hosts del grupo cumplan los siguientes requisitos.

Requisitos de hardware

Todos los servidores de un grupo de recursos de XenServer deben tener CPU ampliamente compatibles, es decir:

- El proveedor de CPU (Intel, AMD) debe ser el mismo en todas las CPU de todos los servidores.
- Todas las CPU deben tener habilitada la virtualización.

Otros requisitos

Además de los requisitos previos de hardware identificados anteriormente, existen otros requisitos previos de configuración para que un host se una a un grupo:

- Debe tener una dirección IP coherente (una dirección IP estática en el host o una concesión de DHCP estática). Este requisito también se aplica a los servidores que proporcionan almacenamiento NFS o iSCSI compartido.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- El reloj del sistema debe estar sincronizado con el coordinador del grupo (por ejemplo, a través de NTP).
- No puede ser miembro de un grupo de recursos existente.
- No puede tener máquinas virtuales en ejecución o suspendidas ni ninguna operación activa en curso en sus máquinas virtuales, como cerrar o exportar. Apague todas las máquinas virtuales del host antes de agregarlo a un grupo.
- No puede tener ningún almacenamiento compartido configurado.
- No puede tener una interfaz de administración consolidada. Vuelva a configurar la interfaz de administración y muévala a una NIC física antes de agregar el host al grupo. Una vez que el host se haya unido al grupo, puede volver a configurar la interfaz de administración.
- Debe ejecutar la misma versión de XenServer, al mismo nivel de parche, que los hosts que ya están en el grupo.
- Debe configurarse con los mismos paquetes complementarios que los hosts que ya están en el grupo. Los paquetes complementarios se utilizan para instalar software complementario en el dominio de control de XenServer, dom0. Para evitar una experiencia de usuario incoherente en un grupo, todos los hosts del grupo deben tener instalados los mismos paquetes complementarios en la misma revisión.
- Debe tener la misma licencia de XenServer que los hosts que ya están en el grupo. Puede cambiar la licencia de cualquier miembro del grupo después de unirse al grupo. El anfitrión con la licencia más baja determina las funciones disponibles para todos los miembros del grupo.

Los hosts de XenServer de los grupos de recursos pueden contener diferentes números de interfaces de red físicas y tener repositorios de almacenamiento local de distintos tamaños.

> **Nota:**
>
> Los servidores que proporcionan almacenamiento NFS o iSCSI compartido para el grupo deben tener una dirección IP estática o ser direccionables por DNS.

Piletas homogéneas

Un grupo de recursos homogéneo es un conjunto de servidores con CPU idénticas. Las CPU de un servidor que se une a un grupo de recursos homogéneo deben tener el mismo proveedor, modelo y funciones que las CPU de los servidores que ya están en el grupo.

Grupos heterogéneos

La creación de grupos heterogéneos es posible gracias al uso de tecnologías en las CPU Intel (FlexMigration) y AMD (migración extendida) que proporcionan *enmascaramiento* o *nivelación*de CPU. Estas

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

funciones permiten configurar una CPU para que *parezca* que proporciona una marca, un modelo o un conjunto de funciones diferentes a los que realmente ofrece. Estas capacidades le permiten crear grupos de hosts con diferentes CPU, pero aun así admitir migraciones en vivo de manera segura.

Para obtener información sobre la creación de grupos heterogéneos, consulte Hosts y grupos de recursos.

Límites de configuración

April 10, 2024

Utilice los siguientes límites de configuración como guía al seleccionar y configurar el entorno virtual y físico para XenServer. Los siguientes límites de configuración probados y recomendados son totalmente compatibles con XenServer.

- Límites de máquinas virtuales
- Límites de hosts de XenServer
- Límites de la agrupación de recursos

Factores como el hardware y el entorno pueden afectar a las limitaciones que se enumeran a continuación. Puede encontrar más información sobre el hardware compatible en la Lista de compatibilidad de hardware. Consulte los límites documentados de los fabricantes de hardware para asegurarse de que no supera los límites de configuración admitidos para su entorno.

Límites de máquinas virtuales (VM)

Elemento	Límite
Procesamiento	
CPU virtuales por VM (Linux)	32/64 (véase la nota 1)
CPU virtuales por VM (Windows)	32/64 (véase la nota 1)
Memoria	
RAM por VM	1,5 TiB (ver nota 2)
Almacenamiento	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Elemento	Límite
Imágenes de disco virtual (VDI) (incluido el CD-ROM) por VM	241 (véase la nota 3)
Unidades de CD-ROM virtuales por VM	1
Tamaño del disco vDisk (NFS)	2040 GiB
Tamaño del disco vDisk (LVM)	2040 GiB
Tamaño del disco virtual (GFS2)	16 TiB
Redes	
NIC virtuales por VM	7 (véase la nota 4)
Capacidad gráfica	
vGPU por VM	8
Pasado a través de GPU por VM	1
Dispositivos	
Dispositivos USB de transferencia	6

Notas:

1. Consulte la documentación del sistema operativo invitado para asegurarse de que no supera los límites admitidos. Hasta el momento, Red Hat Enterprise Linux 8 y sus derivados no admiten más de 32 vCPU. Aunque el límite es de 64, recomendamos establecerlo en 32 si es posible que sus máquinas virtuales no sean confiables o si desea evitar un posible impacto en la disponibilidad del sistema.
2. La cantidad máxima de memoria física direccionable por el sistema operativo varía. Establecer la memoria en un nivel superior al límite admitido por el sistema operativo puede provocar problemas de rendimiento en el huésped.
3. La cantidad máxima de VDI admitidos depende del sistema operativo invitado. Consulte la documentación del sistema operativo invitado para asegurarse de que no supera los límites admitidos.
4. Varios sistemas operativos invitados tienen un límite inferior, otros huéspedes requieren la instalación de XenServer VM Tools para alcanzar este límite.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Límites de hosts de XenServer

Elemento	Límite
Procesamiento	
Procesadores lógicos por host	960 (véase la nota 1)
VM simultáneas por host	1000 (véase la nota 2)
VM protegidas simultáneas por host con alta disponibilidad habilitada	500
VM de GPU virtuales por host	128 (véase la nota 3)
Memoria	
RAM por host	6 TB
Almacenamiento	
Discos vDisk activos simultáneos por host	2048 (véase la nota 4)
Repositorios de almacenamiento por host (NFS)	400
Redes	
NIC físicas por host	16
NIC físicas por enlace de red	4
NIC virtuales por host	512
VLAN por host	800
Vínculos de red por host	4
Capacidad gráfica	
GPU por host	8 (véase la nota 5)

> **Notas:**
>
> 1. La cantidad máxima de procesadores físicos lógicos admitidos varía según la CPU. Para obtener más información, consulte la Lista de compatibilidad de hardware.
> 2. La cantidad máxima de máquinas virtuales por host admitidas depende de la carga de tra-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

bajo de la máquina virtual, la carga del sistema, la configuración de la red y ciertos factores del entorno. Nos reservamos el derecho de determinar qué factores ambientales específicos afectan el límite máximo en el que puede funcionar un sistema. Para grupos más grandes (más de 32 hosts), recomendamos asignar al menos 8 GB de RAM al dominio de control (Dom0). Para los sistemas que ejecutan más de 500 máquinas virtuales o cuando se usa el acelerador PVS, se recomienda asignar al menos 16 GB de RAM al dominio de control. Para obtener información sobre la configuración de la memoria Dom0, consulte CTX134951 - Cómo configurar la memoria dom0.

3. Para vGPU NVIDIA, 128 VM aceleradas por vGPU por host con 4 tarjetas M60 (4 x 32 = 128 VM) o 2 tarjetas M10 (2 x 64 = 128 VM). Para Intel GVT-g, 7 VM por host con un tamaño de apertura de 1024 MB. Los tamaños de apertura más pequeños pueden restringir aún más la cantidad de VM GVT-g admitidas por host. Esta cifra puede cambiar. Para conocer los límites actuales admitidos, consulte la Lista de compatibilidad de hardware.
4. La cantidad de discos virtuales activos simultáneos por host también está limitada por la cantidad de SR que haya conectado al host y la cantidad de VDI conectados que se permiten para cada SR (600). Para obtener más información, consulte la entrada "VDI adjuntos por SR"en los límites del conjunto de recursos.
5. Esta cifra puede cambiar. Para conocer los límites actuales admitidos, consulte la Lista de compatibilidad de hardware.

Límites de la agrupación de recursos

Elemento	Límite
Procesamiento	
VM por grupo de recursos	2400
Hosts por grupo de recursos	64 (véase la nota 1)
Redes	
VLAN por grupo de recursos	800
Recuperación ante desastres	
Repositorios de almacenamiento de recuperación de sitios integrados por grupo de recursos	8

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Elemento	Límite
Almacenamiento	
Rutas a un LUN	16
LUNs de rutas múltiples por host	150 (véase la nota 2)
LUNs de rutas múltiples por host (utilizados por los repositorios de almacenamiento de información)	150 (véase la nota 2)
VDI por SR (NFS, SMB, EXT, XFS, GFS2)	20000
VDI por SR (LVM)	1000
VDI conectados por SR (todos los tipos)	600
Repositorios de almacenamiento por grupo (NFS)	400
Repositorios de almacenamiento por grupo (GFS2)	62
Migración en vivo de	
VDI (sin CDROM) por VM	6
Instantáneas por VM	1
Transferencias simultáneas	3
XenCenter	
Operaciones simultáneas por grupo	25

Notas:

1. Los grupos agrupados en clúster que usan almacenamiento GFS2 admiten un máximo de 16 hosts en el grupo de recursos.
2. Cuando la alta disponibilidad está habilitada, se recomienda aumentar el tiempo de espera predeterminado a al menos 120 segundos cuando hay más de 30 LUN de rutas múltiples en un host. Para obtener información sobre cómo aumentar el tiempo de espera de alta disponibilidad, consulte CTX139166: Cómo cambiar la configuración del tiempo de espera de alta disponibilidad.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

layout: doc
description: XenServer provides drivers that enable the product to support a wide range of hardware.
—

Controladores de hardware

Colaboramos con organizaciones asociadas para proporcionar controladores y soporte para una amplia gama de hardware. Para obtener más información, consulte la Lista de compatibilidad de hardware.

Para admitir este hardware, la instalación de XenServer 8 incluye controladores de terceros que han sido certificados como compatibles con XenServer. En el artículo de resumen Versiones de controladores para XenServer y Citrix Hypervisor se incluye una lista de los controladores incluidos en la instalación inicial de XenServer.

Actualizaciones de los controladores

Entregamos regularmente versiones actualizadas de estos controladores que pueden habilitar hardware nuevo o resolver problemas con el hardware existente. La mayoría de las actualizaciones de los controladores se entregan a través del mecanismo de actualizaciones. Para obtener más información, consulte Actualizar los hosts de XenServer.

Algunas actualizaciones de controladores se publican como archivos ISO del disco de controladores en el sitio web https://support.citrix.com. Estos controladores se enumeran en el artículo de resumen Versiones de controladores para XenServer y CitrixHypervisor.

Aunque distribuimos los controladores y su código fuente para que los usen nuestros clientes, el proveedor de hardware es el propietario de los archivos fuente de los controladores.

Soporte para conductores

XenServer solo admite los controladores que vienen incluidos con el producto o desde los que se descargan. https://support.citrix.com No se admiten los controladores proporcionados por sitios web de terceros, incluidos los controladores con el mismo nombre o número de versión que los controladores proporcionados por nosotros.

> **Nota:**
>
> La única excepción a esta restricción son los controladores que proporciona NVIDIA para habilitar

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> la compatibilidad con vGPU. Para obtener más información, consulta NVIDIA vGPU.
>
> Otros controladores proporcionados por NVIDIA, por ejemplo, los controladores Mellanox, solo son compatibles con XenServer cuando los distribuimos nosotros.

No descargue controladores del sitio web del proveedor de hardware, incluso si el controlador tiene el mismo número de versión que el proporcionado por XenServer. Estos controladores no son compatibles.

Para que XenServer admita un controlador, debe certificarlo con nosotros y publicarlo mediante uno de los mecanismos aprobados. Este proceso de certificación garantiza que el controlador tiene un formato necesario para poder instalarse en un entorno de XenServer y que es compatible con XenServer 8.

¿Qué pasa si el controlador que necesito no es compatible?

Si el proveedor de hardware recomienda instalar una versión específica del controlador que no está disponible en la caja o en el sitio web https://support.citrix.com, solicite al proveedor que se ponga en contacto con nosotros para certificar esta versión del controlador con XenServer.

Proporcionamos a los proveedores kits de certificación que pueden utilizar para probar las versiones actualizadas de sus controladores que requieren la base de clientes compartida de Citrix Hypervisor y el proveedor de hardware. Una vez que el proveedor nos proporciona los resultados de las pruebas de certificación, validamos que esos resultados no muestren problemas ni regresiones en la versión actualizada del controlador. La versión del controlador ahora está certificada con XenServer y publicamos el controlador en nuestras actualizaciones periódicas o como una ISO del disco del controlador. https://support.citrix.com

Para obtener más información sobre el proceso de certificación que debe seguir el proveedor, consulte el artículo Explicación de la lista de compatibilidad de hardware.

---

layout: doc
description: Learn which VM operating systems are supported on XenServer and how much memory and disk space each operating system requires.—

Compatibilidad con sistemas operativos invitados

Al instalar máquinas virtuales y asignar recursos, como memoria y espacio en disco, siga las pautas del sistema operativo y de cualquier aplicación relevante.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sistema operativo	RAM mínima	RAM máxima	Espacio mínimo en disco
Windows 10 (64 bits)	2 GB	1.5 TB	32 GB (se recomiendan 40 GB o más)
Windows 11 (64 bits)	4 GB	1.5 TB	32 GB (se recomiendan 40 GB o más)
Windows Server 2016, Windows Server Core 2016 (64 bits)	1 GB	1.5 TB	32 GB (se recomiendan 40 GB o más)
Windows Server 2019, Windows Server Core 2019 (64 bits)	1 GB	1.5 TB	32 GB (se recomiendan 40 GB o más)
Windows Server 2022, Windows Server Core 2022 (64 bits)	1 GB	1.5 TB	32 GB (se recomiendan 40 GB o más)
CentOS 7 (64 bits)	2 GB	1.5 TB	10 GB
CentOS Stream 9 (64 bits) (versión preliminar) (consulte la nota 1)	2 GB	1.5 TB	10 GB
Red Hat Enterprise Linux 7 (64 bits)	2 GB	1.5 TB	10 GB
Red Hat Enterprise Linux 8 (64 bits)	2 GB	1.5 TB	10 GB
Red Hat Enterprise Linux 9 (64 bits) (versión preliminar) (consulte la nota 1)	2 GB	1.5 TB	10 GB
SUSE Linux Enterprise Server 12 SP5 (64 bits)	1 GB	1.5 TB	8 GB
SUSE Linux Enterprise Server 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP5 (64 bits)	1 GB	1.5 TB	8 GB
SUSE Linux Enterprise Desktop 15 SP4, 15 SP5 (64 bits)	1 GB	1.5 TB	8 GB
Oracle Linux 7 (64 bits)	2 GB	1.5 TB	10 GB

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sistema operativo	RAM mínima	RAM máxima	Espacio mínimo en disco
Oracle Linux 8 (64 bits)	2 GB	1.5 TB	10 GB
Scientific Linux 7 (64 bits)	2 GB	1.5 TB	10 GB
Debian Buster 10 (64 bits)	512 MB	1.5 TB	10 GB
Debian Bullseye 11 (64 bits)	512 MB	1.5 TB	10 GB
Debian Bookworm 12 (64 bits) (versión preliminar) (ver nota 1)	1 GB	1.5 TB	10 GB
Ubuntu 20.04 (64 bits)	512 MB	1.5 TB	10 GB
Ubuntu 22.04 (64 bits)	1 GB	1.5 TB	10 GB
Servidor avanzado NeoKylin Linux 7.2 (64 bits)	1 GB	1.5 TB	10 GB
Gooroom 2 (64 bits)	1 GB	1.5 TB	10 GB
Rocky Linux 8 (64 bits)	1 GB	1.5 TB	10 GB
Rocky Linux 9 (64 bits) (versión preliminar) (consulte la nota 1)	2 GB	1.5 TB	15 GB

> **Nota:**
>
> 1. Los clientes que quieran utilizar este sistema operativo invitado también deben instalar XenServer VM Tools for Linux v8.3.1-1 o posterior, que se puede descargar desde la página de descargas de productos de XenServer.

- XenServer VM Tools para Linux solo es compatible con los sistemas operativos invitados Linux mencionados anteriormente.
- Todos los sistemas operativos compatibles se ejecutan en modo HVM.
- Las versiones individuales de los sistemas operativos también pueden imponer sus propios límites máximos a la cantidad de memoria admitida (por ejemplo, por motivos de licencia).
- Al configurar la memoria de invitado, no exceda la cantidad máxima de memoria física que su sistema operativo puede abordar. Establecer un máximo de memoria que sea mayor que

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

el límite admitido por el sistema operativo puede provocar problemas de estabilidad en el huésped.

- Para crear una máquina virtual de una versión secundaria de RHEL más reciente que la que se indica en la tabla anterior, utilice el siguiente método:
  - Instale la VM desde los medios compatibles más recientes para la versión principal
  - Use `yum update` para actualizar la VM a la versión secundaria más reciente

  Este enfoque también se aplica a los sistemas operativos basados en RHEL, como CentOS y Oracle Linux.
- XenServer admite todos los SKU (ediciones) de las versiones de Windows enumeradas.

Soporte a huéspedes a largo

XenServer incluye una directiva de soporte de invitados a largo plazo (LTS) para máquinas virtuales Linux. La directiva LTS le permite consumir actualizaciones de versiones secundarias mediante uno de los siguientes métodos:

- Instalación desde un nuevo medio invitado
- Actualización de un invitado admitido existente

Sistemas operativos fuera de soporte

La lista de sistemas operativos invitados compatibles puede contener sistemas operativos compatibles con sus proveedores en el momento en que se lanzó esta versión de XenServer, pero que ahora ya no son compatibles con sus proveedores.

Ya no ofrecemos soporte para estos sistemas operativos (aunque sigan apareciendo en la tabla de invitados compatibles o sus plantillas sigan disponibles en los hosts de XenServer). Al intentar abordar y resolver un problema denunciado, evaluamos si el problema está directamente relacionado con un sistema operativo fuera de soporte en una máquina virtual. Para ayudarlo a tomar esa decisión, es posible que le pidamos que intente reproducir un problema con una versión compatible del sistema operativo invitado. Si el problema parece estar relacionado con un sistema operativo que no es compatible, no investigaremos el problema más a fondo.

> **Nota:**
>
> XenServer admite las versiones de Windows compatibles con Microsoft como parte de una rama LTSB.
> XenServer no admite las versiones de Windows que no son compatibles, pero que forman parte de un acuerdo de actualizaciones de seguridad ampliadas (ESU).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

layout: doc
description: If your XenServer traffic traverses network components such as firewalls or proxy servers, open these ports to ensure communication flow.—

Requisitos de conectividad

Este artículo proporciona una descripción general de los dominios y los puertos comunes que utilizan los componentes de XenServer y que deben considerarse como parte de la arquitectura de red, especialmente si el tráfico de comunicación atraviesa componentes de la red, como firewalls o servidores proxy, donde se deben abrir los puertos o se deben agregar dominios a una lista de permitidos para garantizar el flujo de comunicación.

Dominios externos a los que acceden los componentes del producto XenServer

Según la implementación y los requisitos, configure el firewall para permitir que estos componentes de XenServer accedan a los dominios de la lista.

Hosts XenServer

Sus hosts de XenServer acceden a los siguientes dominios:

Dominio	Puerto	Dirección	Detalles
`repo.ops.xenserver.com`	443	Saliente	El coordinador del grupo de XenServer descarga las actualizaciones disponibles para XenServer 8 desde esta ubicación. Para obtener más información, consulte Actualizaciones.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Dominio	Puerto	Dirección	Detalles
repo-src.ops.xenserver.com	443	Saliente	El coordinador de grupos de XenServer descarga los archivos fuente de las actualizaciones de XenServer 8 desde esta ubicación. Para obtener más información, consulte Actualizaciones.
telemetry.ops.xenserver.com	443	Saliente	El coordinador de grupos de XenServer recopila datos de telemetría y los carga con regularidad en esta ubicación. Para obtener más información, consulte Telemetría .

Al configurar los grupos de XenServer para recibir actualizaciones, puede configurar un servidor proxy para que el coordinador del grupo lo utilice para descargar las actualizaciones. Para obtener más información, consulte Configurar las actualizaciones para su grupo .

XenCenter

La consola de administración de XenCenter accede a los siguientes dominios:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Dominio	Puerto	Dirección	Detalles
`updates.ops.xenserver.com`	443	Saliente	XenCenter sondea la información de este sitio para ver si hay actualizaciones disponibles para los hosts de XenCenter y XenServer 8. Para obtener más información, consulte Actualizar los hosts de XenServer
`citrix.com` y subdominios	443	Saliente	Si usa XenCenter para administrar los hosts y el grupo de la actualización acumulativa 1 de Citrix Hypervisor 8.2, XenCenter accede a los subdominios del `citrix.com`dominio para recibir notificaciones y descargar revisiones. Para obtener más información, consulte Actualizar los hosts de Citrix Hypervisor

Puede configurar un servidor proxy por el que pasa XenCenter para comprobar si hay actualizaciones y descargarlas. Para obtener más información, consulte Servidor proxy.

VM de Windows

Si ha configurado las máquinas virtuales de Windows para recibir actualizaciones del agente de administración de XenServer VM Tools, la máquina virtual de Windows accede a los siguientes dominios:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Dominio	Puerto	Dirección	Detalles
pvupdates.vmd.citrix.com	443	Saliente	Las herramientas de máquina virtual de XenServer para Windows consultan la información de este sitio para ver si hay actualizaciones disponibles para el agente de administración.
downloadns.citrix.com.edgesuite.net	443	Saliente	Las herramientas de máquina virtual de XenServer para Windows descargan los archivos de instalación del agente de administración desde esta ubicación.

Si no desea que su máquina virtual Windows acceda a estos dominios, puede redirigir las actualizaciones del agente de administración a un servidor web interno. Para obtener más información, consulte Redirigir las actualizaciones del agente de administración .

Puertos de comunicación utilizados por los componentes del producto XenServer

Los puertos que se muestran en la tabla siguiente son los puertos comunes que utilizan los componentes de XenServer. No todos los puertos deben estar abiertos, dependiendo de la implementación y los requisitos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Origen	Destino	Tipo	Puerto	Detalles
Hosts XenServer	Hosts XenServer	TCP	80, 443	Comunicación dentro del host entre los miembros de un grupo de recursos mediante la API de administración
	Citrix License Server	TCP	27000	Gestiona la conexión inicial para las solicitudes de licencia
		TCP	7279	Entrada/salida de licencias
	Servicio NTP	TCP, UDP	123	Sincronización de tiempo
	Servicio de DNS	TCP, UDP	53	Búsquedas de DNS
	Controlador de dominio	TCP, UDP	389	LDAP (para autenticación de usuarios de Active Directory)
		TCP	636	LDAP sobre SSL (LDAPS)
	FileServer (con almacenamiento SMB)	TCP, UDP	139	ISOStore:NetBIOSSessionServi
		TCP, UDP	445	ISOStore:Microsoft-DS
	Controlador SAN	TCP	3260	Almacenamiento iSCSI
	Servidor principal y de archivos del NAS	TCP	2049	Almacenamiento NFSv4

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Origen	Destino	Tipo	Puerto	Detalles
		TCP, UDP	2049	Almacenamiento NFSv3. TCP es el predeterminado
		TCP, UDP	111	Almacenamiento NFSv3: conexión a rpcbind
		TCP, UDP	Dinámico	Almacenamiento NFSv3: un conjunto dinámico de puertos elegidos por el archivador
	Syslog	UDP	514	Envía datos a una ubicación central para intercalación
	Agrupar en clústeres	TCP	8892, 8896, 21064	Comunicación entre todos los miembros del grupo en una piscina agrupada
		UDP	5404, 5405	
XenCenter	Hosts XenServer	TCP	22	SSH
		TCP	443	Gestión mediante la API de gestión
	Máquina virtual	TCP	5900	VNC para máquinas virtuales Linux
		TCP	3389	RDP para máquinas virtuales Windows

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Origen	Destino	Tipo	Puerto	Detalles
Dispositivo virtual Equilibrio de carga	Hosts XenServer	TCP	8012	De forma predeterminada, el servidor de Workload Balancing usa 8012. Sin embargo, si especifica un puerto diferente durante la configuración del equilibrio de carga de trabajo, asegúrese de que la comunicación esté permitida en ese puerto.
Otros clientes	Hosts XenServer	TCP	80, 443	Cualquier cliente que utilice la API de administración para comunicarse con los hosts de XenServer

XenServer interactúa con varios productos Citrix. Para obtener más información sobre los puertos que utilizan estos productos, consulte Puertos de comunicación utilizados por Citrix .

> **Nota:**
>
> - Para mejorar la seguridad, puede cerrar el puerto TCP 80 en la interfaz de administración de los hosts de XenServer. Para obtener más información acerca de cómo cerrar el puerto 80, consulte Restringir el uso del puerto 80.
> - Si se usa FQDN en lugar de IP como recurso, asegúrese de que se pueda resolver.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Integración con Active Directory

Si usa Active Directory en su entorno, asegúrese de que los siguientes puertos de firewall estén abiertos para que el tráfico saliente de XenServer acceda a los controladores de dominio.

Puerto	Protocolo	Uso
53	UDP/TCP	DNS
88	UDP/TCP	Kerberos 5
123	UDP	NTP
137	UDP	Servicio de nombres NetBIOS
139	TCP	Sesión NetBIOS (SMB)
389	UDP/TCP	LDAP
445	TCP	SMB a través de TCP
464	UDP/TCP	Cambios de contraseña de máquinas
636	UDP/TCP	LDAP por SSL
3268	TCP	Búsqueda en el catálogo global

Para obtener más información, consulte Integración con Active Directory

Citrix Provisioning Services

Si usa Citrix Provisioning Services en su entorno, asegúrese de que se pueda acceder a los siguientes puertos de firewall:

Puerto	Protocolo	Uso
6901, 6902, 6905	UDP	Comunicación saliente del servidor de aprovisionamiento (paquetes destinados al dispositivo de destino)
6910	UDP	Inicio de sesión del dispositivo de destino con Citrix Provisioning Services

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puerto	Protocolo	Uso
6901	UDP	Puerto de dispositivo de destino configurable. El valor predeterminado es el puerto 6901.
6910–6930	UDP	Intervalo de puertos de servidor configurable. El rango predeterminado es 6910—6930.

Para obtener más información, consulte Citrix Provisioning Services y puertos de comunicación utilizados por Citrix.

---

layout: doc
description: Learn more about XenServer (formerly Citrix Hypervisor) concepts, components, and features.—

Información técnica general

XenServer (anteriormente conocido como Citrix Hypervisor) es una plataforma líder del sector para infraestructuras rentables de virtualización de escritorios, servidores y nubes. XenServer permite a las organizaciones de cualquier tamaño o tipo consolidar y transformar los recursos informáticos en cargas de trabajo virtuales para los requisitos actuales de los centros de datos. Mientras tanto, garantiza un camino sin fisuras para trasladar las cargas de trabajo a la nube.

Las principales funciones de XenServer son:

- Consolidación de varias máquinas virtuales (VM) en un servidor físico
- Reducir la cantidad de imágenes de disco separadas que se administrarán
- Permite una fácil integración con las infraestructuras de almacenamiento y redes existentes
- Le permite programar un mantenimiento sin tiempo de inactividad mediante la migración en vivo de máquinas virtuales entre hosts de XenServer
- Garantizar la disponibilidad de las máquinas virtuales mediante el uso de la alta disponibilidad para configurar directivas que reinicien las máquinas virtuales en otro host en caso de que se produzca un error
- Aumento de la portabilidad de las imágenes de VM, ya que una imagen de VM funciona en una variedad de infraestructuras de implementación

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

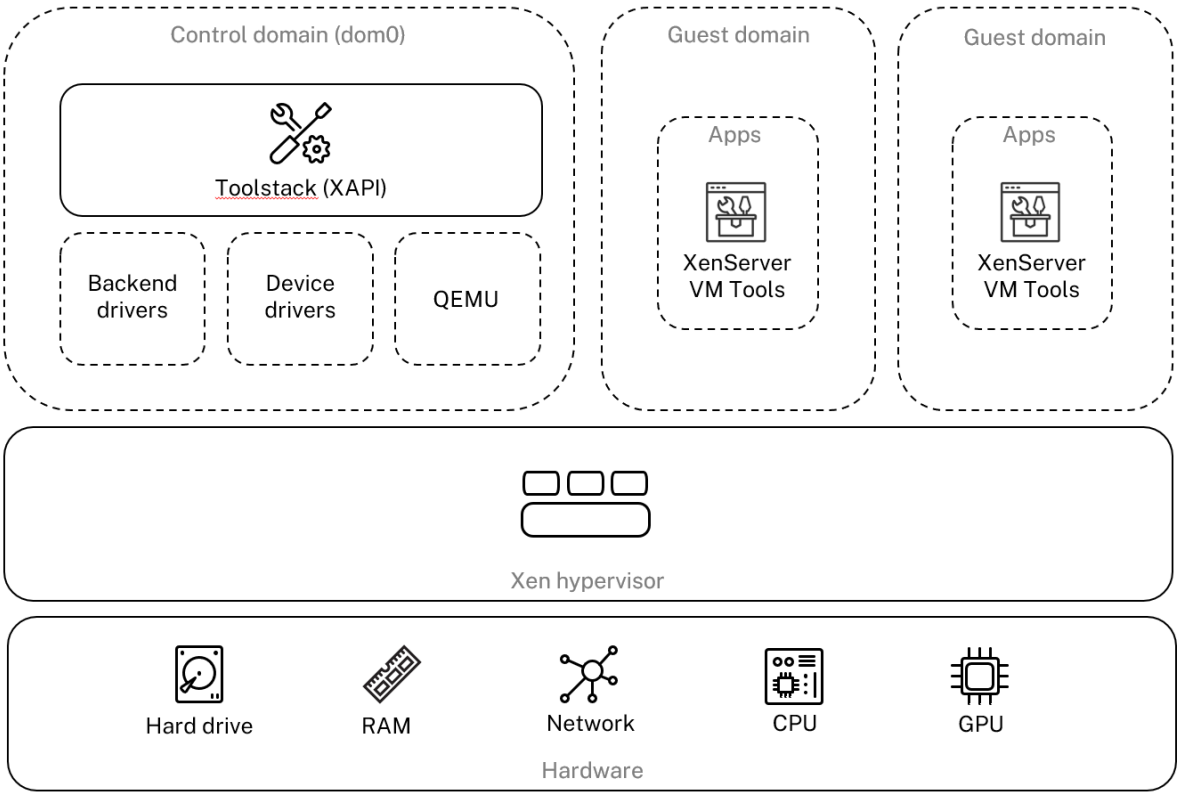
Virtualización e hipervisor

La virtualización, o para ser más específicos, la virtualización de hardware, es un método para ejecutar varias VM independientes en un solo equipo físico. El software que se ejecuta en estas máquinas virtuales está separado de los recursos de hardware subyacentes. Es una forma de utilizar por completo los recursos físicos disponibles en los servidores modernos y potentes, lo que reduce el coste total de propiedad (TCO) de las implementaciones de servidores.

Un hipervisor es la capa básica de abstracción del software. El hipervisor realiza tareas de bajo nivel, como la programación de la CPU, y es responsable del aislamiento de la memoria de las máquinas virtuales residentes. El hipervisor extrae el hardware de las máquinas virtuales. El hipervisor no tiene conocimiento de redes, dispositivos de almacenamiento externos, vídeo, etc.

Componentes principales

En esta sección, se proporciona información detallada sobre el funcionamiento de XenServer. Consulte la siguiente ilustración para ver los componentes clave de XenServer:



Architecture overview

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hardware

La capa de hardware contiene los componentes del servidor físico, como la CPU, la memoria, la red y las unidades de disco.

Necesita un sistema basado en Intel VT o AMD-V x86 de 64 bits con una o más CPU para ejecutar todos los sistemas operativos invitados compatibles. Para obtener más información sobre los requisitos del sistema host de XenServer, consulte Requisitos del sistema.
Para obtener una lista completa del hardware y los sistemas certificados por XenServer, consulte la Lista de compatibilidad de hardware (HCL).

Hipervisor Xen

El hipervisor Xen Project es un hipervisor tipo 1 o bare metal de código abierto. Permite que muchas instancias de un sistema operativo o sistemas operativos diferentes se ejecuten en paralelo en una sola máquina (o host). El hipervisor Xen se utiliza como base para muchas aplicaciones comerciales y de código abierto diferentes, como: virtualización de servidores, infraestructura como servicio (IaaS), virtualización de escritorios, aplicaciones de seguridad, dispositivos integrados y de hardware.

XenServer se basa en el hipervisor del Proyecto Xen y, además, ofrecemos funciones y soporte adicionales. XenServer usa la versión 4.13.4 del hipervisor Xen.

Dominio de control

El **dominio de control**, también denominado dominio 0 o dom0, es una máquina virtual Linux segura y privilegiada que ejecuta el conjunto de herramientas de administración de XenServer conocido como XAPI. Esta máquina virtual Linux se basa en una distribución CentOS 7.5. Además de proporcionar funciones de administración de XenServer, dom0 también ejecuta los controladores de dispositivos físicos para redes, almacenamiento, etc. El dominio de control puede comunicarse con el hipervisor para indicarle que inicie o detenga las máquinas virtuales invitadas.

Toolstack **Toolstack** o XAPI es la pila de software que controla las operaciones del ciclo de vida de las VM, las redes de host y VM, el almacenamiento de VM y la autenticación de usuarios. También permite la administración de grupos de recursos de XenServer.
XAPI proporciona la API de administración documentada públicamente, que utilizan todas las herramientas que administran máquinas virtuales y grupos de recursos. Para obtener más información, consulte la API de administración de XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Dominio invitado (VM)

Los dominios invitados son máquinas virtuales creadas por el usuario que solicitan recursos de dom0. Para obtener una lista detallada de las distribuciones compatibles, consulte Invitados compatibles, memoria virtual y límites de tamaño de disco.

Virtualización completa La virtualización completa o la virtualización asistida por hardware utiliza extensiones de virtualización de la CPU del host para virtualizar a los huéspedes. Los huéspedes totalmente virtualizados no requieren soporte para el núcleo. El invitado se denomina máquina virtual de hardware (HVM). HVM requiere extensiones de hardware Intel VT o AMD-V para la memoria y las operaciones privilegiadas. XenServer usa Quick Emulator (QEMU) para emular el hardware del PC, como la BIOS, la controladora de disco IDE, el adaptador de gráficos VGA, la controladora USB, el adaptador de red, etc. Para mejorar el rendimiento de las operaciones sensibles al hardware, como el acceso al disco o a la red, los huéspedes HVM se instalan con las herramientas de XenServer. Para obtener más información, consulte PV en HVM.

La HVM se usa comúnmente cuando se virtualiza un sistema operativo como Microsoft Windows, donde es imposible modificar el kernel para hacerlo consciente de la virtualización.

PV en HVM La PV on HVM es una mezcla de paravirtualización y virtualización de hardware completa. El objetivo principal es aumentar el rendimiento de los huéspedes de HVM mediante el uso de controladores paravirtualizados especialmente optimizados. Este modo le permite aprovechar las tecnologías de contenedores virtuales x86 en los procesadores más nuevos para mejorar el rendimiento. El acceso a la red y al almacenamiento desde estos huéspedes sigue funcionando en modo fotovoltaico, mediante controladores integrados en los núcleos.

Las distribuciones de Windows y Linux están disponibles en modo PV on HVM en XenServer. Para obtener una lista de las distribuciones compatibles que utilizan PV en HVM, consulte Compatibilidad con sistemas operativos invitados.

Herramientas de máquinas virtuales de XenServer XenServer VM Tools (anteriormente Citrix VM Tools o XenServer PV Tools) proporciona servicios de E/S de alto rendimiento sin la sobrecarga de la emulación de dispositivos tradicional.

- XenServer VM Tools para Windows consta de controladores de E/S (también conocidos como controladores paravirtualizados o controladores PV) y el agente de administración.

  Los controladores de E/S contienen controladores de red y almacenamiento front-end e interfaces de administración de bajo nivel. Estos controladores sustituyen a los dispositivos emulados y proporcionan un transporte de alta velocidad entre las máquinas virtuales y el software de la familia de productos XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El agente de administración, también conocido como agente invitado, es responsable de las funciones de administración de máquinas virtuales de alto nivel. Proporciona funcionalidad completa a XenCenter (para máquinas virtuales de Windows).

Las herramientas de máquina virtual de XenServer para Windows deben estar instaladas en cada máquina virtual de Windows para que la máquina virtual tenga una configuración totalmente compatible. Una máquina virtual funciona sin las herramientas de máquina virtual de XenServer para Windows, pero el rendimiento se verá considerablemente afectado si los controladores de E/S (controladores PV) no están instalados.

- Las herramientas de máquinas virtuales de XenServer para Linux contienen un agente invitado que proporciona información adicional sobre la máquina virtual al host. Instale el agente invitado en cada máquina virtual Linux para habilitar el control de memoria dinámica (DMC).

> **Nota:**
>
> No puede usar la función de control dinámico de memoria (DMC) en las máquinas virtuales Red Hat Enterprise Linux 8, Red Hat Enterprise Linux 9, Rocky Linux 8, Rocky Linux 9 o CentOS Stream 9, ya que estos sistemas operativos no admiten la expansión de memoria con el hipervisor Xen.

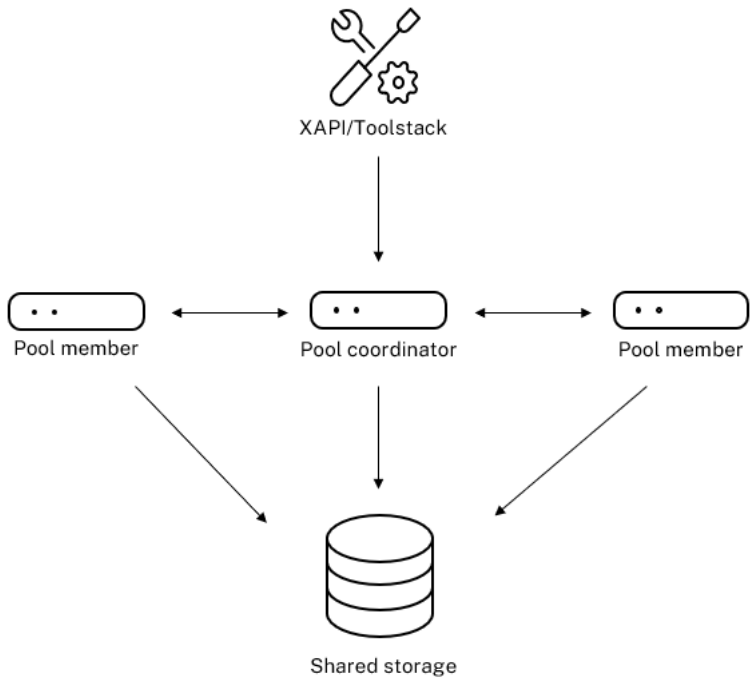
Para obtener más información, consulte XenServer VM Tools.

Conceptos clave

Grupo de recursos

XenServer le permite administrar varios hosts y su almacenamiento compartido conectado como una sola entidad mediante grupos de recursos. Los grupos de recursos le permiten mover y ejecutar máquinas virtuales en diferentes hosts de XenServer. También permiten que todos los hosts compartan un marco común de red y almacenamiento. Un grupo puede contener hasta 64 hosts que ejecuten la misma versión del software XenServer, con el mismo nivel de parche y con hardware ampliamente compatible. Para obtener más información, consulte Hosts y grupos de recursos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



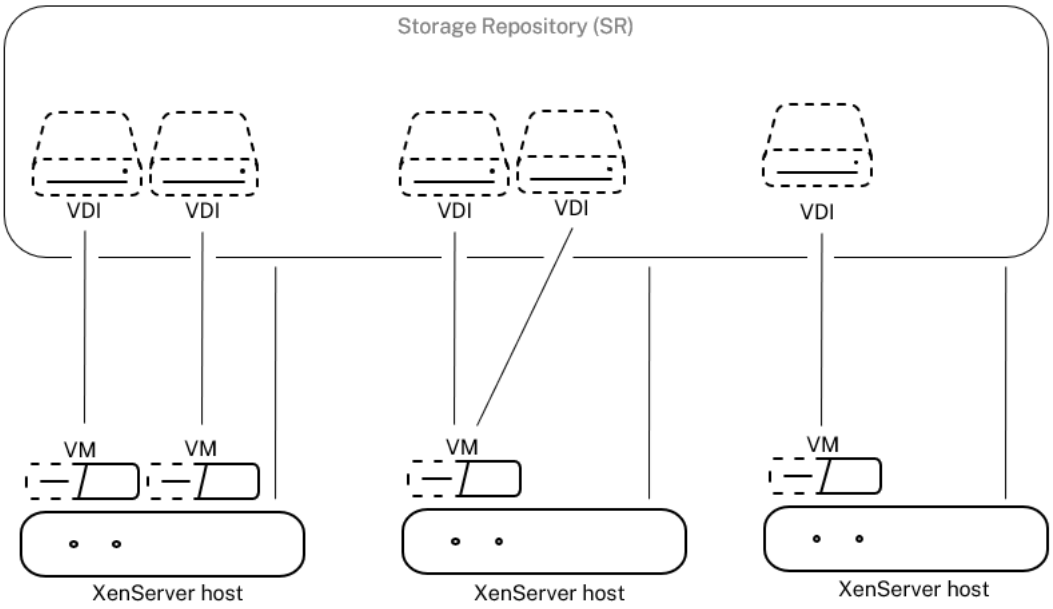
Resource pool overview

El grupo de recursos de XenServer adopta una arquitectura primaria/secundaria, implementada por XAPI. Las llamadas XAPI se reenvían del coordinador del grupo (el principal) a los miembros del grupo (los secundarios). Los miembros del grupo hacen RPC de base de datos contra el coordinador del grupo. El coordinador de la agrupación es responsable de coordinar y bloquear los recursos dentro de la agrupación, y procesa todas las operaciones de control. Los miembros del grupo hablan con el coordinador del grupo a través de HTTP y XMLRPC, pero pueden comunicarse entre sí (a través del mismo canal) a través de discos espejo (migración de almacenamiento)

Repositorio de almacenamiento

Los destinos de almacenamiento de XenServer se denominan repositorios de almacenamiento (SR). Un repositorio de almacenamiento almacena imágenes de disco vDisk (VDI), que contiene el contenido de un disco vDisk.
Los SR son flexibles, con soporte integrado para unidades SATA, SCSI, NVMe y SAS que están conectadas localmente, e iSCSI, NFS, SAS, SMB y Fibre Channel conectados de forma remota. Las abstracciones de SR y VDI permiten que las funciones de almacenamiento avanzadas, como el aprovisionamiento controlado, las instantáneas de VDI y la clonación rápida, se expongan en los destinos de almacenamiento que las admiten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Storage overview

Cada host de XenServer puede usar varios SR y diferentes tipos de SR simultáneamente. Estos SR pueden compartirse entre hosts o dedicarse a hosts particulares. El almacenamiento compartido se agrupa entre varios hosts dentro de un grupo de recursos definido. Un SR compartido debe ser accesible en red para cada host del grupo. Todos los hosts de un único grupo de recursos deben tener al menos un SR compartido. El almacenamiento compartido no se puede compartir entre varios grupos.

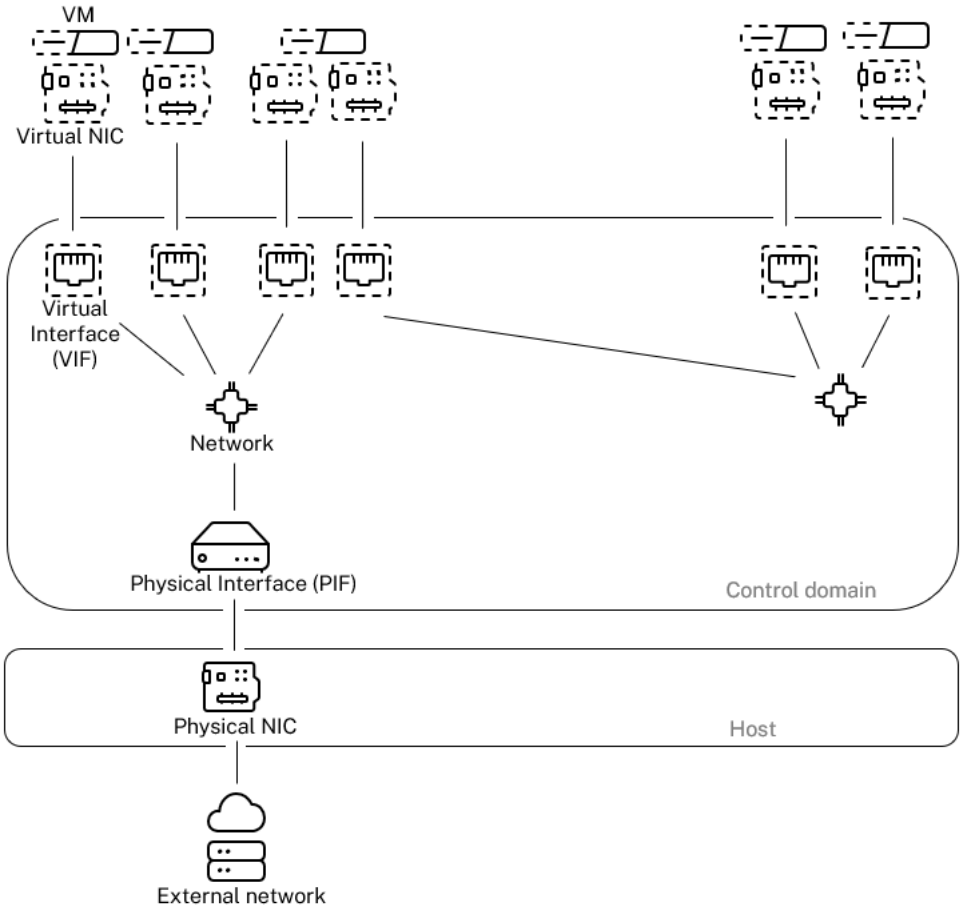
Para obtener más información sobre cómo operar con SR, consulte Configurar el almacenamiento.

Redes

A nivel de arquitectura, hay tres tipos de objetos de software del lado del servidor para representar entidades de red. Estos objetos son:

- Un **PIF**, que es un objeto de software utilizado en dom0 y representa una NIC física en un servidor. Los objetos PIF tienen un nombre y una descripción, un UUID, los parámetros de la NIC que representan y la red y el host a los que están conectados.
- Un **VIF**, que es un objeto de software utilizado en dom0 y representa una NIC virtual en una máquina virtual. Los objetos VIF tienen un nombre y una descripción, un UUID y la red y la VM a las que están conectados.
- Una **red**, que es un conmutador Ethernet virtual en un host que se utiliza para redirigir el tráfico de red en un host de red. Los objetos de red tienen un nombre y una descripción, un UUID y la colección de VIF y PIF conectados a ellos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Networking overview

Las API de administración de XenServer permiten las siguientes operaciones:

- Configuración de las opciones de red
- Control sobre la NIC que se utilizará para las operaciones de administración
- Creación de funciones de red avanzadas, como VLAN y vínculos NIC

Para obtener más información sobre cómo administrar redes en XenServer, consulte Redes.

Complementos y aplicaciones relacionados

Si bien Xen Hypervisor funciona a nivel básico, hay complementos específicos de XenServer, aplicaciones y servicios independientes del hipervisor disponibles para completar la experiencia de virtualización.

- **XenCenter**

  Un cliente GUI de Windows para la administración de VM, implementado en función de la API de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

administración. XenCenter ofrece una rica experiencia de usuario para administrar varios hosts XenServer
, grupos de recursos y toda la infraestructura virtual asociada a ellos.

- **Balance de carga de trabajo (WLB)**

  Un dispositivo que equilibra el grupo reubicando las máquinas virtuales en los mejores hosts posibles para su carga de trabajo en un grupo de recursos. Para obtener más información, consulte Equilibrio de carga de trabajo (/en-us/xenserver/8/wlb.html).

- **Servidor de licencias de Citrix**

  Un dispositivo basado en Linux con el que XenCenter contacta para solicitar una licencia para el servidor especificado.

- **XenServer Conversion Manager**

  Un dispositivo virtual que permite a los usuarios convertir las máquinas virtuales VMware existentes en máquinas virtuales de XenServer, con una conectividad de red y almacenamiento comparable. Para obtener más información, consulte Administrador de conversiones.

- **Citrix Provisioning**

  Provisioning Services que admiten el arranque PXE desde imágenes comunes. Se utiliza ampliamente con Citrix Virtual Desktops y Citrix Virtual Apps. Para obtener más información, consulte Aprovisionamiento.

- **Citrix Virtual Desktops**

  Un producto de infraestructura de escritorio virtual (VDI) especializado en escritorios Windows. Citrix Virtual Desktops usa XAPI para administrar XenServer en una configuración de grupo de varios hosts. Para obtener más información, consulte Citrix Virtual Apps and Desktops.

---

layout: doc
description: Answers to frequently asked questions about XenServer.—

Preguntas frecuentes técnicas

Hardware

¿Cuáles son los requisitos mínimos del sistema para ejecutar XenServer?

Para conocer los requisitos mínimos del sistema para esta versión, consulte Requisitos del sistema.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Necesito un sistema con un procesador x86 de 64 bits para ejecutar XenServer?

Sí. Se requiere un sistema basado en Intel VT o AMD-V x86 de 64 bits con una o más CPU para ejecutar todos los sistemas operativos invitados compatibles.

Para obtener más información sobre los requisitos del sistema host, consulte Requisitos del sistema.

¿Necesito un sistema con soporte de virtualización de hardware?

Necesita un sistema basado en un procesador x86 de 64 bits que admita la tecnología de virtualización de hardware Intel VT o AMD-V en el firmware del procesador y del sistema.

¿Qué sistemas están certificados para ejecutar XenServer?

Para obtener una lista completa de los sistemas certificados por XenServer, consulte la Lista de compatibilidad de hardware (HCL).

¿XenServer es compatible con la indexación rápida de virtualización de AMD y las tablas de páginas extendidas de Intel?

Sí. XenServer es compatible con AMD Rapid Virtualization Indexing y con Intel Extended Page Tables. La indexación de virtualización rápida proporciona una implementación de la tecnología de tablas anidadas que se utiliza para mejorar aún más el rendimiento del hipervisor Xen. Las tablas de páginas extendidas proporcionan una implementación de paginación asistida por hardware que se utiliza para mejorar aún más el rendimiento del hipervisor Xen.

¿Se puede ejecutar XenServer en sistemas portátiles o de escritorio?

XenServer se ejecuta en muchos sistemas portátiles o de sobremesa que cumplen con los requisitos mínimos de CPU. Sin embargo, XenServer solo admite sistemas certificados e incluidos en la Lista de compatibilidad de hardware (HCL).

Puede optar por ejecutarse en sistemas no compatibles con fines de demostración y pruebas. Sin embargo, algunas funciones, como las capacidades de administración de energía, no funcionan.

¿Se puede instalar XenServer en tarjetas SD o USB?

No. XenServer no admite el uso de tarjetas SD o USB para la instalación de XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Solo admitimos hardware que haya sido certificado y esté incluido en la Lista de compatibilidad de hardware (HCL).

Límites de productos

> **Nota:**
>
> Para obtener una lista completa de los límites admitidos por XenServer, consulte Límites de configuración.

¿Cuál es el tamaño máximo de memoria que XenServer puede usar en un sistema host?

Los sistemas host de XenServer pueden utilizar hasta 6 TB de memoria física.

¿Cuántos procesadores puede usar XenServer?

XenServer admite hasta 448 procesadores lógicos por host. La cantidad máxima de procesadores lógicos admitidos varía según la CPU.

Para obtener más información, consulte la Lista de compatibilidad de hardware (HCL).

¿Cuántas máquinas virtuales se pueden ejecutar simultáneamente en XenServer?

La cantidad máxima de máquinas virtuales (VM) que se admiten para ejecutarse en un host de XenServer es 1000. Para los sistemas que ejecutan más de 500 máquinas virtuales, recomendamos asignar al menos 16 GB de RAM a dom0. Para obtener más información, consulte Cambiar la cantidad de memoria asignada al dominio de control.

Para cualquier sistema en particular, la cantidad de máquinas virtuales que se pueden ejecutar simultáneamente y con un rendimiento aceptable depende de los recursos disponibles y de la carga de trabajo de la máquina virtual. XenServer escala automáticamente la cantidad de memoria asignada al dominio de control (dom0) en función de la memoria física disponible.

> **Nota:**
>
> Si hay más de 50 máquinas virtuales por host y la memoria física del host es inferior a 48 GB, puede ser recomendable anular esta configuración. Para obtener más información, consulte Uso de memoria.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Cuántas interfaces de red físicas admite XenServer?

XenServer admite hasta 16 puertos NIC físicos. Estas NIC se pueden unir para crear hasta 8 enlaces de red lógicos. Cada enlace puede incluir hasta 4 NIC.

¿Cuántos procesadores virtuales (vCPU) puede asignar XenServer a una máquina virtual?

XenServer admite hasta 32 vCPU por máquina virtual. La cantidad de CPU virtuales que se pueden admitir varía según el sistema operativo invitado.

> **Nota:**
>
> Consulte la documentación del sistema operativo invitado para asegurarse de que no supera los límites admitidos.

¿Cuánta memoria puede asignar XenServer a una máquina virtual?

XenServer admite hasta 1,5 TB por huésped. La cantidad de memoria que se puede admitir varía según el sistema operativo invitado.

> **Nota:**
>
> La cantidad máxima de memoria física direccionable por el sistema operativo varía. Establecer la memoria en un nivel superior al límite admitido por el sistema operativo puede provocar problemas de rendimiento en el huésped.

¿Cuántas imágenes de disco virtual (VDI) puede asignar XenServer a una máquina virtual?

XenServer puede asignar hasta 255 VDI, incluido un dispositivo de DVD-ROM virtual, por máquina virtual.

> **Nota:**
>
> La cantidad máxima de VDI admitidos depende del sistema operativo invitado. Consulte la documentación del sistema operativo invitado para asegurarse de que no supera los límites admitidos.

¿Cuántas interfaces de red virtuales puede asignar XenServer a una máquina virtual?

XenServer puede asignar hasta 7 NIC virtuales por máquina virtual. La cantidad de NIC virtuales que se pueden admitir varía según el sistema operativo invitado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Intercambio de recursos

¿Cómo se dividen los recursos de procesamiento entre las VM?

XenServer divide los recursos de procesamiento entre las CPU virtuales mediante un algoritmo de equilibrio justo. Este algoritmo garantiza que todas las máquinas virtuales obtengan su parte de los recursos de procesamiento del sistema.

¿Cómo elige XenServer los procesadores físicos que asigna a la máquina virtual?

XenServer no asigna procesadores físicos de forma estática a ninguna máquina virtual específica. En su lugar, XenServer asigna de forma dinámica, según la carga, todos los procesadores lógicos disponibles a la máquina virtual. Esta asignación dinámica garantiza que los ciclos del procesador se usen de manera eficiente porque la VM puede ejecutarse en cualquier lugar donde haya capacidad de reserva.

¿Cómo se dividen los recursos de E/S de disco entre las VM?

XenServer utiliza una división equitativa de recursos para los recursos de E/S de disco entre las máquinas virtuales. También puede proporcionar a una VM acceso de mayor o menor prioridad a los recursos de E/S del disco.

¿Cómo se dividen los recursos de E/S de red entre las VM?

XenServer utiliza una distribución equitativa de los recursos de E/S de la red entre las máquinas virtuales. También puede controlar la velocidad de los datos salientes mediante Open vSwitch. Para obtener más información, consulte Controlar la velocidad de los datos salientes (QoS).

Sistemas operativos invitados

¿Puede XenServer ejecutar sistemas operativos de 32 bits como invitados?

Sí. Para obtener más información, consulte Sistemas operativos invitados compatibles.

¿Puede XenServer ejecutar sistemas operativos de 64 bits como invitados?

Sí. Para obtener más información, consulte Sistemas operativos invitados compatibles.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Qué versiones de Microsoft Windows se pueden ejecutar como huéspedes en XenServer?

Para obtener una lista de los sistemas operativos invitados de Windows compatibles, consulte Sistemas operativos invitados compatibles.

¿Qué versiones de Linux se pueden ejecutar como huéspedes en XenServer?

Para obtener una lista de los sistemas operativos invitados de Linux compatibles, consulte Sistemas operativos invitados compatibles.

¿Puedo ejecutar diferentes versiones de los sistemas operativos compatibles u otros sistemas operativos que no figuran en la lista?

Solo admitimos sistemas operativos (SO) con soporte de proveedores de sistemas operativos. Si bien es posible que los sistemas operativos no compatibles sigan funcionando, es posible que le pidamos que actualice a un service pack de SO compatible antes de que podamos investigar cualquier problema.

Es posible que los controladores aplicables no estén disponibles para las versiones de SO que no son compatibles. Sin los controladores, estas versiones del sistema operativo no funcionan con un rendimiento optimizado.

A menudo es posible instalar otras distribuciones de Linux. Sin embargo, XenServer solo admite los sistemas operativos que figuran en Sistemas operativos invitados compatibles. Es posible que le pidamos que cambie a un sistema operativo compatible antes de que podamos investigar cualquier problema.

¿XenServer admite FreeBSD, NetBSD o cualquier otra variante de BSD como sistema operativo invitado?

XenServer no admite ningún sistema operativo huésped basado en BSD para las implementaciones de virtualización de uso general. Sin embargo, las máquinas virtuales de FreeBSD que se ejecutan en XenServer están certificadas para su uso en productos específicos de NetScaler.

¿Qué son las herramientas de máquinas virtuales de XenServer?

Las herramientas de máquina virtual de XenServer son paquetes de software para los sistemas operativos invitados Windows y Linux. Para los sistemas operativos Windows, las herramientas de máquinas virtuales de XenServer para Windows incluyen controladores de E/S de alto rendimiento (controladores PV) y el agente de administración.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para los sistemas operativos Linux, las herramientas de máquina virtual de XenServer para Linux incluyen un agente invitado que proporciona información adicional sobre la máquina virtual al host de XenServer.

Para obtener más información, consulte XenServer VM Tools.

Docker

¿Puedo ejecutar contenedores de Docker en mis máquinas virtuales Linux?

Sí. Docker es compatible con las máquinas virtuales Linux alojadas en XenServer.

¿Puedo ejecutar contenedores de Docker en mis máquinas virtuales Windows?

No. No puede ejecutar contenedores de Docker en una máquina virtual Windows alojada en XenServer. Esta restricción se debe a que XenServer no admite la virtualización anidada para las máquinas virtuales de Windows.

¿XenServer ofrece funciones adicionales para trabajar con Docker?

No.

En versiones anteriores de XenServer y Citrix Hypervisor, estaba disponible un paquete complementario de administración de contenedores que le permitía administrar los contenedores de Docker a través de XenCenter. Se ha eliminado esta función.

XenCenter

Para obtener más información, consulte XenCenter.

¿Debo ejecutar XenCenter en un equipo con Windows?

Sí. La consola de administración de XenCenter se ejecuta en un sistema operativo Windows. Para obtener información sobre los requisitos del sistema, consulte Requisitos del sistema

Si no quiere ejecutar Windows, puede administrar los hosts y grupos de XenServer mediante la CLI xe o mediante `xsconsole`una consola de configuración del sistema.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Puedo iniciar sesión en XenCenter mediante mis cuentas de usuario de Active Directory?

Sí. Puede configurar las solicitudes de inicio de sesión de XenCenter para usar Active Directory en todas las ediciones de XenServer.

Para obtener más información, consulte Administrar usuarios.

¿Puedo restringir el acceso a determinadas funciones de XenCenter a determinados usuarios?

Sí. La función de control de acceso basado en roles combinada con la autenticación de Active Directory puede restringir el acceso de los usuarios en XenCenter.

Para obtener más información, consulte Administrar usuarios.

¿Puedo usar una sola consola XenCenter para conectarme a varios hosts de XenServer?

Sí. Puede usar una sola consola XenCenter para conectarse a varios sistemas host de XenServer.

¿Puedo usar XenCenter para conectarme a varios hosts que ejecuten diferentes versiones de XenServer?

Dependiendo de la versión de XenServer, sí. XenCenter es compatible con versiones anteriores de Citrix Hypervisor 8.0 y versiones posteriores. Sin embargo, tenga en cuenta que solo Citrix Hypervisor 8.2 CU 1 recibe soporte completo.

¿Puedo usar XenCenter para conectarme a varios grupos de recursos?

Sí. Puede conectarse a varios grupos de recursos desde una sola consola de XenCenter.

¿Cómo puedo obtener acceso a la consola de una VM Linux?

La ficha **Consola** de XenCenter proporciona acceso a las consolas gráficas y basadas en texto de las máquinas virtuales que ejecutan sistemas operativos Linux. Antes de poder conectarse con la consola gráfica de una VM Linux, instale y configure un servidor VNC y un administrador de pantalla X en la VM.

XenCenter también le permite conectarse a máquinas virtuales Linux a través de SSH mediante la opción **Abrir consola SSH** en la ficha **Consola** de la máquina virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Cómo puedo obtener acceso a la consola de una VM Windows?

XenCenter proporciona acceso a los gráficos emulados para una VM de Windows. Si XenCenter detecta capacidades de escritorio remoto en la máquina virtual, XenCenter proporciona un botón de conexión rápida para iniciar un cliente RDP integrado que se conecta a la máquina virtual. O bien, puede conectarse directamente con sus invitados mediante un software de escritorio remoto externo.

Interfaz de línea de comandos (CLI)

Para obtener más información, consulte Interfaz de línea de comandos.

¿Incluye XenServer una CLI?

Sí. Todas las ediciones de XenServer incluyen una interfaz de línea de comandos (CLI) completa, conocida como. `xe`

¿Puedo acceder a la CLI xe directamente en el host?

Sí. Puede acceder a la CLI conectando una pantalla y un teclado directamente al host, o a través de un emulador de terminal conectado al puerto serie del host.

¿Puedo acceder a la CLI xe desde un sistema remoto?

Sí. XenServer incluye la CLI xe, que se puede instalar en máquinas Windows y Linux de 64 bits para controlar XenServer de forma remota. También puede usar XenCenter para acceder a la consola del host desde la ficha Consola.

¿Puedo usar la CLI xe con mis cuentas de usuario de Active Directory?

Sí. Puede iniciar sesión con Active Directory en todas las ediciones de XenServer.

¿Puedo restringir el acceso al uso de ciertos comandos de la CLI a ciertos usuarios?

Sí. Puede restringir el acceso de los usuarios en la CLI xe.

VM

Para obtener más información, consulte Administrar máquinas virtuales.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Se pueden ejecutar las máquinas virtuales creadas con VMware o Hyper-V en XenServer?

Sí. Puede exportar e importar máquinas virtuales mediante el formato OVF estándar del sector.

También puede convertir máquinas virtuales en lotes mediante XenServer Conversion Manager. También hay disponibles herramientas de terceros.

Para obtener más información, consulte Conversion Manager.

¿Qué tipos de medios de instalación puedo usar para instalar un sistema operativo invitado?

Puede instalar un sistema operativo invitado mediante:

- Un CD en la unidad de CD-ROM del host
- Una unidad de CD-ROM virtual que utiliza tecnología como DRAC
- Colocación de imágenes ISO en una unidad de red compartida
- Instalación en red, si es compatible con el invitado específico.

Para obtener más información, consulte Administrar máquinas virtuales.

¿Puedo hacer un clon de una VM existente?

Sí. Cualquier máquina virtual creada en XenServer se puede clonar o convertir en una plantilla de máquina virtual. A continuación, se puede usar una plantilla de VM para crear más VM.

¿Se pueden exportar las máquinas virtuales de una versión de XenServer y moverlas a otra?

Sí. Las máquinas virtuales exportadas desde versiones anteriores de XenServer se pueden importar a una versión más reciente.

¿Puedo convertir una máquina virtual de la versión de código abierto de Xen a XenServer?

No.

¿XenServer proporciona capacidades de instantáneas de disco para las máquinas virtuales?

Sí. XenServer admite el uso de instantáneas en todas las ediciones. Para obtener más información, consulte Instantáneas de VM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Almacenamiento

Para obtener más información, consulte Almacenamiento.

¿Qué tipos de almacenamiento local se pueden usar con XenServer?

XenServer admite almacenamiento local como SATA, SAS y NVMe.

¿Qué tipo de almacenamiento SAN/NAS se puede usar con XenServer?

XenServer admite repositorios de almacenamiento Fibre Channel, FCoE, iSCSI basado en hardware (HBA), iSCSI, NFS y SMB.

Para obtener más información, consulte Almacenamiento y lista de compatibilidad de hardware.

¿XenServer admite iSCSI basado en software?

Sí. XenServer incluye un iniciador iSCSI integrado basado en software (iSCSI abierto).

¿Qué versión de NFS se requiere para el uso de almacenamiento remoto?

XenServer requiere NFSv3 o NFSv4 a través de TCP para el uso del almacenamiento remoto. Actualmente, XenServer no admite NFS a través del Protocolo de datagramas de usuario (UDP).

¿Puedo usar NFS basado en software que se ejecuta en un servidor de uso general para el almacenamiento compartido remoto?

Sí. Sin embargo, recomendamos utilizar un dispositivo NAS dedicado con NFSv3 o NFSv4 con almacenamiento en caché no volátil de alta velocidad para lograr niveles aceptables de rendimiento de E/S.

¿Puedo arrancar un sistema host XenServer desde una SAN iSCSI, Fibre Channel o FCoE?

Sí. XenServer admite el arranque desde SAN mediante HBAs Fibre Channel, FCoE o iSCSI.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Puedo arrancar un host de XenServer desde UEFI?

Sí. XenServer admite el arranque desde UEFI. Sin embargo, los hosts XenServer no admiten el arranque seguro UEFI.

Actualmente se admite el arranque desde la BIOS, pero se eliminará en una versión futura.

Para obtener más información, consulte Instalaciones mediante arranque de red

¿XenServer admite E/S de múltiples rutas (MPIO) para las conexiones de almacenamiento?

Sí. Recomendamos usar rutas múltiples para conexiones de almacenamiento resilientes.

¿XenServer admite una implementación de RAID basada en software?

No. XenServer no admite RAID de software.

¿XenServer es compatible con las soluciones HostRAID o FakeRAID?

No. XenServer no admite soluciones patentadas tipo RAID, como HostRAID o FakeRAID.

¿XenServer admite la clonación ligera de las máquinas virtuales existentes?

Sí. La clonación ligera está disponible en discos locales formateados como EXT3/EXT4, además de en los repositorios de almacenamiento NFS y SMB.

¿XenServer admite el almacenamiento de dispositivos de bloques replicados distribuidos (DRBD)?

No. XenServer no admite DRBD.

¿XenServer admite ATA a través de Ethernet?

No. XenServer no admite almacenamiento basado en ATA a través de Ethernet.

Redes

Para obtener más información, consulte Redes

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Puedo crear redes privadas que aíslen grupos de VM?

Sí. Puede crear una red privada en un único host para las VM residentes.

¿XenServer admite varias conexiones de red físicas?

Sí. Puede conectarse o asociar varias redes físicas que se conectan a diferentes interfaces de red en el sistema host físico.

¿Se pueden conectar las VM a varias redes?

Sí. Las VM se pueden conectar a cualquier red disponible para el host.

¿XenServer admite IPv6?

Las máquinas virtuales alojadas en XenServer pueden usar cualquier combinación de direcciones configuradas para IPv4 e IPv6.

Sin embargo, XenServer no admite el uso de IPv6 en su dominio de control (dom0). No puede usar IPv6 para la red de administración de hosts ni para la red de almacenamiento. El protocolo IPv4 debe estar disponible para que lo utilice el host de XenServer.

¿XenServer admite VLAN en una interfaz de red física?

Sí. XenServer admite la asignación de redes de máquinas virtuales a VLAN específicas.

¿Las redes virtuales de XenServer transmiten todo el tráfico de red a todas las máquinas virtuales?

De forma predeterminada, las interfaces de red de XenServer no son promiscuas y una máquina virtual solo puede ver el tráfico de esa máquina virtual y el tráfico de difusión.

Este comportamiento se puede configurar en función de la pila de red que esté utilizando.

- Si utiliza el puente de Linux como pila de red, las interfaces de red virtual se pueden configurar para el modo promiscuo. Este modo le permite ver todo el tráfico en un conmutador virtual. Para obtener más información sobre la configuración del modo promiscuo, consulte los siguientes artículos de Knowledge Center:
  - CTX116493 - Cómo habilitar el modo promiscuo en una tarjeta de red física
  - CTX121729: Cómo configurar una máquina virtual promiscua en XenServer

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Al habilitar el modo promiscuo en una interfaz de red virtual, para que una máquina virtual utilice esta configuración, también debe habilitar el modo promiscuo dentro de la máquina virtual.

- Si utiliza Open vSwitch (OVS) como pila de red, actúa como conmutador de capa 2. Una VM solo ve el tráfico de esa VM. Además, el bloqueo del puerto del conmutador en XenServer permite aumentar los niveles de aislamiento y seguridad. El OVS no se puede configurar en modo promiscuo.

¿XenServer admite la unión o la formación de equipos de interfaces de red físicas?

Sí. XenServer admite la vinculación de interfaces de red físicas para la conmutación por error y la agregación de enlaces con compatibilidad opcional con LACP. Para obtener más información, consulte Redes.

Memoria

¿Cuánta memoria consume la ejecución de XenServer?

Tres componentes contribuyen al consumo de memoria de un host de XenServer.

1. El hipervisor Xen
2. El dominio de control en el host (dom0)
3. El kernel que se bloquea de XenServer

La cantidad de memoria necesaria para ejecutar dom0 se ajusta automáticamente. De forma predeterminada, XenServer asigna 1 GiB más el 5% de la memoria física total al dominio de control, hasta un máximo inicial de 8 GiB.

> **Nota:**
>
> La cantidad de memoria asignada al dominio de control se puede aumentar más allá de la cantidad predeterminada.

En XenCenter, **el campo Xen de la** ficha Memoria indica **la** memoria utilizada por el dominio de control, por el propio hipervisor Xen y por el kernel de bloqueo de XenServer. La cantidad de memoria utilizada por el hipervisor es mayor para los hosts con más memoria.

Para obtener más información, consulte Uso de memoria

¿XenServer optimiza el uso de la memoria de las máquinas virtuales?

Sí. XenServer usa el control dinámico de memoria (DMC) para ajustar automáticamente la memoria de las máquinas virtuales en ejecución. Estos ajustes mantienen la cantidad de memoria asignada a cada

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

VM entre los valores de memoria mínimos y máximos especificados, lo que garantiza el rendimiento y permite una mayor densidad de VM.

Para obtener más información, consulte Memoria de VM.

Grupos de recursos

Para obtener más información, consulte Hosts y grupos de recursos.

¿Qué es un grupo de recursos?

Un grupo de recursos es un conjunto de hosts de XenServer administrados como una unidad. Por lo general, un grupo de recursos comparte cierta cantidad de almacenamiento en red para permitir que las VM migren rápidamente de un host a otro dentro del grupo.

¿Requiere XenServer un host dedicado para administrar un grupo de recursos?

No. Se debe especificar un único anfitrión del grupo como coordinador del grupo. El coordinador del grupo controla todas las actividades administrativas necesarias en el grupo. Este diseño significa que no hay un punto único externo de falla. Si el coordinador del grupo falla, otros hosts del grupo siguen funcionando y las máquinas virtuales residentes siguen ejecutándose normalmente. Si el coordinador del grupo no puede volver a conectarse, XenServer convierte a uno de los otros hosts del grupo en coordinador para recuperar el control del grupo.

Este proceso se automatiza con la función de alta disponibilidad. Para obtener más información, consulte Alta disponibilidad.

¿Dónde se almacenan los datos de configuración de una agrupación de recursos?

Se almacena una copia de los datos de configuración en cada host del grupo de recursos. Si el coordinador del grupo actual falla, estos datos permiten que cualquier host del grupo de recursos se convierta en el nuevo coordinador del grupo.

¿Qué tipos de configuraciones se pueden realizar en el nivel del grupo de recursos?

Las configuraciones de redes y almacenamiento remoto compartido se pueden realizar en el nivel del grupo de recursos. Cuando se comparte una configuración en la agrupación de recursos, el sistema coordinador propaga automáticamente los cambios de configuración a todos los sistemas miembros.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Se agregan nuevos sistemas host a un grupo de recursos que se configuran automáticamente con configuraciones compartidas?

Sí. Todos los sistemas host nuevos que se agreguen a un grupo de recursos reciben automáticamente las mismas configuraciones para el almacenamiento compartido y la configuración de red.

¿Puedo usar diferentes tipos de CPU en el mismo grupo de recursos de XenServer?

Sí. Recomendamos que se utilice el mismo tipo de CPU en todo el grupo (grupo de recursos homogéneo). Sin embargo, es posible que los hosts con diferentes tipos de CPU se unan a un grupo (heterogéneo), siempre que las CPU sean del mismo proveedor.

Para obtener más información, consulte Hosts y grupos de recursos.

Para obtener información actualizada sobre la compatibilidad con el enmascaramiento de funciones para tipos de CPU específicos, consulte Lista de compatibilidad de hardware.

Migración en vivo (anteriormente XenMotion)

Para obtener más información, consulte Migrar máquinas virtuales.

¿Puedo mover una VM en ejecución de un host a otro?

Con la migración en vivo, puede mover las VM en ejecución cuando los hosts comparten almacenamiento (en un grupo).

Además, la migración en vivo del almacenamiento permite la migración entre hosts que no comparten almacenamiento de información. Las VM se pueden migrar dentro de los grupos o entre ellos.

Alta disponibilidad

Para obtener más información, consulte Alta disponibilidad.

¿XenServer ofrece funciones de alta disponibilidad?

Sí. Si la alta disponibilidad está habilitada, XenServer supervisa continuamente el estado de los hosts de un grupo. Si la alta disponibilidad detecta que un host está dañado, el host se apaga automáticamente. Esta acción permite que las VM se reinicien de forma segura en un host alternativo en buen estado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿La alta disponibilidad de XenServer admite el almacenamiento local?

No. Si quiere utilizar la alta disponibilidad, se requiere almacenamiento compartido. Este almacenamiento compartido permite que las VM se reubiquen si falla un host. Sin embargo, la alta disponibilidad permite que las máquinas virtuales almacenadas en el almacenamiento local se marquen para el reinicio automático cuando el host se recupere después de un reinicio.

¿Puedo usar la alta disponibilidad para secuenciar automáticamente el reinicio de las VM recuperadas?

Sí. La configuración de alta disponibilidad le permite definir el orden en que se inician las VM. Esta capacidad permite que las máquinas virtuales que dependen unas de otras se secuencien automáticamente.

Métricas de rendimiento

¿Las herramientas de administración de XenServer recopilan información sobre el rendimiento?

Sí. XenServer proporciona una supervisión detallada de las métricas de rendimiento. Estas métricas incluyen información de CPU, memoria, disco, red, estado C/estado P y almacenamiento. Cuando corresponda, estas métricas están disponibles por host y por VM. Las métricas de rendimiento están disponibles directamente (se exponen como bases de datos por turnos) o se puede acceder a ellas y verlas gráficamente en XenCenter u otras aplicaciones de terceros. Para obtener más información, consulte Supervisar y administrar su implementación.

¿Cómo se recopilan las métricas de rendimiento de XenServer?

Los datos de las métricas de rendimiento de XenServer se recopilan de varias fuentes. Estas fuentes incluyen el hipervisor Xen, Dom0, las interfaces Linux estándar y las interfaces estándar de Windows, como WMI.

¿XenCenter muestra métricas de rendimiento en tiempo real?

Sí. XenCenter muestra las métricas de rendimiento en tiempo real en **la** ficha Rendimiento para cada máquina virtual en ejecución y para el host de XenServer. Puede personalizar las métricas que se muestran.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿XenCenter almacena y muestra métricas de rendimiento históricas?

Sí. XenServer mantiene las métricas de rendimiento del año pasado (con una granularidad decreciente). XenCenter proporciona una visualización de estas métricas en pantallas gráficas en tiempo real.

Instalación

Para obtener más información, consulte Instalación.

¿Se instala XenServer sobre sistemas que ya ejecutan un sistema operativo existente?

No. XenServer se instala directamente en el hardware básico, lo que evita la complejidad, la sobrecarga y los cuellos de botella en el rendimiento de un sistema operativo subyacente.

¿Puedo actualizar una instalación de XenServer existente a una versión más reciente?

Sí. Si ejecuta una versión compatible de XenServer, puede actualizar a una versión más reciente de XenServer en lugar de realizar una instalación nueva. Para obtener más información, consulte Actualizar.

¿Puedo actualizar desde una versión no compatible de Citrix Hypervisor o XenServer a esta versión?

Si su versión actual de Citrix Hypervisor o XenServer ya no es compatible, no puede actualizarla a la versión más reciente de XenServer. Solo se admiten las actualizaciones desde la actualización acumulativa 1 de Citrix Hypervisor 8.2.

Para obtener más información, consulte Actualizar.

¿Cuánto almacenamiento local necesita XenServer para la instalación en el sistema host físico?

XenServer requiere un mínimo de 46 GB de almacenamiento local en el sistema host físico.

¿Puedo usar PXE para realizar una instalación de red de XenServer en el sistema host?

Sí. Puede instalar XenServer en el sistema host mediante PXE. También puede instalar XenServer automáticamente mediante PXE mediante la creación de un archivo de respuesta preconfigurado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿El hipervisor Xen funciona en Linux?

No. Xen es un hipervisor Tipo 1 que se ejecuta directamente en el hardware host ("bare metal"). Una vez que se carga el hipervisor, inicia el dominio de administración con privilegios, el dominio de control (dom0), que contiene un entorno Linux mínimo.

¿De dónde obtiene XenServer su compatibilidad con los controladores de dispositivos?

XenServer usa los controladores de dispositivo disponibles en el núcleo de Linux. Como resultado, XenServer se ejecuta en una amplia variedad de dispositivos de almacenamiento y hardware. Sin embargo, le recomendamos que utilice controladores de dispositivo certificados.

Para obtener más información, consulte la Lista de compatibilidad de hardware.

Licencias

Para obtener información sobre las licencias de XenServer, consulte Licencias.

Asistencia técnica

Para obtener más información sobre asistencia, consulte Asistencia técnica.

¿XenServer proporciona soporte técnico directo para XenServer?

Sí. Para obtener más información, visite las páginas de asistencia de XenServer.

¿Debo comprar un contrato de soporte técnico de XenServer al mismo tiempo que compro XenServer?

No. La compra de la licencia incluye un contrato de asistencia técnica. Para obtener información sobre el nivel de asistencia que ofrecemos a los clientes de las ediciones Premium y Standard, visite las páginas de asistencia de XenServer.

¿A qué nivel de asistencia me da derecho mi licencia?

Al comprar una licencia de XenServer por socket, también se beneficia de nuestros servicios de asistencia técnica. Para obtener más información sobre los niveles de asistencia técnica, consulte https://xenserver.com/support.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Puedo obtener asistencia si mis hosts usan la edición de prueba?

Si es usuario de la edición de prueba, no reúne los requisitos para recibir asistencia. Sin embargo, valoramos sus comentarios: Envíenos sus comentarios.

¿Hay canales alternativos para obtener asistencia para XenServer?

Sí. Existen varios canales alternativos para obtener soporte técnico para XenServer. También puede usar Citrix Knowledge Center o contratar a socios de XenServer autorizados que ofrecen servicios de asistencia técnica.

¿XenServer proporciona soporte técnico para el proyecto Xen de código abierto?

No. XenServer no proporciona soporte técnico para el proyecto Xen de código abierto. Para obtener más información, consulte http://www.xen.org/.

¿Puedo abrir un incidente de soporte técnico con XenServer si tengo un problema no técnico?

No. Plantee cualquier problema no técnico a través del Servicio de atención al cliente de Citrix. Por ejemplo, problemas relacionados con el mantenimiento del software, las licencias, el soporte administrativo y la confirmación del pedido.

Descripción general del sistema de licencias

April 10, 2024

> **Importante:**
>
> Si utiliza XenServer para ejecutar las cargas de trabajo de Citrix Virtual Apps and Desktops, debe tener una licencia Premium Edition. Para obtener más información sobre cómo obtener una licencia de XenServer, consulte https://xenserver.com/buy.
> Este requisito supone un cambio de comportamiento con respecto a la versión anterior de Citrix Hypervisor/XenServer. Para obtener más información, consulte las preguntas frecuentes sobre licencias.
>
> Los clientes actuales pueden solicitar participar en nuestra promoción y recibir hasta 10 000 licencias de socket de XenServer Premium Edition de forma gratuita. Más información.

XenServer 8 está disponible en las siguientes ediciones:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Premium Edition** es nuestra oferta premium, optimizada para cargas de trabajo de escritorio, servidor y nube. Además de las funciones disponibles en la Standard Edition, la Premium Edition ofrece las siguientes funciones:
  - Balance dinámico de cargas
  - Virtualización de GPU con NVIDIA vGPU e Intel GVT-g
  - Aprovisionamiento controlado para dispositivos de almacenamiento en bloques compartidos
  - Soporte para almacenamiento de pequeñas y medianas empresas
  - API de Direct Inspect
  - Exportar datos de recursos del grupo
  - Almacenamiento en caché de lectura en memoria
  - PVS-Accelerator
  - Habilitación para el modo tableta de Citrix Virtual Desktops
  - Seguimiento de bloques modificado
  - Indagación IGMP
  - Paso a través de USB
  - Soporte de red SR-IOV
  - Supervisar los recursos del host y del dom0 con NRPE
  - Supervisar los recursos de host y dom0 con SNMP
- **La edición estándar** es nuestra oferta comercial básica. Cuenta con una gama de funciones para los clientes que desean una plataforma de virtualización sólida y de alto rendimiento, pero que no requieren las funciones premium de la Edición Premium. Mientras tanto, todavía quieren beneficiarse de la garantía de un soporte y un mantenimiento integrales.
- **La edición Trial Edition** actualmente incluye el conjunto de funciones de la edición Premium para un grupo de tamaño restringido (tres hosts como máximo), pero no permite la actualización sucesiva de grupos a través de XenCenter.

Para obtener más información, consulte https://www.xenserver.com/editions.

	Premium Edition	Standard Edition	Edición de prueba
Conjunto de funciones premium	Sí		Sí
Actualización progresiva de la agrupación a través de XenCenter	Sí	Sí	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	Premium Edition	Standard Edition	Edición de prueba
Actualizaciones funcionales y de seguridad continuas	Sí	Sí	Sí
Tamaño máximo de agrupación	64 (16 con SR GFS2)	64 (16 con SR GFS2)	3

La licencia de XenServer se otorga *por* socket. La asignación de licencias se gestiona de forma centralizada y se aplica mediante un servidor de licencias Citrix independiente (físico o virtual) en el entorno. Para obtener más información sobre las licencias de XenServer, consulte las Preguntas frecuentes sobre licencias.

Concesión de licencias para sus hosts y grupos

XenServer utiliza el mismo proceso de concesión de licencias que algunos productos Citrix. Para usar XenServer Premium Edition o XenServer Standard Edition, necesita una licencia válida para instalarse en un servidor de licencias Citrix y asignarla a su host XenServer. Este proceso se describe en detalle en la guía de licencias de XenServer.

> **Nota:**
>
> Actualmente, XenServer no admite licencias alojadas en Citrix Cloud. Se requiere un servidor de licencias Citrix local.

Para licenciar sus hosts, necesita los siguientes elementos:

- Una licencia
- Un servidor de licencias Citrix
- Un host de XenServer
- XenCenter

1. Instalar el servidor de licencias de Citrix

Puede descargar el servidor de licencias de Citrix para Windows desde la página de descargas de licencias de Citrix.

Instale el servidor de licencias Citrix en un sistema Windows según las instrucciones de la documentación de Citrix Licensing.

El sistema Windows en el que instale el servidor de licencias de Citrix puede ser una máquina virtual de Windows alojada en su grupo de XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

XenServer funciona con una licencia "estándar"hasta que el servidor de licencias pueda arrancar. Este comportamiento significa que, después de haber licenciado los hosts XenServer de su grupo, si reinicia el host en el que se ejecuta el servidor de licencias Citrix, se aplica un período de gracia hasta que se reinicie el servidor de licencias.

2. Descargar archivos de licencia

Descargue un archivo de licencias que esté vinculado al nombre de host de su servidor de licencias Citrix, que distinga mayúsculas de minúsculas, y que contenga una cantidad suficiente de licencias por socket como para compartirlas entre los hosts correspondientes.

Para obtener información sobre la compra de una licencia de XenServer, consulte https://xenserver.com/buy.

Para obtener más información sobre cómo obtener los archivos de licencia, consulte la documentación del producto Citrix Licensing.

3. Agregar el archivo de licencias al servidor de licencias de Citrix

Utilice Citrix Licensing Manager para instalar las licencias en su servidor de licencias Citrix. Para obtener más información, consulte la documentación del producto Citrix Licensing.

4. Aplicar las licencias a los hosts de su agrupación de recursos

Puede asignar licencias alojadas en un servidor de licencias Citrix a los hosts y grupos de XenServer mediante XenCenter o la CLI xe.

Aplique una licencia a todos los hosts mediante XenCenter R: Siga este procedimiento para aplicar una licencia:

1. En el menú **Herramientas**, haga clic en **Administrador de licencias**.
2. Seleccione el grupo o los hosts para los que quiera licenciar y, a continuación, haga clic en **Asignar licencia**.
3. En el cuadro de diálogo **Aplicar licencia**, especifique el tipo de **edición** que quiere asignar al host.
4. Escriba el nombre de host o la dirección IP del servidor de licencias de Citrix.
5. Haga clic en **Aceptar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aplicar una licencia a los hosts o grupos mediante la CLI xe Para aplicar una licencia a un único host, ejecute el comando `host-apply-edition`:

```
    xe host-apply-edition edition=premium-per-socket|standard-per-
       socket  \

        license-server-address=<license_server_address> host-uuid=<
           uuid_of_host>  \

        license-server-port=<license_server_port>
<!--NeedCopy-->
```

Para aplicar una licencia a todos los hosts de un grupo, ejecute el comando `pool-apply-edition` :

```
    xe pool-apply-edition edition=premium-per-socket|standard-per-
       socket  \

        license-server-address=<license_server_address> pool-uuid=<
           uuid_of_pool>  \

        license-server-port=<license_server_port>
<!--NeedCopy-->
```

Preguntas frecuentes sobre licencias

April 10, 2024

Este artículo contiene preguntas frecuentes sobre la concesión de licencias a los hosts y grupos de XenServer.

- Preguntas generales
- Citrix Virtual Apps and Desktops
- Servidores de licencias Citrix
- Licenciar un grupo de XenServer
- Más información

Preguntas generales

P: ¿Dónde puedo comprar una licencia de XenServer?

R: Puede obtener información sobre la compra de una licencia de XenServer en. http://www.xenserver.com/buy

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

P: ¿Cómo puedo aplicar una licencia de XenServer?

R: XenServer requiere un servidor de licencias. Después de licenciar XenServer, se le proporciona un código de acceso a la licencia.LIC. Instale este código de acceso a la licencia en su servidor de licencias Citrix.

Al asignar una licencia a un host de XenServer, XenServer se pone en contacto con el servidor de licencias de Citrix especificado y solicita una licencia para los hosts especificados. Si tiene éxito, se desprotege una licencia y el Administrador de licencias muestra información sobre la licencia con la que los hosts tienen licencia.

P: ¿Cuántas licencias necesito para licenciar mi agrupación de recursos?

R: La licencia de XenServer se otorga *por socket de CPU* . Para que un grupo se considere con licencia, todos los hosts XenServer del grupo deben tener licencia. XenServer solo cuenta los sockets de CPU llenos.

Puede usar el servidor de licencias de Citrix para ver el número de licencias disponibles que se muestran en el *panel de la consola de administración de licencias*.

P: ¿Necesito una licencia por socket para los sockets que no están llenos?

R: No, solo los sockets de CPU ocupados se cuentan para la cantidad de sockets para los que se va a licenciar.

P: ¿Pierdo mi máquina virtual (VM) cuando caduque mi licencia?

R: No, no pierde ninguna VM ni sus datos.

P: ¿Qué ocurre si tengo un grupo de licencias y el servidor de licencias deja de estar disponible?

R. Si su licencia no ha caducado y el servidor de licencias no está disponible, dispondrá de un *período de gracia* de 30 días en el nivel de licencia que se aplicó anteriormente.

Tras el período de gracia, si su licencia sigue sin estar disponible, su grupo pasará a ser de edición de prueba y solo estarán disponibles las funciones incluidas en la edición de prueba. El grupo sigue siendo del mismo tamaño, pero si tiene tres o más hosts, no puede agregarle más hosts.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

P: ¿Cómo puedo obtener una licencia para evaluar XenServer?

R: Con Trial Edition, puede instalar XenServer sin licencia y probar todas las funciones de la edición Premium Edition en un grupo de tamaño reducido. Para obtener más información, consulte Ediciones de XenServer.

P: ¿Puedo usar XenServer 8 sin licencia?

R: Sí. La edición de prueba de XenServer 8 permite que XenServer esté disponible sin licencia. La edición incluye todas las funciones de la Edición Premium en un grupo reducido de hasta tres anfitriones. Para obtener más información, consulte Ediciones de XenServer.

P: ¿Puedo usar Citrix Cloud para aplicar una licencia a XenServer?

No, XenServer no admite actualmente licencias alojadas en Citrix Cloud. Para licenciar XenServer, necesita un servidor de licencias. Para obtener más información, consulte Licencias para sus hosts y grupos.

P: ¿A qué nivel de asistencia me da derecho mi licencia?

Al comprar una licencia de XenServer por socket, también se beneficia de nuestros servicios de asistencia técnica. Para obtener más información sobre los niveles de asistencia técnica, consulte https://xenserver.com/support.

Si es usuario de la edición de prueba, no reúne los requisitos para recibir asistencia. Sin embargo, valoramos sus comentarios: Envíenos sus comentarios.

Para obtener más información, consulte Preguntas de asistencia técnica y Asistencia técnica

P: Voy a actualizar a XenServer 8 desde una versión anterior de Citrix Hypervisor con una licencia por socket. ¿Tengo que hacer algo?

R: No. Puede actualizar sus hosts a XenServer 8 con las licencias por socket adquiridas anteriormente, siempre que Customer Success Services sea válido al menos hasta el 1 de marzo de 2024.

Si ha renovado sus Customer Success Services después de la compra original, es posible que deba actualizar el archivo de licencia en el servidor de licencias para asegurarse de que muestre la elegibilidad de los Customer Success Services.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

P: Voy a actualizar a XenServer 8 desde una versión anterior de Citrix Hypervisor con una licencia de Citrix Virtual Apps and Desktops. ¿Tengo que hacer algo?

R: Sí. Antes de intentar actualizar a XenServer 8, debe obtener las licencias de XenServer Premium Edition, importarlas al servidor de licencias de Citrix y asignarlas a los hosts de XenServer que utilizan actualmente las licencias de Citrix Virtual Apps and Desktops.

Para obtener más información, consulte las preguntas sobre Citrix Virtual Apps and Desktops.

P: Voy a pasar de la versión Technical Preview de XenServer 8 a la versión GA de XenServer 8. ¿Tengo que hacer algo?

R: Quizás. Depende de su licencia.

- Si utiliza una licencia Premium o Standard Edition o utiliza la versión Technical Preview de XenServer 8 sin licencia (Trial Edition), los hosts de XenServer no requieren cambios en las licencias.
- Si utiliza una licencia de Citrix Virtual Apps and Desktops, sus hosts de XenServer muestran esta licencia como obsoleta. Debe obtener una licencia de XenServer Premium Edition para seguir ejecutando las cargas de trabajo de Citrix Virtual Apps and Desktops en XenServer.

Para obtener más información, consulte las preguntas sobre Citrix Virtual Apps and Desktops.

Citrix Virtual Apps and Desktops

P: ¿Qué edición de XenServer necesito para ejecutar las cargas de trabajo de Citrix Virtual Apps and Desktops en XenServer?

R: Para ejecutar las cargas de trabajo de Citrix Virtual Apps and Desktops en XenServer, debe tener una licencia Premium Edition por socket para XenServer. Premium Edition ofrece muchas funciones avanzadas que convierten a XenServer en una plataforma de hipervisor altamente optimizada para su carga de trabajo. Para obtener más información, consulte Ediciones de XenServer.

Para obtener más información sobre cómo obtener una licencia de XenServer, consulte https://xenserver.com/buy.

Los clientes actuales pueden solicitar participar en nuestra promoción y recibir hasta 10 000 licencias de socket de XenServer Premium Edition de forma gratuita. Más información.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

P: Soy cliente de Citrix Virtual Apps and Desktops o Citrix DaaS y estoy pasando de una versión anterior de Citrix Hypervisor a XenServer 8. ¿Tengo que hacer algo?

R: Sí. Antes de intentar actualizar a XenServer 8, debe obtener las licencias de XenServer Premium Edition, importarlas al servidor de licencias de Citrix y asignarlas a los hosts de XenServer que utilizan actualmente las licencias de Citrix Virtual Apps and Desktops.

Para obtener más información sobre cómo obtener una licencia de XenServer, consulte https://xenserver.com/buy. Los clientes actuales pueden solicitar participar en nuestra promoción y recibir hasta 10 000 licencias de socket de XenServer Premium Edition de forma gratuita. Más información.

Este comportamiento es diferente al de las versiones anteriores de Citrix Hypervisor y XenServer. Citrix Hypervisor 8.2 Cumulative Update 1 y versiones anteriores estaban disponibles por derecho para los clientes de Citrix Virtual Apps and Desktops.

P: Soy un Citrix Service Provider con licencia para Citrix Virtual Apps and Desktops o Citrix DaaS. ¿Puedo usar esta licencia para XenServer cuando actualice a XenServer 8?

R: No. Antes de intentar actualizar a XenServer 8, debe obtener las licencias de XenServer Premium Edition, importarlas al servidor de licencias de Citrix y asignarlas a los hosts de XenServer que utilizan actualmente las licencias de Citrix Virtual Apps and Desktops.

Para obtener más información sobre cómo obtener una licencia de XenServer, consulte https://xenserver.com/buy. Los clientes actuales pueden solicitar participar en nuestra promoción y recibir hasta 10 000 licencias de socket de XenServer Premium Edition de forma gratuita. Más información.

Este comportamiento es diferente al de las versiones anteriores de Citrix Hypervisor y XenServer. Citrix Hypervisor 8.2 Cumulative Update 1 y versiones anteriores estaban disponibles por derecho para los clientes de Citrix Virtual Apps and Desktops.

P: Soy un cliente con una suscripción a Citrix DaaS. ¿Tengo derecho a usar XenServer 8?

R: No. Debe obtener licencias de XenServer Premium Edition, importarlas al servidor de licencias de Citrix y asignarlas a los hosts de XenServer.

Para obtener más información sobre cómo obtener una licencia de XenServer, consulte https://xenserver.com/buy. Los clientes actuales pueden solicitar participar en nuestra promoción y recibir hasta 10 000 licencias de socket de XenServer Premium Edition de forma gratuita. Más información.

Este comportamiento es diferente al de las versiones anteriores de Citrix Hypervisor y XenServer. La actualización CU 1 de Citrix Hypervisor 8.2 y las versiones anteriores estaban disponibles por derecho para los clientes de Citrix DaaS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

P: ¿Cuáles son las restricciones en cuanto al uso de las funciones avanzadas de administración de la virtualización de XenServer que se ofrecen como parte de Citrix Virtual Apps and Desktops?

R: Para ejecutar las cargas de trabajo de Citrix Virtual Apps and Desktops en XenServer, necesita una licencia Premium Edition. Premium Edition ofrece muchas funciones avanzadas que convierten a XenServer en una plataforma de hipervisor altamente optimizada para su carga de trabajo.

Para obtener información sobre las funciones avanzadas que ofrece XenServer para Citrix Virtual Apps and Desktops, consulte Uso de XenServer con productos Citrix.

Para obtener más información sobre cómo obtener una licencia de XenServer, consulte https://xenserver.com/buy. Los clientes actuales pueden solicitar participar en nuestra promoción y recibir hasta 10 000 licencias de socket de XenServer Premium Edition de forma gratuita. Más información.

Servidores de licencias Citrix

P: ¿Qué servidores de licencias puedo usar con XenServer?

R: Puede utilizar la versión 11.16 o posterior del software Citrix License Server en un servidor que ejecute Microsoft Windows.

En versiones anteriores, admitimos un dispositivo virtual de servidor de licencias basado en Linux. Este producto ya no es compatible. Si utiliza el dispositivo virtual del servidor de licencias con un grupo existente, migre a la última versión de Citrix License Server para Windows antes de actualizar a XenServer 8.

P: ¿Cómo puedo importar mi licencia en el servidor de licencias de Citrix?

R: Para obtener información sobre la importación de un archivo de licencia, consulte la documentación de Citrix Licensing.

P: ¿Puedo ejecutar el servidor de licencias en mi grupo de XenServer?

R: Sí. Puede instalar el software Citrix License Server en una VM Windows.

XenServer funciona con una licencia "estándar"hasta que el servidor de licencias pueda arrancar. Este comportamiento significa que, después de haber licenciado los hosts de XenServer de su grupo y de reiniciar el host en el que se ejecuta el servidor de licencias Citrix, se aplica un período de gracia a ese host hasta que se reinicie el servidor de licencias.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

P: ¿Puedo usar la versión para Windows del servidor de licencias de Citrix con XenServer?

R: Sí.

P: ¿Puedo instalar licencias para productos Citrix en el software Citrix License Server instalado en Windows?

R: Sí, puede licenciar los productos Citrix mediante el software Citrix License Server instalado en Windows. Para obtener más información, consulte Licencias en el sitio web de documentación de productos Citrix.

Licenciar un grupo de XenServer

P: ¿Cómo aplico una licencia a todos los hosts que usan XenCenter?

R: Siga este procedimiento para aplicar una licencia:

1. En el menú **Herramientas**, haga clic en **Administrador de licencias**.
2. Seleccione el grupo o los hosts que quiera licenciar y, a continuación, haga clic en **Asignar licencia**.
3. En el cuadro de diálogo **Aplicar licencia**, especifique el tipo de **edición** que quiere asignar al host y escriba el nombre de host o la dirección IP del servidor de licencias.

P: ¿Puedo aplicar una licencia sin usar XenCenter?

R: Sí, puede usar la CLI xe. Ejecute el comando `host-apply-edition`. Por ejemplo, introduzca lo siguiente para obtener la licencia de un host:

```
1     xe host-apply-edition edition=enterprise-per-socket|standard-per-
         socket  \
2
3         license-server-address=<license_server_address> host-uuid=<
             uuid_of_host>  \
4
5         license-server-port=<license_server_port>
6 <!--NeedCopy-->
```

Para licenciar un grupo, utilice el comando `pool-apply-edition`. Por ejemplo, introduzca lo siguiente para licenciar un grupo:

```
1     xe pool-apply-edition edition=enterprise-per-socket|standard-per-
         socket  \
2
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
        license-server-address=<license_server_address> host-uuid=<
            uuid_of_host>  \

        license-server-port=<license_server_port>
<!--NeedCopy-->
```

P: ¿Cómo puedo averiguar el estado de las licencias de mis hosts y grupos?

R: XenCenter muestra el tipo de licencia de un host o grupo.

Para ver el tipo de licencia de un host o grupo, seleccione ese host o grupo en la vista de árbol. XenCenter muestra el estado de la licencia en la barra de título de ese host o grupo, después del nombre del host o grupo.

También puede ir a la ficha **General** del host y buscar el tipo de licencia en la sección **Detalles de la licencia**.

Para encontrar el tipo de licencia de un host mediante la línea de comandos, ejecute el siguiente comando en la consola de un host de su grupo:

```
xe host-license-view host\_uuid=<UUID> | grep sku\_marketing\_name
```

Más información

- Para obtener más información sobre la versión 8 de XenServer, consulte las notas de la versión de XenServer8.
- Para acceder a la documentación del producto de XenServer 8, consulte la documentación del producto de XenServer8.
- Para obtener información general sobre el producto XenServer, consulte Descripción técnica.
- Para obtener información sobre asistencia técnica, consulte https://xenserver.com/support.

---

layout: doc
description: Install XenServer directly on a dedicated 64-bit x86 server. Set up XenCenter on a Windows system and connect it to your XenServer hosts.—

Instalación

XenServer se instala directamente en hardware completo, lo que evita la complejidad, la sobrecarga y los cuellos de botella de rendimiento de un sistema operativo subyacente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

XenServer usa los controladores de dispositivo disponibles en el núcleo de Linux. Como resultado, XenServer puede ejecutarse en una amplia variedad de dispositivos de almacenamiento y hardware. Sin embargo, asegúrese de utilizar controladores de dispositivo certificados. Para obtener más información, consulte la Lista de compatibilidad de hardware (HCL).

> **Importante:**
>
> El host XenServer debe instalarse en un servidor x86 dedicado de 64 bits. No instale ningún otro sistema operativo en una configuración de arranque doble con el host XenServer. No se admite esta configuración.

Esta sección está dirigida principalmente a los administradores de sistemas que desean configurar los hosts de XenServer en servidores físicos. Contiene procedimientos que le guiarán a través del proceso de instalación o actualización. También contiene información sobre la solución de problemas que pueden producirse durante la instalación y le indica recursos adicionales.

Antes de comenzar

Según el entorno, el método de instalación que se debe utilizar para que los hosts y grupos tengan la versión más reciente de XenServer 8 varía.

- Si ya tiene instalado Citrix Hypervisor 8.2 CU 1 en sus hosts y grupos, actualice desde Citrix Hypervisor 8.2 CU 1.
- Si ya ha instalado XenServer 8 (incluso durante el período de Technical Preview), no puede actualizar ni actualizar versión desde las imágenes ISO de instalación. En su lugar, aplique el nivel más reciente de actualizaciones frecuentes a través de XenCenter. Para obtener más información, consulte Aplicar actualizaciones.
- Si ya está ejecutando cualquier otra versión de XenServer o Citrix Hypervisor en sus hosts y grupos, no se admite la actualización desde estas versiones. Realice una instalación nueva de XenServer 8.
- Si va a instalar XenServer por primera vez en sus hosts y grupos, realice una instalación nueva de XenServer 8.

Métodos de instalación

XenServer 8 se puede instalar de una de las siguientes maneras:

Instalación nueva Si va a crear una instalación nueva de XenServer 8:

- Utilice el archivo **ISO de instalación de XenServer 8** . Puede descargar este archivo desde la página de descargas de XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Consulte la información en Requisitos del sistema, licencias de XenServer e Instalación de XenServery XenCenter antes de instalar XenServer .

Actualizaciones Si va a actualizar de la actualización acumulativa 1 de Citrix Hypervisor 8.2 a XenServer 8:

- Utilice el archivo **ISO de instalación de XenServer 8** . Puede descargar este archivo desde la página de descargas de XenServer.
- Revise la información presente en Requisitos del sistema, Licencias de XenServer y Actualización desde una versión existente antes de actualizar la versión de XenServer.

El instalador presenta la opción de actualizar cuando detecta una versión de XenServer previamente instalada. El proceso de actualización sigue el proceso de instalación por primera vez, pero se omiten varios pasos de configuración. Se conservan los ajustes existentes, incluida la configuración de red, la hora del sistema, etc.

No puede actualizar directamente desde versiones no compatibles de XenServer o Citrix Hypervisor a XenServer 8. En su lugar, realice una instalación nueva.

Actualización Las instalaciones existentes de XenServer 8 reciben las actualizaciones más recientes mediante el mecanismo de actualización frecuente. Para obtener más información, consulte Aplicar actualizaciones.

Modos de arranque compatibles

XenServer admite el arranque de los hosts mediante el modo de arranque UEFI o BIOS. El arranque seguro UEFI no está disponible actualmente para los hosts de XenServer.

> **Nota:**
>
> El arranque de los hosts de XenServer en modo BIOS ahora está en desuso. Aún puede instalar los hosts de XenServer 8 en el modo de arranque de la BIOS. Sin embargo, esto puede impedir que actualice los hosts de XenServer 8 a una versión futura de XenServer. Se recomienda instalar los hosts de XenServer 8 mediante el modo de arranque UEFI.

El modo de arranque del servidor cambia la forma de iniciar el proceso de instalación. Una vez iniciado el instalador, el proceso de instalación es el mismo para ambos modos de arranque.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Instalar el host de XenServer

Este procedimiento le ayudará a realizar una instalación manual desde un medio local. Para obtener información sobre otros tipos de instalación, como la instalación en red, la instalación desatendida o el arranque desde una SAN, consulte Otros casos de instalación.

> **Sugerencia:**
>
> Durante la instalación, avance rápidamente a la siguiente pantalla pulsando **F12**. Use la tecla **Tab** para moverse entre los elementos y **el espacio** o **Entrar** para seleccionar. Presione **F1** para obtener ayuda general.

Para instalar un host de XenServer:

1. Realice copias de seguridad de los datos que quiera conservar. La instalación de XenServer sobrescribe los datos de los discos duros que seleccione para usar en la instalación.
2. Arranque el equipo desde el medio de instalación:
   - Para instalar el host XenServer desde un USB de arranque:
     a) Cree un USB de arranque desde la ISO de instalación de XenServer. Asegúrese de que la herramienta no altere el contenido del archivo ISO.
        - En Linux, puede usar el comando `dd` para escribir la imagen ISO en una unidad USB. Por ejemplo, `dd if=<path_to_source_iso> of=<path_to_destination_usb>`.
        - En Windows, puede usar Rufus. Asegúrese de seleccionar la **escritura en el modo de imagen DD**. Si no se selecciona, Rufus puede alterar el contenido del archivo ISO y hacer que no arranque.

     b) Inserte la unidad USB de arranque en el sistema de destino.

     c) Reinicie el sistema.

     d) Ve al menú de arranque.

     e) Cambie la configuración para iniciar el sistema desde el USB.

        (Si es necesario, consulte la documentación del proveedor de hardware para obtener información sobre cómo cambiar el orden de arranque)

   - Para instalar el host XenServer desde un CD/DVD:
     a) Grabe el archivo ISO de instalación de XenServer en un CD/DVD.

     b) Inserte el CD/DVD de arranque en la unidad de CD/DVD del sistema de destino.

     c) Reinicie el sistema.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

d) Ve al menú de arranque.

e) Cambie la configuración para iniciar el sistema desde el CD/DVD.

(Si es necesario, consulte la documentación del proveedor de hardware para obtener información sobre cómo cambiar el orden de arranque)

- Para instalar el host XenServer desde un medio virtual:

a) Vaya a la consola virtual de su sistema.

b) Inserte el archivo ISO de instalación de XenServer como medio virtual.

c) Reinicie el sistema.

d) Ve al menú de arranque.

e) Cambie la configuración para iniciar el sistema desde el medio virtual.

(Si es necesario, consulte la documentación del proveedor de hardware para obtener información sobre cómo cambiar el orden de arranque)

- Para obtener información sobre la instalación en red, consulte Otros casos de instalación.

3. Tras los mensajes de arranque iniciales y la pantalla de **bienvenida a XenServer**, seleccione el mapa de teclas (distribución del teclado) para la instalación.

> **Nota:**
>
> Si aparece una pantalla de advertencia de hardware del sistema y el soporte de asistencia de virtualización de hardware está disponible en el sistema, consulte con el fabricante del hardware para obtener actualizaciones de BIOS.

4. En la pantalla **Bienvenido a la configuración de XenServer**, XenServer ofrece las siguientes opciones:

- **Para cargar un controlador de dispositivo, pulse <F9>**

  XenServer incluye un amplio conjunto de controladores que admite la mayoría de las configuraciones de hardware de servidor modernas. Sin embargo, es posible que necesite aplicar discos de controladores (un tipo de paquete complementario) para poder realizar la instalación de XenServer. Si se le ha proporcionado algún controlador de dispositivo esencial adicional, presione F9. El instalador le guiará en la carga de los controladores necesarios.

  > **Advertencia:**
  >
  > No puede instalar otros tipos de paquetes complementarios en este momento

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> del proceso de instalación. Puede instalarlos junto con discos de controladores adicionales cerca del final del proceso de instalación.

- **Para configurar clases de almacenamiento avanzadas, pulse <F10>**

  Si ha realizado la configuración necesaria en su infraestructura de red, puede configurar la instalación de XenServer para que arranque desde el software FCoE (obsoleto). Pulse F10 y siga las instrucciones que aparecen en la pantalla para configurar el FCoE del software. Para obtener más información, consulte Otros casos de instalación.

Una vez que haya completado los pasos necesarios en esta página, seleccione **Aceptar** para continuar.

5. Desplácese y lea el Acuerdo de usuario final (EUA) de XenServer. Selecciona **Aceptar EUA** para continuar.

   Si decide no aceptar la EUA, no podrá continuar con la instalación.

6. Seleccione la acción adecuada de la lista. Esta lista siempre incluye:

   - **Realizar una instalación limpia**: seleccione esta opción para continuar con una instalación nueva.

   Según el estado del servidor, es posible que también veas las siguientes opciones:

   - **Actualización**: si el instalador detecta una versión previamente instalada de XenServer o Citrix Hypervisor, ofrece la opción de actualizarla. Para obtener información sobre cómo actualizar el host de XenServer, consulte Actualización desde una versión existente.
   - **Restaurar**: si el instalador detecta una instalación de respaldo creada anteriormente, ofrece la opción de restaurar XenServer a partir de una copia de seguridad.

   Haga su selección y elija **Aceptar** para continuar.

7. Si tiene varios discos duros locales, elija un disco principal para la instalación. Seleccione **OK**.

8. Elija qué discos quiere usar para el almacenamiento de máquinas virtuales. Para ver información sobre un disco específico, presione **F5**. Seleccione **OK**.

9. Si seleccionó discos que tienen bloques de 512 bytes, tiene la opción de usar el aprovisionamiento ligero para optimizar el uso del almacenamiento disponible. Seleccione **Habilitar el aprovisionamiento ligero** para permitir el uso de la SR local del host para el almacenamiento en caché local de las VDI de VM. Se recomienda a los usuarios de Citrix Virtual Desktops y DaaS que seleccionen esta opción para que el almacenamiento en caché local funcione correctamente. Para obtener más información, consulte Almacenamiento.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Si seleccionó discos nativos de 4 KB, el almacenamiento de la máquina virtual se configurará automáticamente para un bloque de disco de gran tamaño.

Seleccione **Aceptar** para continuar.

10. Seleccione la fuente de medios de instalación.

    - Para realizar la instalación desde un USB, un CD o un medio virtual, selecciona **Medio local**.
    - Para realizar la instalación desde la red, seleccione **HTTP**, **FTP** o **NFS**.

    Seleccione **Aceptar** para continuar.

11. Si selecciona HTTP, FTP o NFS en el paso anterior, configure la red para que el instalador pueda conectarse a los archivos multimedia de instalación de XenServer:

    a) Si el equipo tiene varias NIC, seleccione una de ellas para utilizarla para acceder a los archivos multimedia de instalación de XenServer. Presione **Aceptar** para continuar.

    b) Elija **Configuración automática (DHCP)** para configurar la NIC mediante DHCP o Configuración estática para configurar la NIC manualmente. Si elige **Configuración estática**, introduzca los detalles según corresponda.

    c) Proporcione el identificador de VLAN si tiene los medios de instalación presentes en una red VLAN.

    d) Si elige **HTTP** o **FTP**, proporcione la URL de su repositorio HTTP o FTP, así como un nombre de usuario y una contraseña, si procede.

    Si elige **NFS**, proporcione el servidor y la ruta de su recurso compartido NFS.

    e) Presione **Aceptar** para continuar.

    Para obtener más información sobre la configuración de los medios de instalación en NFS, FTP o HTTP, consulte Otros casos de instalación.

12. Indique si quiere comprobar la integridad de los medios de instalación. Si selecciona **Verificar origen de instalación**, la suma de comprobación SHA256 de los paquetes se calcula y se compara con el valor conocido. La verificación puede llevar algún tiempo. Haga su selección y elija **Aceptar** para continuar.

13. Establezca y confirme una contraseña raíz, que XenCenter usa para conectarse al host de XenServer. También utiliza esta contraseña (con el nombre de usuario "root") para iniciar sesión en **xsconsole**, la consola de configuración del sistema.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Las contraseñas raíz de XenServer solo deben contener caracteres ASCII.

14. Configure la interfaz de administración principal que utiliza XenCenter para conectarse al host y administrarlo.

    Si su equipo tiene varias NIC, seleccione la NIC que desee usar para la administración. Presione **Aceptar** para continuar.

15. Configure la interfaz de administración con las siguientes opciones:

    - Elija **Configuración automática (DHCP)** para configurar la NIC mediante DHCP.
    - Elija **Configuración estática** para configurar la NIC manualmente. Proporcione una dirección IP, una máscara de subred y una puerta de enlace.
    - Seleccione **Usar VLAN** para tener la interfaz de administración en una red VLAN. Proporcione el ID de VLAN.

    > **Nota:**
    >
    > Para formar parte de un grupo, los hosts de XenServer deben tener direcciones IP estáticas o ser direccionables por DNS. Cuando utilice DHCP, asegúrese de que exista una directiva de reserva DHCP estática.

16. Especifique el nombre de host y la configuración de DNS.

    a) En la sección **Configuración del nombre de host**, seleccione una de las siguientes opciones:

    - Seleccione **Configurar automáticamente mediante DHCP** para que el servidor DHCP proporcione el nombre de host junto con la dirección IP.
    - Elija **Especificar manualmente** para definir usted mismo el nombre de host. Introduzca el nombre de host del servidor en el campo correspondiente.

    > **Nota:**
    >
    > Si especifica el nombre de host manualmente, introduzca un nombre de host corto y *no el nombre de dominio completo (FQDN)*. La introducción de un FQDN puede provocar un error en la autenticación externa o puede que el host de XenServer se agregue a Active Directory con un nombre diferente.

    a) En la sección **Configuración de DNS**, seleccione una de las siguientes opciones:

    - Elija **Establecer automáticamente mediante DHCP** para obtener la configuración del servicio de nombres mediante DHCP.
    - Seleccione **Especificar manualmente** para definir usted mismo los servidores DNS. Introduzca las direcciones IP de sus servidores DNS principal (obligatorio), secundario (opcional) y terciario (opcional) en los campos correspondientes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Seleccione **Aceptar** para continuar.

17. Seleccione su zona horaria por área geográfica y ciudad. Puede escribir la primera letra de la configuración regional deseada para saltar a la primera entrada que comienza por esta letra. Presione **Aceptar** para continuar.

18. Especifique cómo quiere que el host de XenServer determine la hora local. XenServer ofrece las siguientes opciones:

    - **Uso de NTP**: seleccione esta opción para usar el protocolo NTP para configurar la hora del servidor. En la siguiente pantalla, configúrelo de una de las siguientes maneras:

      – Seleccione **NTP configurado por mi servidor DHCP** para que su red proporcione el nombre de host o la dirección IP del servidor NTP.

      – Introduzca manualmente al menos un nombre o dirección IP de servidor NTP.

      Presione **Aceptar** para continuar.

    - **Entrada manual de hora**: seleccione esta opción para configurar la fecha y la hora manualmente.

      En la siguiente pantalla, introduce la hora actual en UTC.

      Presione **Aceptar** para continuar.

    > **Nota:**
    >
    > XenServer asume que la configuración de hora del servidor es la hora actual en UTC.

    Presione **Aceptar** para continuar.

19. Seleccione **Instalar XenServer**.

    Se inicia el proceso de instalación. Este proceso puede tardar algunos minutos.

20. La siguiente pantalla le preguntará si desea instalar algún paquete complementario (incluidos los discos de controladores).

    > **Nota:**
    >
    > Si ya cargó un disco de controlador durante la instalación inicial, es posible que se le pida que vuelva a insertar el disco de controlador para poder instalarlo en el disco. En este punto, vuelva a insertar el disco del controlador para asegurarse de que la instancia de XenServer contiene el nuevo controlador.

    - Si quiere instalar paquetes adicionales o discos de controladores proporcionados por su proveedor de hardware, elija **Sí**.

      a) Se le solicitará que inserte el paquete suplementario. Extraiga el medio de instalación de XenServer e inserte el medio del paquete complementario.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

b) Elija **Aceptar**.

c) Seleccione **Usar medios** para continuar con la instalación.

d) Repita para instalar cada paquete.

- Si no quiere instalar un paquete complementario, elija **No**.

  Se completa el proceso de instalación. Este proceso puede tardar unos minutos.

21. Cuando aparezca la pantalla **Instalación completa, extraiga** el soporte de instalación (si se instala desde un USB o un CD).
22. Seleccione **Aceptar** para reiniciar el host.

Una vez reiniciado el host, XenServer **muestra**xsconsole, una consola de configuración del sistema. Para acceder a un shell local desde **xsconsole**, presione **Alt+F3**; para volver a **xsconsole**, presione **Alt+F1**.

> **Nota:**
>
> Anote la dirección IP que se muestra. Use esta dirección IP cuando conecte XenCenter al host XenServer.

Instale XenCenter

XenCenter debe instalarse en una máquina Windows que pueda conectarse al host de XenServer a través de la red. Asegúrese de que la versión 4.8 o una posterior de .NET Framework esté instalada en este sistema.

Para instalar XenCenter:

1. Descargue el instalador de la versión más reciente de XenCenterdesde la página de descargas de XenServer.
2. Inicie el archivo `.msi` del instalador.
3. Siga el asistente **de configuración**, que le permite modificar la carpeta de destino predeterminada y, a continuación, instalar XenCenter.

Para obtener más información sobre el uso de XenCenter, consulte la documentación de XenCenter.

Conectar XenCenter al host XenServer

Para conectar XenCenter al host de XenServer:

1. Inicie XenCenter. El programa se abre en la ficha **Inicio**.
2. Haga clic en el icono **Agregar nuevo servidor**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Introduzca la dirección IP del host de XenServer en el campo **Servidor**. Escriba el nombre de usuario raíz y la contraseña que estableció durante la instalación de XenServer. Haga clic en **Agregar**.
4. La primera vez que agregue un host, aparecerá el cuadro de diálogo **Guardar y restaurar el estado de la conexión**. Este cuadro de diálogo le permite establecer sus preferencias para almacenar la información de conexión de host y restaurar automáticamente las conexiones de host.

   Si más adelante quiere cambiar sus preferencias, puede hacerlo desde el menú principal de XenCenter, seleccionar **Herramientas** y, a continuación, **Opciones**. Se abre el cuadro de diálogo **Opciones**. Seleccione la ficha **Guardar y restaurar** y establezca sus preferencias. Haga clic en **OK** para guardar los cambios.

Conceder licencias a sus hosts de XenServer

Los hosts de XenServer recién instalados pueden ejecutarse en Trial Edition sin una licencia. Esta edición restringe el tamaño del grupo y no permite la actualización sucesiva del grupo a través de XenCenter. Para obtener más información, consulte http://www.xenserver.com/editions.

Para obtener información sobre la concesión de licencias a los hosts de XenServer, consulte Licencias de XenServer.

---

layout: doc
h3InToc: true
description: Configure your servers to enable PXE booting of XenServer host installations, boot from SAN, or unattended installation.—

Otros casos de instalación

Además de un proceso de instalación manual estándar, XenServer ofrece la posibilidad de realizar otros tipos de instalaciones, incluidas las siguientes:

- Instalaciones de red mediante arranque PXE
- Instalaciones desatendidas
- Configuración del host para que arranque desde el SAN
- Configuración de múltiples rutas de host

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Modos de arranque compatibles

XenServer admite el arranque de los hosts mediante el modo de arranque UEFI o BIOS. El arranque seguro UEFI no está disponible actualmente para los hosts de XenServer.

> **Nota:**
>
> El arranque de los hosts de XenServer en modo BIOS ahora está en desuso. Aún puede instalar los hosts de XenServer 8 en el modo de arranque de la BIOS. Sin embargo, esto puede impedir que actualice los hosts de XenServer 8 a una versión futura de XenServer. Se recomienda instalar los hosts de XenServer 8 mediante el modo de arranque UEFI.

El modo de arranque del servidor cambia la forma de iniciar el proceso de instalación. Una vez iniciado el instalador, el proceso de instalación es el mismo para ambos modos de arranque.

Al actualizar los hosts de XenServer, asegúrese de que la actualización utilice el mismo modo de arranque que la instalación inicial.

Instalación de red

Si el servidor en el que quiere realizar la instalación tiene una tarjeta Ethernet con arranque PXE, puede utilizar esta función para realizar una instalación en red con arranque PXE.

El uso del arranque PXE para realizar la instalación desde la red implica los siguientes pasos:

- Copie los archivos de instalación en un servidor TFTP y configure los servidores TFTP y DHCP para la instalación de arranque PXE. El método para hacerlo depende del modo de arranque: BIOS o UEFI.
- Aloje los medios de instalación en NFS, FTP o HTTP. Solo se accede a los archivos de instalación desde el servidor TFTP. Los archivos de XenServer que se van a instalar en el servidor se alojan en un servidor NFS, FTP o HTTP. Como alternativa, después de iniciar la instalación mediante el arranque PXE, puede completarla desde un medio local alojado en el servidor de destino.
- Cree un archivo de respuesta para la instalación desatendida. En su lugar, puede optar por realizar una instalación asistida y recorrer el instalador manualmente.
- Inicie el proceso de instalación.

> **Nota:**
>
> El arranque PXE no se admite en una red VLAN etiquetada. Asegúrese de que la red VLAN que utiliza para el arranque PXE no esté etiquetada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configure sus servidores TFTP y DHCP

Antes de configurar los medios de instalación de XenServer, configure los servidores TFTP y DHCP. Las siguientes secciones contienen información sobre cómo configurar el servidor TFTP para el arranque PXE con BIOS o UEFI. Consulte la documentación de su proveedor para conocer los procedimientos generales de configuración.

Configure su servidor TFTP para el arranque PXE con BIOS

> **Nota:**
>
> El arranque de los hosts de XenServer en modo BIOS ahora está en desuso. Se recomienda instalar los hosts de XenServer 8 mediante el modo de arranque UEFI.

Aloje los archivos del instalador en un servidor TFTP y configure el servidor TFTP para habilitar el arranque PXE con el modo de arranque de BIOS. Esta configuración se utiliza para iniciar el proceso de instalación.

1. En el directorio raíz de TFTP (por ejemplo, `/tftpboot`), cree un directorio llamado `xenserver`.
2. Desde el medio de instalación de XenServer, copie los archivos `mboot.c32` y `pxelinux.0` del directorio `/boot/pxelinux` del medio de instalación al directorio raíz de TFTP.

   > **Nota:**
   >
   > Se recomienda encarecidamente utilizar archivos `mboot.c32` y `pxelinux.0` del mismo origen (por ejemplo, de la misma ISO de instalación de XenServer).

3. Desde el medio de instalación de XenServer, copie los archivos en el nuevo `xenserver` directorio del servidor TFTP:

   - `install.img` desde el directorio raíz
   - `vmlinuz` del directorio `/boot`
   - `xen.gz` del directorio `/boot`

4. En el directorio raíz de TFTP (por ejemplo, `/tftpboot`), cree un directorio llamado `pxelinux.cfg`.
5. En el directorio `pxelinux.cfg`, cree su archivo de configuración llamado **`default`**.

   El contenido de este archivo depende de cómo quiera configurar el entorno de arranque PXE y de los valores adecuados para los servidores.

   - **Ejemplo: instalación desatendida** Este ejemplo de configuración realiza una instalación desatendida mediante el archivo de respuesta en la URL especificada:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    default xenserver-auto
    label xenserver-auto
        kernel mboot.c32
        append xenserver/xen.gz dom0_max_vcpus=1-16 \
            dom0_mem=max:8192M com1=115200,8n1 \
            console=com1,vga ---  xenserver/vmlinuz \
            console=hvc0 console=tty0 \
            answerfile=<http://pxehost.example.com/
               answer_file> \
            answerfile_device=<device> \
            install ---  xenserver/install.img
<!--NeedCopy-->
```

> **Nota:**
>
> Para especificar qué adaptador de red utilizar para recuperar el archivo de respuesta, incluya el parámetro`answerfile_device=ethX` o `answerfile_device=MAC` y especifique el número de dispositivo Ethernet o la dirección MAC del dispositivo.

Para obtener más información sobre el uso de un archivo de respuesta, consulte Crear un archivo de respuesta para una instalación desatendida.

- **Ejemplo: instalación manual** Este ejemplo de configuración inicia una instalación que se inicia desde el servidor TFTP y requiere respuestas manuales:

```
    default xenserver
    label xenserver
        kernel mboot.c32
        append xenserver/xen.gz dom0_max_vcpus=1-16 \
        dom0_mem=max:8192M com1=115200,8n1 \
        console=com1,vga ---  xenserver/vmlinuz \
        console=hvc0 console=tty0 \
        ---  xenserver/install.img
<!--NeedCopy-->
```

Para obtener más información sobre el contenido del archivo de configuración de PXE, consulte el sitio web de SYSLINUX.

Paso siguiente: aloje los medios de instalación en NFS, FTP o HTTP. Además de los servidores TFTP y DHCP, necesita un servidor NFS, FTP o HTTP para alojar los archivos de XenServer que están instalados en el servidor.

Configure su servidor TFTP para el arranque PXE con UEFI Aloje los archivos del instalador en un servidor TFTP y configure los servidores DHCP y TFTP para habilitar el arranque PXE con el modo de arranque UEFI. Esta configuración se utiliza para iniciar el proceso de instalación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. En el directorio raíz de TFTP (por ejemplo, `/tftpboot`), cree un directorio llamado `EFI/xenserver`.
2. Copie los siguientes archivos del medio de instalación de XenServer al nuevo `EFI/xenserver` directorio del servidor TFTP:
   - `grubx64.efi` del directorio `/EFI/xenserver`
   - `install.img` desde el directorio raíz
   - `vmlinuz` del directorio `/boot`
   - `xen.gz` del directorio `/boot`
3. Configure el servidor DHCP para que proporcione `/EFI/xenserver/grubx64.efi` como archivo de arranque.
4. En el `EFI/xenserver` directorio del servidor TFTP, cree el `grub.cfg` archivo.

   El contenido de este archivo depende de cómo quiera configurar el entorno de arranque PXE y de los valores adecuados para los servidores.

   - **Ejemplo: instalación desatendida** Este ejemplo de configuración realiza una instalación desatendida mediante el archivo de respuesta en la URL especificada:

```
menuentry "XenServer Install (serial)" {

    multiboot2 /EFI/xenserver/xen.gz dom0_max_vcpus=1-16
       dom0_mem=max:8192M com1=115200,8n1 console=com1,vga
    module2 /EFI/xenserver/vmlinuz console=hvc0 console=tty0
       answerfile_device=eth0 answerfile=http://<ip_address
       >/<path_to_answer_file> install
    module2 /EFI/xenserver/install.img
 }

<!--NeedCopy-->
```

     > **Nota:**
     >
     > Para especificar qué adaptador de red utilizar para recuperar el archivo de respuesta, incluya el parámetro`answerfile_device=ethX` o `answerfile_device=MAC` y especifique el número de dispositivo Ethernet o la dirección MAC del dispositivo.

     Para obtener más información sobre el uso de un archivo de respuesta, consulte Crear un archivo de respuesta para una instalación desatendida.

   - **Ejemplo: instalación manual** Este ejemplo de configuración inicia una instalación que se inicia desde el servidor TFTP y requiere respuestas manuales:

```
menuentry "XenServer Install (serial)" {

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
3       multiboot2 /EFI/xenserver/xen.gz dom0_max_vcpus=1-16
           dom0_mem=max:8192M com1=115200,8n1 console=com1,vga
4       module2 /EFI/xenserver/vmlinuz console=hvc0 console=tty0
5       module2 /EFI/xenserver/install.img
6    }
7
8   <!--NeedCopy-->
```

Paso siguiente: aloje los medios de instalación en NFS, FTP o HTTP. Además de los servidores TFTP y DHCP, necesita un servidor NFS, FTP o HTTP para alojar los archivos de XenServer que están instalados en el servidor.

Aloje sus medios de instalación en NFS, FTP o HTTP

El servidor TFTP aloja los archivos necesarios para iniciar el instalador, pero los archivos que se van a instalar se alojan en un servidor NFS, FTP o HTTP.

También puede usar archivos alojados en NFS, FTP o HTTP para completar una instalación que se haya iniciado desde un medio local del servidor.

1. En el servidor HTTP, FTP o NFS, cree un directorio desde el que se puedan exportar los medios de instalación de XenServer mediante HTTP, FTP o NFS.
2. Copie todo el contenido de los medios de instalación de XenServer en el directorio recién creado en el servidor HTTP, FTP o NFS. Este directorio es el repositorio de instalación.

   > **Nota:**
   >
   > Al copiar los medios de instalación de XenServer, asegúrese de copiar el archivo `.treeinfo` en el directorio recién creado.
   >
   > Si utiliza IIS para alojar los medios de instalación, asegúrese de que el escape doble esté habilitado en IIS antes de extraer la ISO de instalación en él.

Próximo paso:

- Si está completando una instalación desatendida: cree un archivo de respuesta para la instalación desatendida.
- Si utiliza el arranque PXE para iniciar una instalación manual: inicie la instalación de red.

Crear un archivo de respuesta para una instalación desatendida

Para realizar las instalaciones de forma desatendida, cree un archivo de respuesta XML.

Contener todos los nodos dentro de un nodo raíz denominado *instalación*. Al crear el archivo de respuesta, consulte la referencia del archivo de respuesta.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

He aquí un ejemplo de archivo de respuesta:

```
<?xml version="1.0"?>
    <installation srtype="ext">
        <primary-disk>sda</primary-disk>
        <guest-disk>sdb</guest-disk>
        <guest-disk>sdc</guest-disk>
        <keymap>us</keymap>
        <root-password>mypassword</root-password>
        <source type="url">http://pxehost.example.com/xenserver/</
           source>
        <script stage="filesystem-populated" type="url">
          http://pxehost.example.com/myscripts/post-install-script
        </script>
        <admin-interface name="eth0" proto="dhcp" />
        <timezone>Europe/London</timezone>
    </installation>
<!--NeedCopy-->
```

Siguiente paso: iniciar la instalación de la red.

Actualizaciones automatizadas con un archivo de respuestas También puede realizar actualizaciones automatizadas cambiando el archivo de respuesta de manera apropiada.

1. Defina el atributo `mode` del elemento `installation` en `upgrade`.
2. Especifique el disco en el que vive la instalación existente con el elemento `existing-installation`.
3. Deje los elementos `primary-disk` y `guest-disk` sin especificar.

Por ejemplo:

```
<?xml version="1.0"?>
<installation mode="upgrade">
    <existing-installation>sda</existing-installation>
    <source type="url">http://pxehost.example.com/xenserver/</source>
    <script stage="filesystem-populated" type="url">
        http://pxehost.example.com/myscripts/post-install-script
    </script>
</installation>
<!--NeedCopy-->
```

Referencia del archivo de respuesta A continuación se presenta un resumen de los elementos. Todos los valores de nodo son texto, a menos que se indique lo contrario Se indican los elementos requeridos.

`<installation>` **¿Obligatorio?** Sí

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Descripción: el elemento raíz que contiene todos los demás elementos.

Atributos:

`srtype`

El atributo `srtype` puede tener uno de los valores siguientes: `lvm`, `ext`, o `xfs`:

- `lvm` - establezca el tipo de almacenamiento local en LVM.
- `ext` - establezca el tipo de almacenamiento local en EXT4. Esto permite que el almacenamiento en caché local de Citrix Virtual Desktops funcione correctamente. Para obtener más información, consulte Almacenamiento.
- `xfs` - establezca el tipo de almacenamiento local en XFS. Esta opción también le permite crear dispositivos de almacenamiento local con bloques físicos de 4 KB sin necesidad de un tamaño de bloque lógico de 512 bytes.

Para habilitar el aprovisionamiento ligero, puede especificar el atributo `srtype` como `ext` o `xfs`. Si no especifica el atributo `srtype`, el valor predeterminado de `srtype` es `lvm`. Si no especifica el atributo `srtype` pero configura un disco nativo de 4 KB para el almacenamiento local en el archivo de respuesta, el valor predeterminado es `xfs`.

> **Nota:**
>
> No puede usar los tipos de almacenamiento LVM local o EXT3/EXT4 local con bloques físicos de 4 KB. Si intenta especificar `lvm` o `ext` para el atributo `srtype` mientras configura bloques físicos de 4 KB, la configuración del archivo de respuesta se rechazará por ser incompatible.

`mode`

Para cambiar el tipo de instalación para actualizar, especifique un `mode` atributo con el valor `upgrade`. Si no se especifica este atributo, el instalador realiza una instalación nueva y sobrescribe los datos existentes en el servidor.

`<driver-source>` ¿Obligatorio? Sí

Descripción: El código fuente de un paquete complementario que contiene los controladores de dispositivos que el instalador debe cargar e incluir tras la instalación del repositorio principal.

Atributos: ninguno

`<primary-disk>` ¿Obligatorio? Sí

> **Nota:**
>
> Obsoleto para escenarios de actualización.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Descripción: el nombre del dispositivo de almacenamiento en el que está instalado el dominio de control. Este elemento es equivalente a la elección realizada en el paso *Seleccionar disco primario* del proceso de instalación manual.

Atributos: Puede especificar un atributo `guest-storage` con valores posibles `yes` y `no`.
Por ejemplo: `<primary-disk guest-storage="no">sda</primary-disk>`

El valor predeterminado es `yes`. Si lo especifica `no`, puede automatizar un caso de instalación en el que no se cree ningún repositorio de almacenamiento. En este caso, no especifique ninguna clave de disco invitado.

`<guest-disk>` ¿Obligatorio? No

Descripción: El nombre del dispositivo de almacenamiento que se utilizará para almacenar invitados. Use uno de estos elementos para cada disco adicional.

Atributos: ninguno

`<ntp>` ¿Obligatorio? Sí

Descripción:especifica el origen de los servidores NTP. Si no se especifica el `<ntp>`elemento, el valor predeterminado será `manual`si `<ntp-server>`se especifica, `dhcp`si se usa DHCP, en caso contrario **`default`**.

Atributos:

El atributo `source`puede tener uno de los valores siguientes: `dhcp`, **`default`**`manual`, o `none`.

- `dhcp` - usar servidores NTP desde DHCP
- **`default`** - usar servidores NTP predeterminados
- `manual` - utilice los servidores NTP proporcionados; en este caso, se debe especificar al menos `<ntp-server>`una entrada
- `none` - NTP está desactivado

Si `source`es `dhcp`, **`default`**, o `none`, no especifique `<ntp-server>`.

`<ntp-server>` ¿Obligatorio? No

Descripción:especifica uno o más servidores NTP. Debe usarse solo con el `ntp`elemento y el atributo `manual`.

Atributos: ninguno

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

<keymap> **¿Obligatorio?** No

Descripción: El nombre del mapa de teclas que se utilizará durante la instalación. <keymap>us</keymap> El valor predeterminado, us, se tiene en cuenta si no se especifica un valor para este elemento.

Atributos: ninguno

<root-password> **Requerido:** No

Descripción: la contraseña raíz deseada para el host de XenServer. Si no se proporciona una contraseña, se muestra un mensaje cuando se inicia el host por primera vez.

Atributos: Puede especificar un type que sea hash o plaintext

Por ejemplo:

```
<root-password type="hash">hashedpassword</root-password>
<!--NeedCopy-->
```

El valor hash puede usar cualquier tipo de hash admitido por crypt(3) en glibc. El tipo de hash predeterminado es SHA-512.

Puede usar el siguiente código Python para generar una cadena de contraseña con hash para incluirla en el archivo de respuesta:

```
python -c 'import crypt; print(crypt.crypt("mypasswordhere", crypt.
    mksalt(crypt.METHOD_SHA512)))'
<!--NeedCopy-->
```

<source> **Requerido:** sí

Descripción: La ubicación del medio de instalación de XenServer cargado o de un paquete complementario. Este elemento puede aparecer varias veces.

Atributos: El atributo type puede tener uno de los siguientes valores: url, nfs o local.

Si el valor es local, deje el elemento vacío. Por ejemplo,

```
<source type="url">http://server/packages</source>
<source type="local" />
<source type="nfs">server:/packages</source>
<!--NeedCopy-->
```

<script> **Requerido:** No

Descripción: Dónde se encuentra el script posterior a la instalación.

Atributos:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El atributo `stage` puede tener uno de los siguientes valores: `filesystem-populated`, `installation-start` o `installation-complete`.

- Cuando `filesystem-populated` se usa el valor, el script se ejecuta justo antes de desmontar el sistema de archivos raíz (por ejemplo, después de la instalación/actualización, initrds ya creado, etc.). El script recibe un argumento que es el punto de montaje del sistema de archivos raíz.
- Cuando se usa el valor`installation-start`, el script se ejecuta antes de iniciar la secuencia de instalación principal, pero después de que el instalador se haya inicializado, cargado los controladores y procesado el archivo de respuesta. El script no recibe ningún argumento.
- Cuando se usa el valor `installation-complete`, el script se ejecuta después de que el instalador haya finalizado todas las operaciones (y, por lo tanto, se desmonta el sistema de archivos raíz). El script recibe un argumento que tiene un valor de cero si la instalación se ha completado correctamente y no es cero si la instalación ha fallado por cualquier motivo.

El atributo `type` puede tener uno de los siguientes valores: `url`, `nfs` o `local`.

Si el valor es `url` o `nfs`, coloque la ruta URL o NFS en el PCDATA. Si el valor es `local`, deje el PCDATA vacío. Por ejemplo,

```
<script stage="filesystem-populated" type="url">
    http://prehost.example.com/post-install-script
</script>
<script stage="installation-start" type="local">
    file:///scripts/run.sh
</script>
<script stage="installation-complete" type="nfs">
    server:/scripts/installation-pass-fail-script
</script>
<!--NeedCopy-->
```

> **Nota:**
>
> Si se utiliza un archivo local, asegúrese de que la ruta sea absoluta. Por lo general, esto significa que el prefijo `file:` / / va seguido de otra barra inclinada y, a continuación, de la ruta completa del script.

`<admin-interface>` **Obligatorio:** A veces

> **Nota:**
>
> Necesario durante la instalación o reinstalación, pero no durante la actualización o la restauración.

Descripción: La interfaz de red única que se utilizará como interfaz de administración del host.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Atributos:

Especifique uno de los siguientes atributos:

- `name` - El nombre de la interfaz de red, por ejemplo `eth0`.
- `hwaddr` - La dirección MAC de la interfaz de red, por ejemplo `00:00:11:aa:bb:cc`.

El atributo `proto` puede tener uno de los valores siguientes: `dhcp` o **`static`**.

Si lo especifica `proto="static"`, también debe especificar todos estos elementos secundarios:

Elementos secundarios

- `<ipaddr>`: La dirección IP
- `<subnet>`: La máscara de subred
- `<gateway>`: La puerta de enlace

`<timezone>` **Requerido:** No

Descripción: La zona horaria en el formato utilizado por la variable TZ, por ejemplo, Europa/Londres o América/Los_Ángeles. El valor predeterminado es `Etc/UTC`.

`<name-server>` **Requerido:** No

Descripción: La dirección IP de un servidor de nombres. Usa uno de estos elementos para cada servidor de nombres que quieras usar.

`<hostname>` **Requerido:** No

Descripción: especifique este elemento si quiere establecer manualmente un nombre de host.

`<ntp-server>` **Requerido:** No

Descripción: especifique uno o más servidores NTP.

Iniciar la instalación de la red

Tras configurar los servidores de red necesarios para una instalación de arranque PXE, complete los siguientes pasos en el servidor en el que va a realizar la instalación:

1. Inicie el sistema y entre en el menú de arranque (**F12** en la mayoría de los programas de BIOS).
2. Seleccione iniciar desde la tarjeta Ethernet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. A continuación, el sistema PXE se inicia desde la fuente de instalación que ha configurado y se inicia el script de instalación.

    - Si ha configurado un archivo de respuesta, la instalación se realiza sin supervisión.
    - Si ha decidido realizar una instalación manual, proporcione la información cuando se le solicite. Para obtener más información, consulte Instalación.

Arranque desde SAN

Los entornos de arranque desde SAN ofrecen varias ventajas, que incluyen alto rendimiento, redundancia y consolidación del espacio. En estos entornos, el disco de arranque se encuentra en una SAN remota y no en el host local.

Se admiten los siguientes tipos de configuración de arranque desde SAN:

- HBA y Fibre Channel de hardware
- Software FCoE (obsoleto)
- Arranque de software desde iSCSI

Para un entorno de arranque desde SAN totalmente redundante, debe configurar varias rutas para el acceso de E/S. Para obtener más información, consulte Habilitar rutas múltiples.

HBA y Fibre Channel de hardware

Este tipo de implementación de arranque desde SAN depende de las matrices de discos basadas en SAN que admitan el hardware Fibre Channel o el adaptador iSCSI HBA en el host. El host se comunica con la SAN a través de un adaptador de bus de host (HBA). El BIOS de la HBA contiene las instrucciones que permiten al host encontrar el disco de arranque.

Toda la configuración para configurar el arranque desde una SAN a través de un adaptador HBA o Fibre Channel de hardware se realiza en la infraestructura de red antes de instalar XenServer en los servidores. Para obtener información sobre cómo completar esta configuración, consulte la documentación proporcionada por el proveedor.

Una vez que la infraestructura de red esté configurada correctamente, habilite las rutas múltiples en los servidores durante el proceso de instalación de XenServer. Para obtener más información, consulte Habilitar rutas múltiples. Continúe con la instalación con normalidad.

Software FCoE (obsoleto)

Puede arrancar un host XenServer desde una SAN FCoE mediante una pila de software FCoE.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para este tipo de implementación de arranque desde SAN, antes de instalar el host de XenServer, complete manualmente la configuración necesaria para exponer un LUN al host. Esta configuración manual incluye la configuración de la estructura de almacenamiento y la asignación de los LUNs al nombre público mundial (PWWN) de su SAN. Después de completar esta configuración, el LUN disponible se monta en el CNA del host como un dispositivo SCSI. El dispositivo SCSI se puede usar para acceder al LUN como si fuera un dispositivo SCSI conectado localmente. Al configurar la estructura FCoE, no use VLAN 0. El host de XenServer no puede encontrar el tráfico que se encuentra en la VLAN 0.

Para obtener información sobre cómo configurar el conmutador físico y el arreglo de discos para admitir FCoE, consulte la documentación proporcionada por el proveedor.

Una vez que la infraestructura de red esté configurada correctamente, habilite las rutas múltiples en los servidores durante el proceso de instalación de XenServer. Para obtener más información, consulte Habilitar rutas múltiples. Continúe con la instalación con normalidad.

Durante una instalación manual de XenServer, en la pantalla de **bienvenida a XenServer Setup se le ofrece la opción de configurar** clases de almacenamiento avanzadas. Pulse **F10** y siga las instrucciones que aparecen en la pantalla para configurar el FCoE del software.

Arranque de software desde iSCSI

La función de arranque por software desde iSCSI permite a los clientes instalar y arrancar XenServer desde una SAN mediante iSCSI. Con esta función, XenServer se puede instalar, arrancar y ejecutar desde un LUN proporcionado por un destino iSCSI. El destino iSCSI se especifica en la tabla de firmware de arranque iSCSI. Esta capacidad permite que el disco raíz se conecte a través de iSCSI. Este disco de arranque se puede ubicar en el mismo destino que proporciona un SR.

Para utilizar esta función, asegúrese de que su entorno cumpla los siguientes requisitos:

- La interfaz de red o las interfaces dedicadas al arranque iSCSI deben estar separadas de las interfaces de administración y las interfaces utilizadas para el tráfico de máquinas virtuales.
- El almacenamiento (destinos iSCSI) debe estar en una red de capa 3 (IP) separada de todas las demás interfaces de red con direcciones IP en el host.
- No utilice una VLAN etiquetada para las interfaces de red dedicadas a los destinos de arranque iSCSI.
- Le recomendamos que habilite las rutas múltiples en sus servidores.

Para configurar la función de arranque de software desde iSCSI, debe agregar el parámetro a los parámetros de arranque. `use_ibft` La forma de agregar este parámetro depende del modo de arranque y del tipo de instalación que esté realizando.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Habilite la función de arranque por software desde iSCSI en un servidor de arranque UEFI durante una instalación desde un medio local

1. Arranque el equipo desde el medio de instalación. Para obtener más información, consulte Instalar el host de XenServer.

   Tras los mensajes de arranque iniciales, verá un menú de GRUB. Este menú se muestra durante 5 segundos.

2. Use las teclas de cursor para seleccionar una opción de instalación:

   - Para un LUN de ruta única, seleccione **instalar**.
   - Para un LUN con múltiples rutas, seleccione **multiruta** (recomendado).

3. Presione la tecla e para modificar los comandos antes del arranque.

4. Modifique la línea empezando por lo siguiente:

```
module2 /EFI/xenserver/vmlinuz ...
<!--NeedCopy-->
```

   Con las teclas del cursor, modifique esta línea para incluir `use_ibft` al final:

```
module2 /EFI/xenserver/vmlinuz ... use_ibft
<!--NeedCopy-->
```

5. Presiona **Entrar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Continúe con el proceso de instalación del host de XenServer como de costumbre.

Habilite la función de arranque de software desde iSCSI en un servidor de arranque de BIOS durante una instalación desde un medio local

> **Nota:**
>
> El arranque de los hosts de XenServer en modo BIOS ahora está en desuso. Se recomienda instalar los hosts de XenServer 8 mediante el modo de arranque UEFI.

1. Arranque el equipo desde el medio de instalación. Para obtener más información, consulte Instalar el host de XenServer.

   Tras los mensajes de arranque iniciales, verá la pantalla **Bienvenido a XenServer**.

2. En la línea de comandos de arranque, introduzca `menu.c32`.
3. Use las teclas de cursor para seleccionar una opción de instalación:

   - Para un LUN de ruta única, seleccione **instalar**.
   - **Para un LUN con múltiples rutas, seleccione multiruta.**

4. Presione la tecla de tabulación.
5. Modifique la línea que termina con lo siguiente:

   ```
   ---  /install.img
   <!--NeedCopy-->
   ```

   Con las teclas de cursor, modifique esta línea para que diga:

   ```
   use_ibft ---  /install.img
   <!--NeedCopy-->
   ```

6. Presiona **Entrar**.
7. Continúe con el proceso de instalación del host de XenServer como de costumbre.

Habilite la función de arranque por software desde iSCSI en un servidor de arranque UEFI durante una instalación de arranque PXE Al realizar la instalación mediante PXE, asegúrese de agregar la palabra clave **use_ibft** en los parámetros del núcleo. Si se requieren rutas múltiples, debe agregar **device_mapper_multipath=enabled**.

Por ejemplo:

```
menuentry "XenServer Install (serial)" {

    multiboot2 /EFI/xenserver/xen.gz dom0_max_vcpus=1-16 dom0_mem=max
       :8192M com1=115200,8n1 console=com1,vga
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    module2 /EFI/xenserver/vmlinuz console=hvc0 console=tty0
       answerfile_device=eth0 answerfile=http://<ip_address>/<
       path_to_answer_file> install use_ibft device_mapper_multipath=
       enabled
    module2 /EFI/xenserver/install.img
     }

<!--NeedCopy-->
```

Para obtener más información sobre cómo configurar el arranque PXE, consulte Configurar el servidor TFTP para el arranque PXEcon UEFI.

Habilite la función de arranque de software desde iSCSI en un servidor de arranque de BIOS durante una instalación de arranque PXE

> **Nota:**
>
> El arranque de los hosts de XenServer en modo BIOS ahora está en desuso. Se recomienda instalar los hosts de XenServer 8 mediante el modo de arranque UEFI.

Al realizar la instalación mediante PXE, asegúrese de agregar la palabra clave **use_ibft** en los parámetros del núcleo. **Si usa rutas múltiples (recomendado), debe agregar device_mapper_multipath=enabled.**

Por ejemplo:

```
default xenserver-auto
label xenserver-auto
    kernel mboot.c32
    append xenserver/xen.gz dom0_max_vcpus=1-16 \
    dom0_mem=max:8192M com1=115200,8n1 \
    console=com1,vga ---  xenserver/vmlinuz \
    console=hvc0 console=tty0 \
    answerfile=<http://pxehost.example.com/answer_file> \
    answerfile_device=<device> \
    use_ibft device_mapper_multipath=enabled ---  xenserver/install.img
<!--NeedCopy-->
```

Para obtener más información sobre cómo configurar el arranque PXE, consulte Configurar el servidor TFTP para el arranque PXEcon BIOS.

Habilitar multipathing

Para un entorno de arranque desde SAN totalmente redundante, debe configurar varias rutas para el acceso de E/S. Para hacerlo, asegúrese de que el dispositivo raíz tenga habilitada la compatibilidad con múltiples rutas.

Para obtener información acerca de si hay varios paths disponibles para su entorno SAN, consulte a su proveedor o administrador de almacenamiento de información.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Advertencia:**
>
> La configuración de rutas múltiples *no* se hereda durante el proceso de actualización. Al realizar la actualización mediante la ISO o el arranque de red, siga las mismas instrucciones que se utilizan en el siguiente proceso de instalación para asegurarse de que `multipath` está correctamente configurado.

Si tiene varias rutas disponibles, habilite las múltiples rutas en la implementación de XenServer mientras inicializa el proceso de instalación. La forma de habilitar las múltiples rutas depende del modo de arranque y del tipo de instalación que esté realizando.

Habilitar las rutas múltiples en un servidor de arranque UEFI durante una instalación manual

1. Arranque el equipo desde el medio de instalación. Para obtener más información, consulte Instalar el host de XenServer.

   Tras los mensajes de arranque iniciales, verá un menú de GRUB. Este menú se muestra durante 5 segundos.

2. En el menú de GRUB, elija `multipath` y presione **Entrar**.

El proceso de instalación de XenServer configura el host de XenServer, que se inicia desde una SAN remota con las rutas múltiples habilitadas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Habilitar las múltiples rutas en un servidor de arranque de BIOS durante una instalación manual

> **Nota:**
>
> El arranque de los hosts de XenServer en modo BIOS ahora está en desuso. Se recomienda instalar los hosts de XenServer 8 mediante el modo de arranque UEFI.

1. Arranque el equipo desde el medio de instalación. Para obtener más información, consulte Instalar el host de XenServer.

   Tras los mensajes de arranque iniciales, verá la pantalla **Bienvenido a XenServer**.

2. En la pantalla de bienvenida, pulse **F2** para seleccionar Instalación **avanzada**.
3. En la línea de comandos de arranque, introduzca `multipath`.

El proceso de instalación de XenServer configura el host de XenServer, que se inicia desde una SAN remota con las rutas múltiples habilitadas.

Habilitar las rutas múltiples en un servidor de arranque UEFI durante una instalación desatendida Para habilitar las múltiples rutas del sistema de archivos durante la instalación de PXE, agréguelo `device_mapper_multipath=enabled` al archivo de configuración.

Por ejemplo:

```
menuentry "XenServer Install (serial)" {

    multiboot2 /EFI/xenserver/xen.gz dom0_max_vcpus=1-16 dom0_mem=max
       :8192M com1=115200,8n1 console=com1,vga
    module2 /EFI/xenserver/vmlinuz console=hvc0 console=tty0
       answerfile_device=eth0 answerfile=http://<ip_address>/<
       path_to_answer_file> install use_ibft device_mapper_multipath=
       enabled
    module2 /EFI/xenserver/install.img
     }

<!--NeedCopy-->
```

Para obtener más información sobre cómo configurar el arranque PXE, consulte Configurar el servidor TFTP para el arranque PXEcon UEFI.

Habilitar las múltiples rutas en un servidor de arranque de BIOS durante una instalación desatendida

> **Nota:**
>
> El arranque de los hosts de XenServer en modo BIOS ahora está en desuso. Se recomienda instalar los hosts de XenServer 8 mediante el modo de arranque UEFI.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para habilitar las múltiples rutas del sistema de archivos durante la instalación de PXE, agréguelo `device_mapper_multipath=enabled` al archivo de configuración.

Por ejemplo:

```
default xenserver-auto
label xenserver-auto
    kernel mboot.c32
    append xenserver/xen.gz dom0_max_vcpus=1-16 \
    dom0_mem=max:8192M com1=115200,8n1 \
    console=com1,vga ---  xenserver/vmlinuz \
    console=hvc0 console=tty0 \
    answerfile=<http://pxehost.example.com/answer_file> \
    answerfile_device=<device> \
    device_mapper_multipath=enabled \
    install ---  xenserver/install.img
<!--NeedCopy-->
```

Para obtener más información sobre cómo configurar el arranque PXE, consulte Configurar el servidor TFTP para el arranque PXEcon BIOS.

Instalar paquetes complementarios

Los paquetes complementarios se utilizan para modificar y ampliar las capacidades de XenServer mediante la instalación de software en el dominio de control (dom0). Por ejemplo, un socio OEM puede querer enviar XenServer con un conjunto de herramientas de administración que requieren la instalación de agentes SNMP. Puede instalar un paquete complementario durante la instalación inicial de XenServer o en cualquier momento posterior en una instancia de XenServer en ejecución.

Al instalar paquetes complementarios durante la instalación de XenServer, descomprima cada paquete complementario en un directorio independiente de un servidor web.

Puede instalar el paquete complementario de una de las siguientes maneras:

- Durante una instalación interactiva, cuando se le pida que instale paquetes complementarios, especifique la URL del medio del paquete complementario.
- Si utiliza un archivo de respuesta para la instalación, agregue un elemento <`source`> adicional para especificar la ubicación del paquete complementario.

Instalación de discos de controladores

Puede instalar un disco de controladores mediante uno de los métodos siguientes:

- Mediante XenCenter (recomendado)
- Durante una instalación limpia de XenServer

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Mediante la CLI xe

Para obtener información sobre cómo instalar un disco de controlador mediante XenCenter, consulteInstalación de discos de controladores. Para obtener información sobre cómo instalar un disco de controladores durante una instalación limpia de XenServer, consulte Instalar el host de XenServer.

Tras instalar el controlador, reinicie el servidor para que surta efecto la nueva versión del controlador. Al igual que con cualquier actualización de software, le recomendamos que haga una copia de seguridad de los datos antes de instalar un disco de controladores.

Instalación de un disco de controlador mediante la CLI xe

Realice los siguientes pasos para instalar el disco del controlador de forma remota mediante la CLI xe:

1. Descargue el disco del controlador en una ubicación conocida de un equipo que tenga instalada la CLI xe remota.
2. Extrae el contenido del archivo zip.

   Para el siguiente paso, asegúrese de utilizar la ISO del controlador y no la ISO que contiene los archivos fuente.
3. Cargue el disco del controlador:

   ```
   xe [connection_parameters] update-upload file-name=
   <!--NeedCopy-->
   ```

   El UUID del disco del controlador se devuelve cuando finaliza la carga.
4. Aplique el disco del controlador:

   ```
   xe [connection_parameters] update-apply uuid=
   <!--NeedCopy-->
   ```
5. Para completar la instalación, reinicie el host. El controlador no surte efecto hasta que se haya reiniciado el host.

---

layout: doc
description: Upgrade from older versions of XenServer. You can complete the update manually or automatically.—

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Actualización desde la Actualización acumulativa 1 de Citrix Hypervisor 8.2

Al actualizar desde una instalación existente de la actualización acumulativa 1 de Citrix Hypervisor 8.2 a XenServer 8, puede conservar las máquinas virtuales, SR y la configuración existentes.

Realice una actualización progresiva del grupo para mantener disponibles todos los servicios y recursos que ofrece el grupo y, al mismo tiempo, actualice todos los hosts del grupo. Este método de actualización solo desconecta un host de XenServer a la vez. Las máquinas virtuales críticas se mantienen en funcionamiento durante el proceso mediante la migración en vivo de las máquinas virtuales a otros hosts del grupo.

Puede completar una mejora continua de una agrupación de una de las siguientes maneras:

- Si tiene una licencia Premium Edition, puede usar el asistente de actualización de **XenCenter** **Rolling**Pool. Este asistente organiza la ruta de actualización automáticamente y lo guía a través del procedimiento de actualización.

  Para obtener más información, consulte Actualización progresiva de grupos mediante XenCenter.

- Puede usar la CLI xe para realizar una actualización progresiva del grupo de forma manual mediante la migración en vivo de las máquinas virtuales en ejecución entre los hosts de XenServer en consecuencia.

  Para obtener más información, consulte Actualización progresiva de grupos mediante la CLI xe.

¿Puedo actualizar?

Asegúrese de poder actualizar a XenServer 8:

- ¿Sus hosts ejecutan actualmente la actualización acumulativa 1 de Citrix Hypervisor 8.2?

  De lo contrario, no podrá actualizar directamente a XenServer 8. En su lugar, realice una instalación limpia. Para obtener más información, consulte Instalación.

  Si ya usa XenServer 8, no intente actualizar mediante la imagen ISO de instalación. En su lugar, aplique actualizaciones para que su grupo de XenServer 8 alcance el nivel más reciente. Para obtener más información, consulte Aplicar actualizaciones.

- ¿Está utilizando un diseño de particiones compatible?

  El diseño de particiones heredado ya no se admite. Si lo usa, es posible que no pueda actualizar a XenServer 8. Para obtener más información, consulte Diseño de particiones antiguo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- ¿Utiliza el dispositivo virtual Citrix Licensing Server?

  En versiones anteriores, admitíamos el dispositivo virtual del servidor de licencias basado en Linux. Este producto ya no es compatible. Si utiliza el dispositivo virtual del servidor de licencias con un grupo existente, migre a la última versión de Citrix License Server para Windows antes de actualizar a XenServer 8. Para obtener más información, consulte Licencias.

- ¿El tamaño de la clave del certificado de identidad del servidor es inferior a 2048 bytes?

  Si el grupo se instaló por primera vez con XenServer 7.6 o anterior, es posible que aún tenga certificados con un tamaño de clave inferior a 2048 bytes. En este caso, cuando intenta actualizar a XenServer 8, el asistente de actualización muestra un error durante las comprobaciones previas. Para continuar con la actualización, debe restablecer el certificado autofirmado en cada servidor afectado ejecutando el siguiente comando:

  ```
  1  xe host-emergency-reset-server-certificate
  ```

  Este comando puede interrumpir las operaciones en curso en el grupo.

- ¿Su hardware es compatible con XenServer 8?

  Compruebe que el hardware en el que está instalado su grupo sea compatible con la versión de XenServer a la que va a actualizarse. Para obtener más información, consulte la Lista de compatibilidad de hardware (HCL).

- ¿Los sistemas operativos de sus máquinas virtuales son compatibles con XenServer 8?

  Compruebe que los sistemas operativos de sus máquinas virtuales sean compatibles con XenServer 8. Si el sistema operativo de la máquina virtual no es compatible, actualice el sistema operativo de la máquina virtual a una versión compatible antes de actualizar XenServer. Para obtener más información, consulte Compatibilidad con sistemas operativos invitados.

- ¿Utiliza XenServer para alojar sus cargas de trabajo de Citrix Virtual Apps and Desktops?

  Si usa su licencia de Citrix Virtual Apps and Desktops con Citrix Hypervisor 8.2 CU1, esta licencia ya no se aplica a XenServer 8. En su lugar, debe obtener una licencia de Xenserver Premium Edition. Para obtener más información, consulte https://xenserver.com/buy.

  Los clientes actuales pueden solicitar participar en nuestra promoción y recibir hasta 10 000 licencias de socket de XenServer Premium Edition de forma gratuita. Más información.

  Aplique las nuevas licencias al grupo antes de comenzar la actualización.

  Puede actualizar a XenServer 8 mediante los métodos que se describen en este artículo. Sin embargo, según el entorno de XenServer y la carga de trabajo de Citrix Virtual Apps and Desktops, es posible que haya que tener en cuenta comportamientos y requisitos específicos para optimizar el proceso de actualización de XenServer. Para obtener más información, consulte Escenarios de actualización para Citrix Virtual Apps and Desktops.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Antes de comenzar

Revise la siguiente información antes de iniciar la actualización. Tome las medidas necesarias para asegurarse de que el proceso de actualización se lleve a cabo correctamente.

Planifique la actualización

1. Trace su ruta de mejora con cuidado. La actualización de los hosts de XenServer, y en particular de un grupo de hosts de XenServer, requiere una planificación y una atención cuidadosas para evitar perder los datos existentes.

   Tenga en cuenta la siguiente información al planificar la actualización:

   - No puede migrar una máquina virtual de una versión más reciente de XenServer a una anterior.
   - No opere el grupo en modo mixto (con varias versiones de XenServer) durante más tiempo del necesario. El grupo funciona en un estado degradado durante la actualización.
   - Las operaciones de control clave no están disponibles durante el proceso de actualización. No intente realizar ninguna operación de control.
   - No copie, apague ni exporte máquinas virtuales durante el proceso de actualización.
   - No realice operaciones relacionadas con el almacenamiento, como agregar, quitar o cambiar el tamaño de los discos virtuales, durante el proceso de actualización.
   - Durante la actualización del coordinador de la agrupación, los demás hosts de la agrupación entran en *modo de emergencia*.

2. Asegúrese de que sus servidores no estén sobreaprovisionados: compruebe que los servidores tengan suficiente memoria para llevar a cabo la actualización.

   Por lo general, si N es igual al número total de servidores de un grupo, debe haber suficiente memoria en N-1 servidores para ejecutar todas las máquinas virtuales activas del grupo. Es mejor suspender las máquinas virtuales que no sean críticas durante el proceso de actualización.

3. Asegúrese de que su grupo tenga almacenamiento compartido para mantener sus máquinas virtuales en funcionamiento durante una actualización progresiva del grupo. Si su grupo no tiene almacenamiento compartido, debe suspender las máquinas virtuales antes de la actualización, ya que las máquinas virtuales no se pueden migrar en vivo.

   La migración en vivo del almacenamiento no se admite con las actualizaciones progresivas de grupos.

4. Si usa su licencia de Citrix Virtual Apps and Desktops con Citrix Hypervisor 8.2 CU 1, aplique una licencia de Xenserver Premium Edition a todos los hosts del grupo. Para obtener más información, consulte https://xenserver.com/buy.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Si realiza una actualización sucesiva de grupos de Citrix Hypervisor 8.2 CU1 a XenServer 8, no podrá usar Workload Balancing 8.2.2 y versiones anteriores con los grupos de XenServer 8. Actualice su dispositivo virtual Workload Balancing a la versión 8.3.0 antes de realizar la actualización sucesiva del grupo. Puede descargar la versión más reciente del dispositivo virtual Workload Balancing desde la página de descargas de XenServer.
6. Tenga en cuenta los siguientes comportamientos:
    - La actualización debe usar el mismo modo de arranque que la instalación inicial.
    - La configuración de arranque desde SAN *no* se hereda durante el proceso de actualización manual. Al actualizar mediante el proceso ISO o PXE, debe asegurarse de que `multipathd` está correctamente configurado. Para obtener más información, consulte Arrancar desde SAN.
    - Al actualizar XenServer, los paquetes suplementarios aplicados anteriormente se eliminan y, por lo tanto, se deben volver a aplicar durante la actualización o después de ella. Sin embargo, ya no es necesario instalar el paquete complementario PVS-Accelerator en XenServer 8. Sus funciones ahora están incluidas en la instalación principal del producto.

Preparar su agrupación

1. Realice una copia de seguridad del estado de su grupo existente mediante el comando xe de la interfaz de línea de comandos `xe pool-dump-database`.

   La realización de una copia de seguridad del estado garantiza que pueda revertir una actualización sucesiva parcialmente completa a su estado original sin perder los datos de la VM.
2. Inhabilita la alta disponibilidad.

Prepare sus máquinas virtuales

1. Si tiene máquinas virtuales de Windows ejecutándose en su grupo, siga los siguientes pasos para cada máquina virtual:
    - Asegúrese de que esté instalada la versión más reciente de XenServer VM Tools para Windows.
    - Cree una instantánea de la máquina virtual.
2. Si tiene máquinas virtuales Linux ejecutándose en su grupo, asegúrese de que esté instalada la última versión de XenServer VM Tools for Linux.
3. Si tiene máquinas virtuales habilitadas para NVIDIA vGPU ejecutándose en su grupo, complete los siguientes pasos para migrar el grupo mientras estas máquinas virtuales están en ejecución:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a) Asegúrese de que la GPU que está utilizando sea compatible con la versión a la que planea actualizar.
b) Identifique una versión de los controladores NVIDIA GRID que esté disponible tanto para su versión actual de Citrix Hypervisor o XenServer como para la versión de XenServer a la que va a actualizar. Si es posible, elija los controladores más recientes disponibles.
c) Instale los nuevos controladores GRID en los hosts de XenServer y los controladores invitados correspondientes en cualquiera de las máquinas virtuales habilitadas para vGPU.
d) Asegúrese de tener también la versión del controlador GRID que coincida con la versión de XenServer a la que está actualizando. Se le pedirá que instale estos controladores como un paquete complementario como parte del proceso de actualización sucesiva del grupo.

4. Vacíe las unidades de CD/DVD de todas las máquinas virtuales del grupo.

Obtenga los archivos necesarios

1. Si utiliza XenCenter para actualizar los hosts, descargue e instale la versión más reciente de XenCenter desde el sitio de descargas de XenServer.

   Para obtener más información, consulte Instalar XenCenter.

2. Descargue la ISO de instalación de XenServer 8 desde el sitio de descargas de XenServer.

3. Prepare los medios de instalación:

   - Para actualizar sus hosts desde un USB de arranque, utilice una herramienta como `rufus` o `diskpart` cree un USB de arranque mediante la ISO de instalación de XenServer 8. Asegúrese de que la herramienta no altere el contenido del archivo ISO.
   - Para actualizar los hosts desde un CD, grabe el archivo ISO de instalación de XenServer 8 en un CD.
   - Para actualizar los hosts desde un medio virtual, vaya a la consola virtual del sistema y monte el archivo ISO de instalación de XenServer como medio virtual.
   - Para actualizar desde una ubicación de red:

     a) Configure un servidor TFTP accesible a la red desde el que arrancar el instalador.

     b) Configure una ubicación de red en la que pueda acceder a la ISO de instalación a través de HTTP, FTP o NFS.

     c) Descomprima la ISO de instalación en la ubicación de red.

        Si utiliza IIS para alojar los medios de instalación, asegúrese de que el escape doble esté habilitado en IIS antes de extraer la ISO de instalación en él.

     d) Anote la información que necesita durante la actualización:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Para HTTP o FTP, anote la URL de su repositorio HTTP o FTP y un nombre de usuario y contraseña, si corresponde.
- En el caso de NFS, anote el servidor y la ruta de su recurso compartido de NFS.

Para obtener más información, consulte Arranque de red.

Una vez completados estos pasos previos, puede realizar una actualización progresiva del grupo mediante uno de los siguientes métodos:

- Actualización progresiva del grupo mediante XenCenter
- Actualización progresiva de la agrupación mediante la CLI xe

Actualización progresiva del grupo mediante XenCenter

El asistente de **actualización sucesiva** de grupos le guía a través del procedimiento de actualización y organiza la ruta de actualización automáticamente. En el caso de los grupos, cada uno de los servidores del grupo se actualiza por separado, empezando por el coordinador del grupo. Antes de iniciar una actualización, el asistente lleva a cabo una serie de comprobaciones previas. Estas comprobaciones previas garantizan que determinadas funciones del grupo, como la alta disponibilidad, estén inhabilitadas temporalmente y que todos los servidores del grupo estén preparados para la actualización. Solo hay un servidor fuera de línea a la vez. Todas las máquinas virtuales en ejecución se migran automáticamente fuera de cada servidor antes de que se instale la actualización en ese servidor.

> **Nota:**
>
> El asistente de **actualización de XenCenter Rolling Pool** solo está disponible si tiene una licencia Premium Edition.

Si aún no ha instalado XenCenter, descargue la versión más reciente del sitio de descargas de XenServer y siga los pasos que se indican en Instalar XenCenter.

El asistente puede funcionar en modo manual o automático:

- En el modo manual, debe ejecutar manualmente el instalador de XenServer en cada servidor por turno y seguir las instrucciones que aparecen en pantalla en la consola serie del servidor. Cuando comience la actualización, XenCenter le pedirá que inserte el medio de instalación o que especifique un servidor de arranque de red para cada servidor que actualice.
- En modo automático, el asistente usa archivos de instalación de red en un servidor HTTP, NFS o FTP para actualizar cada servidor sucesivamente. Este modo no requiere que insertes medios de instalación, reinicies manualmente ni pases por el instalador en cada servidor. Si realiza una actualización gradual del grupo de esta manera, debe desempaquetar los medios de instalación en el servidor HTTP, NFS o FTP antes de iniciar la actualización.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para actualizar los hosts de XenServer mediante el asistente de actualización gradual de grupos de XenCenter:

1. En el menú **XenCenter** Tools, **seleccione**Rolling Pool Upgrade.
2. Consulte la información de **Antes de empezar**. Haga clic en **Next** para continuar.
3. Seleccione los grupos y los hosts individuales que quiera actualizar y, a continuación, haga clic en **Siguiente**.
4. Elige uno de los siguientes modos:

   - **Modo automático** para una actualización automática desde los archivos de instalación de red en un servidor HTTP, NFS o FTP.

     Si elige **Modo automático** y utiliza IIS para alojar los medios de instalación, asegúrese de que el escape doble esté habilitado en IIS antes de extraer la ISO de instalación en él.

   - **Modo manual** para una actualización manual desde un USB/CD/DVD o mediante el arranque de red (utilizando la infraestructura existente).

     Si elige el **modo manual**, debe ejecutar el instalador de XenServer en cada host por turno. Siga las instrucciones que aparecen en pantalla en la consola serie del host. Cuando comienza la actualización, XenCenter le pide que inserte los medios de instalación de XenServer o que especifique un servidor de arranque de red para cada host que actualice.

5. Después de seleccionar el modo de actualización, haga clic en **Ejecutar comprobaciones previas**.
6. Siga las recomendaciones para resolver cualquier comprobación previa de actualización que haya fallado. Si quiere que XenCenter resuelva automáticamente todas las comprobaciones previas fallidas, haga clic en **Resolver todo**.

   > **Nota:**
   >
   > Algunas comprobaciones previas no se pueden resolver automáticamente. Por ejemplo, si sus hosts usan una licencia de Citrix Virtual Apps and Desktops, XenCenter muestra que esta licencia no se aplica a los hosts de XenServer 8. No puede actualizar hasta que obtenga una licencia de XenServer Premium Edition. Para obtener más información, consulte https://xenserver.com/buy.

7. Cuando se hayan resuelto todas las comprobaciones previas, haga clic en **Siguiente** para continuar.
8. Prepare los medios de instalación de XenServer.

   - Si ha elegido el **modo automático**, introduzca los detalles de los medios de instalación. Elija **HTTP**, **NFS**o **FTP** y, a continuación, especifique la URL, el nombre de usuario y la contraseña, según corresponda.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Notas:**
>
> ```
> - Si elige FTP, asegúrese de que se escapan las barras
>   principales que se encuentran en la sección de la
>   ruta del archivo de la URL.
>
> - Introduzca el nombre de usuario y la contraseña
>   asociados a su servidor HTTP o FTP, si ha
>   configurado las credenciales de seguridad. No
>   introduzca el nombre de usuario y la contraseña
>   asociados a su grupo de XenServer.
>
> - XenServer solo admite FTP en modo pasivo.
> ```

- Si eligió el **modo manual**, anote el plan de actualización y siga las instrucciones.

9. Haga clic en **Iniciar actualización**.
10. Cuando comience la actualización, el asistente de **actualización progresiva** de grupos le guiará por las acciones que debe realizar para actualizar cada host. Siga las instrucciones hasta que actualice y actualice todos los hosts de los grupos.
11. Si tiene máquinas virtuales habilitadas para vGPU, cuando llegue al paso que le da la opción de suministrar un paquete complementario, cargue el controlador de NVIDIA que coincida con el de sus máquinas virtuales habilitadas para vGPU. Asegúrese de cargar la versión del controlador correspondiente a la versión de XenServer a la que va a actualizar.
12. El asistente de **actualización sucesiva** de grupos imprime un resumen cuando se completa la actualización. Haga clic en **Finalizar** para cerrar el asistente.

> **Nota:**
>
> Si la actualización o el proceso de actualización fallan por algún motivo, el asistente **Rolling Pool Upgrade** detiene el proceso. Esto le permite solucionar el problema y reanudar el proceso de actualización o actualización haciendo clic en el botón **Reintentar**.

Después de la actualización de versión

Después de actualizar su grupo, le recomendamos que complete las siguientes tareas:

- Habilite la función de verificación de certificados. Para obtener más información, consulte Verificación de certificados.
- Configure las actualizaciones y aplique el conjunto más reciente. Para obtener más información, consulte Actualizar los hosts de XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Una vez completada la actualización progresiva del grupo, es posible que una máquina virtual no esté ubicada en su host principal. Para reubicar la máquina virtual, puede realizar una de las siguientes acciones:

- Migre la máquina virtual en directo a su host principal
- Apague la máquina virtual y, a continuación, iníciela en su host principal.

Actualización progresiva de la agrupación mediante la CLI xe

Antes de realizar una actualización sucesiva del grupo mediante la CLI de xe, asegúrese de haber completado todos los pasos previos de Antes de empezar.

> **Importante:**
>
> Asegúrese de actualizar todos los servidores de su grupo. Se recomienda encarecidamente no ejecutar un grupo de modo mixto (uno con varias versiones de XenServer) durante más tiempo del necesario, ya que el grupo funciona en un estado degradado durante la actualización.
>
> Las operaciones de control clave no están disponibles durante el proceso de actualización. No intente realizar ninguna operación de control. Aunque las VM siguen funcionando normalmente, las acciones de VM distintas a la migración no están disponibles (por ejemplo, apagar, copiar y exportar). En particular, no es seguro realizar operaciones relacionadas con el almacenamiento de información, como agregar, quitar o cambiar el tamaño de discos vDisk.

Para realizar una actualización progresiva de un grupo mediante la CLI xe:

Comience con el coordinador de la agrupación:

1. Desactiva el coordinador de la agrupación. Esto impide que cualquier máquina virtual nueva se inicie o se migre al host especificado.

   ```
   1 xe host-disable host-selector=<host_selector_value>
   ```

2. Asegúrese de que no haya máquinas virtuales ejecutándose en el coordinador del grupo. Cierre, suspenda o migre las máquinas virtuales a otros hosts del grupo.

   - Para apagar una máquina virtual, utilice el siguiente comando:

     ```
     1 xe vm-shutdown
     ```

   - Para suspender una máquina virtual, utilice el siguiente comando:

     ```
     1 xe vm-suspend
     ```

   - Para migrar una máquina virtual específica, utilice el siguiente comando:

     ```
     1 xe vm-migrate
     ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La migración de máquinas virtuales específicas a hosts específicos le proporciona un control total sobre la distribución de las máquinas virtuales migradas a otros hosts del grupo.

- Para evacuar el anfitrión, utilice el siguiente comando:

```
xe host-evacuate
```

Al evacuar todas las máquinas virtuales de un host, se deja la distribución de las máquinas virtuales migradas a XenServer.

3. Cierre el coordinador de agrupaciones.

```
xe host-shutdown
```

> **Importante:**
>
> No puede ponerse en contacto con el coordinador de la agrupación hasta que se complete la actualización del coordinador de la agrupación. Al cerrar el coordinador de la agrupación, los demás anfitriones de la agrupación entran en *modo de emergencia.* Los anfitriones pueden entrar en modo de emergencia cuando se encuentran en un grupo cuyo coordinador de grupo ha desaparecido de la red y no se puede contactar con ellos tras varios intentos. Las VM siguen ejecutándose en hosts en modo de emergencia, pero las operaciones de control no están disponibles.

4. Arranque el coordinador del grupo mediante el medio de instalación de XenServer y el método que prefiera (por ejemplo, USB o red).
5. Siga el procedimiento de instalación de XenServer hasta que el instalador le ofrezca la opción de actualizar. Elija actualizar.

   Cuando el coordinador de la agrupación se reinicia, los demás anfitriones de la agrupación abandonan el modo de emergencia y el servicio normal se restablece después de unos minutos.
6. Inicie o reanude cualquier máquina virtual apagada o suspendida.
7. Migre las máquinas virtuales que quiera volver al coordinador del grupo.

Si algo interrumpe la actualización del coordinador del grupo o si la actualización falla por algún motivo, no intente continuar con la actualización. Reinicie el coordinador del grupo y restaure a una versión funcional.

Repita estos pasos para todos los demás hosts del grupo:

1. Seleccione el siguiente host de XenServer en la ruta de actualización. Inhabilite el host.

```
xe host-disable host-selector=<host_selector_value>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Asegúrese de que no se ejecuten máquinas virtuales en el host. Cierre, suspenda o migre las máquinas virtuales a otros hosts del grupo.

   - Para apagar una máquina virtual, utilice el siguiente comando:

     ```
     xe vm-shutdown
     ```

   - Para suspender una máquina virtual, utilice el siguiente comando:

     ```
     xe vm-suspend
     ```

   - Para migrar una máquina virtual específica, utilice el siguiente comando:

     ```
     xe vm-migrate
     ```

     La migración de máquinas virtuales específicas a hosts específicos le proporciona un control total sobre la distribución de las máquinas virtuales migradas a otros hosts del grupo.

   - Para evacuar el anfitrión, utilice el siguiente comando:

     ```
     xe host-evacuate
     ```

     Al evacuar todas las máquinas virtuales de un host, se deja la distribución de las máquinas virtuales migradas a XenServer.

3. Apaga el host.

   ```
   xe host-shutdown
   ```

4. Arranque el host mediante el medio de instalación de XenServer y el método que prefiera (por ejemplo, USB o red).
5. Siga el procedimiento de instalación de XenServer hasta que el instalador le ofrezca la opción de actualizar. Elija actualizar.
6. Una vez completada la actualización del host, inicie o reanude las máquinas virtuales apagadas o suspendidas.
7. Migre las máquinas virtuales que quiera volver al host.

Si la actualización de un host subordinado falla o se interrumpe, no es necesario revertirla. Ejecuta el comando `xe host-forget` en la agrupación para olvidar ese anfitrión. Vuelva a instalar XenServer en el host y, a continuación, únalo, como un nuevo host, al grupo mediante el comando. `xe pool-join`

Después de la actualización de versión

Después de actualizar su grupo, le recomendamos que complete las siguientes tareas:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Habilite la función de verificación de certificados. Para obtener más información, consulte Verificación de certificados.
- Configure las actualizaciones y aplique el conjunto más reciente. Para obtener más información, consulte Actualizar los hosts de XenServer.

Una vez completada la actualización progresiva del grupo, es posible que una máquina virtual no esté ubicada en su host principal. Para reubicar la máquina virtual, puede realizar una de las siguientes acciones:

- Migre la máquina virtual en directo a su host principal
- Apague la máquina virtual y, a continuación, iníciela en su host principal.

Otros casos

Diseño de partición heredado

El diseño de particiones heredado ya no se admite. Si lo usa, es posible que no pueda actualizar a XenServer 8 y, en su lugar, deba realizar una instalación nueva.

XenServer 6.5 y versiones anteriores utilizan una partición de dominio de control (dom0) de 4 GB para todas las funciones de dom0, incluidos el intercambio y el registro. Esta configuración de particiones se denomina diseño de particiones heredado. Las versiones posteriores de XenServer y Citrix Hypervisor introdujeron un diseño de particiones que aumentaba la partición del dominio de control a 18 GB e incluía una partición de registro independiente. En XenServer 8, solo se admite el diseño de particiones más reciente.

¿Cómo sé qué distribución de particiones usa mi servidor? Es posible que tenga el diseño de particiones heredado en los hosts de XenServer en los siguientes casos:

- Inicialmente instaló el host de XenServer con XenServer 5.6 Service Pack 2 o una versión anterior y, desde entonces, se ha actualizado a versiones posteriores compatibles.
- Está utilizando hardware antiguo que tiene menos de 46 GB de espacio en disco principal.
- El hardware requiere que haya una partición de utilidades.

Para saber cuántas particiones tiene su host de XenServer, ejecute el siguiente comando en la consola del servidor
:

```
fdisk -l
```

- Si el comando muestra 6 particiones, está utilizando el nuevo diseño de particiones y puede actualizar a XenServer 8.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si el comando enumera 3 o 4 particiones, está utilizando el diseño de particiones heredado.

¿Qué puedo hacer ahora? Si utiliza el nuevo diseño de particiones, puede actualizar a XenServer 8.

Si utiliza el diseño de particiones heredado:

- Si tiene menos de 46 GB de espacio en el disco principal o si su hardware requiere que haya una partición de utilidades, no podrá instalar ni actualizar a XenServer 8.
- Si el disco es GPT y la SR local está vacía con al menos 38 GB libres, puede cambiar del diseño de particiones heredado al nuevo durante la actualización. Debe usar XenCenter para intentar la actualización en un servidor con el diseño de particiones heredado. Para obtener más información, consulte Actualización progresiva de grupos mediante XenCenter.
- En el caso de otro hardware, puede realizar una instalación nueva de XenServer 8. Para obtener más información, consulte Instalación.

Entornos de Citrix Virtual Apps and Desktops

Si utiliza XenServer para alojar sus cargas de trabajo de Citrix Virtual Apps and Desktops, consulte Escenarios de actualización para Citrix Virtual Apps and Desktops.

Actualice los hosts de XenServer

April 10, 2024

Con XenServer 8, las nuevas funciones y las correcciones de errores se envían con frecuencia a la red de entrega de contenido (CDN) en forma de actualizaciones disponibles para los hosts y grupos de XenServer, lo que le permite beneficiarse de un proceso de publicación más eficiente que le entrega contenido nuevo a un ritmo más rápido de lo que era posible anteriormente.

Para garantizar que siempre esté al día con la última y mejor actualización, no hay que elegir: cuando aplica actualizaciones a su grupo, se actualiza al estado más reciente y completamente probado. Configure su grupo para que se sincronice automáticamente con un canal de actualización. Esta acción descarga todas las actualizaciones disponibles para el coordinador del grupo. A continuación, puede aplicar todas las actualizaciones descargadas mediante XenCenter o la CLI xe.

> **Nota:**
>
> Si usó XenServer 8 durante el período de Technical Preview, no necesita volver a instalar ni actualizar los hosts para pasar a la versión GA. Aplique las actualizaciones más recientes a través de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> XenCenter para obtener asistencia en producción.

Ciclo de vida

Durante su ciclo de vida, XenServer 8 proporciona un flujo de actualizaciones frecuentes y fáciles de aplicar, que le permiten usar nuevas funciones y corregir errores lo antes posible. Debe aplicar todas las actualizaciones disponibles de forma periódica. Como resultado, el comportamiento y el conjunto de funciones de XenServer 8 pueden cambiar.

Para obtener más información, consulte Ciclo de vida de XenServer.

Proceso de actualización

La transmisión de versiones de XenServer 8 y la red de entrega de contenido (CDN) funcionan juntas para permitirle aplicar actualizaciones frecuentes a los hosts y grupos de XenServer desde XenCenter.

1. Ponemos a su disposición actualizaciones frecuentes para XenServer 8 en nuestra CDN segura.
2. En XenCenter, compruebe cuándo hay actualizaciones disponibles para su grupo.
3. Con XenCenter, inicie el proceso de aplicación de actualizaciones al grupo de XenServer.

Canales de actualización

La transmisión de versiones de XenServer 8 consta de dos fases, también denominadas canales de actualización:

- Acceso anticipado
- Normal

Para recibir actualizaciones frecuentes, configure el grupo de XenServer para suscribirse a uno de esos canales de actualización.

1. Cuando las actualizaciones se envían por primera vez a nuestra CDN, entran en el canal de actualizaciones de acceso anticipado.

   El acceso anticipado es perfecto para los entornos de prueba, ya que le permite obtener las actualizaciones más recientes cuando se publiquen. Si optas por recibir actualizaciones con antelación, tendrás la oportunidad de probarlas antes de que estén disponibles en el canal de actualizaciones normal.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Se admite el acceso anticipado para su uso en producción. Sin embargo, no lo recomendamos para entornos de producción críticos.

2. Estas actualizaciones luego fluyen secuencialmente a Normal, el siguiente canal de actualización.

   A menos que hayamos retrasado esta progresión, podéis esperar que las actualizaciones de acceso anticipado estén disponibles en modo normal de forma regular. Se recomienda lo normal para entornos de producción.

Ocasionalmente, es posible que vea que las actualizaciones están disponibles para sus grupos de acceso anticipado y normal al mismo tiempo. Estas actualizaciones nos permiten entregar parches de seguridad y correcciones críticas a todos los canales de actualización de forma inmediata.

Introducción a las actualizaciones

Para obtener información sobre cómo configurar y aplicar actualizaciones para los hosts de XenServer mediante XenCenter, consulte Aplicar actualizaciones mediante XenCenter. Como alternativa, puede usar la CLI xe para aplicar actualizaciones a los hosts de XenServer. Para obtener más información, consulte Aplicar actualizaciones mediante la CLI xe.

> **Importante:**
>
> No admitimos el uso directo ni la modificación de los componentes de actualización subyacentes en dom0. Solo puede usar XenCenter o la CLI xe para configurar y aplicar actualizaciones.

Aplicar actualizaciones mediante XenCenter

April 10, 2024

Aplique actualizaciones a los hosts y grupos de XenServer 8 mediante la versión más reciente de XenCenter. La versión más reciente de XenCenter se proporciona en la página de descargas de productos de XenServer.

Para proporcionar notificaciones de actualización, XenCenter requiere acceso a Internet. Si el XenCenter está protegido por un firewall, asegúrese de que tiene acceso al dominio. `updates.ops.xenserver.com` Para recibir las actualizaciones, los hosts de XenServer necesitan acceso a Internet. Si sus hosts están detrás de un firewall, asegúrese de que tengan acceso a los subdominios de `ops.xenserver.com`. Para obtener más información, consulte Requisitos de conectividad .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Complete los siguientes pasos para poder actualizar los grupos de XenServer:

1. Instale la versión más reciente de XenCenter.
2. Instale o actualice a XenServer 8.
3. Configure las actualizaciones para su grupo.
4. Consulte las actualizaciones disponibles para su grupo.
5. Aplique actualizaciones a su grupo.
6. Realice las tareas de actualización.

Configure las actualizaciones para su agrupación

Antes de poder aplicar actualizaciones a los hosts y grupos de XenServer, debe configurar las actualizaciones del host suscribiendo el grupo o el host a un canal de actualizaciones. Estos canales controlan la rapidez con la que puede acceder a las actualizaciones que están disponibles en la red de entrega de contenido (CDN).

Los dos canales de actualización son:

- Acceso anticipado : perfecto para entornos de prueba
- Normal : recomendado para entornos de producción

Después de suscribir su grupo a uno de los canales de actualización, su grupo se sincroniza de forma periódica y automática con el canal de actualización. Esta acción descarga todas las actualizaciones disponibles para el coordinador del grupo. A continuación, puede aplicar todas las actualizaciones descargadas mediante XenCenter.

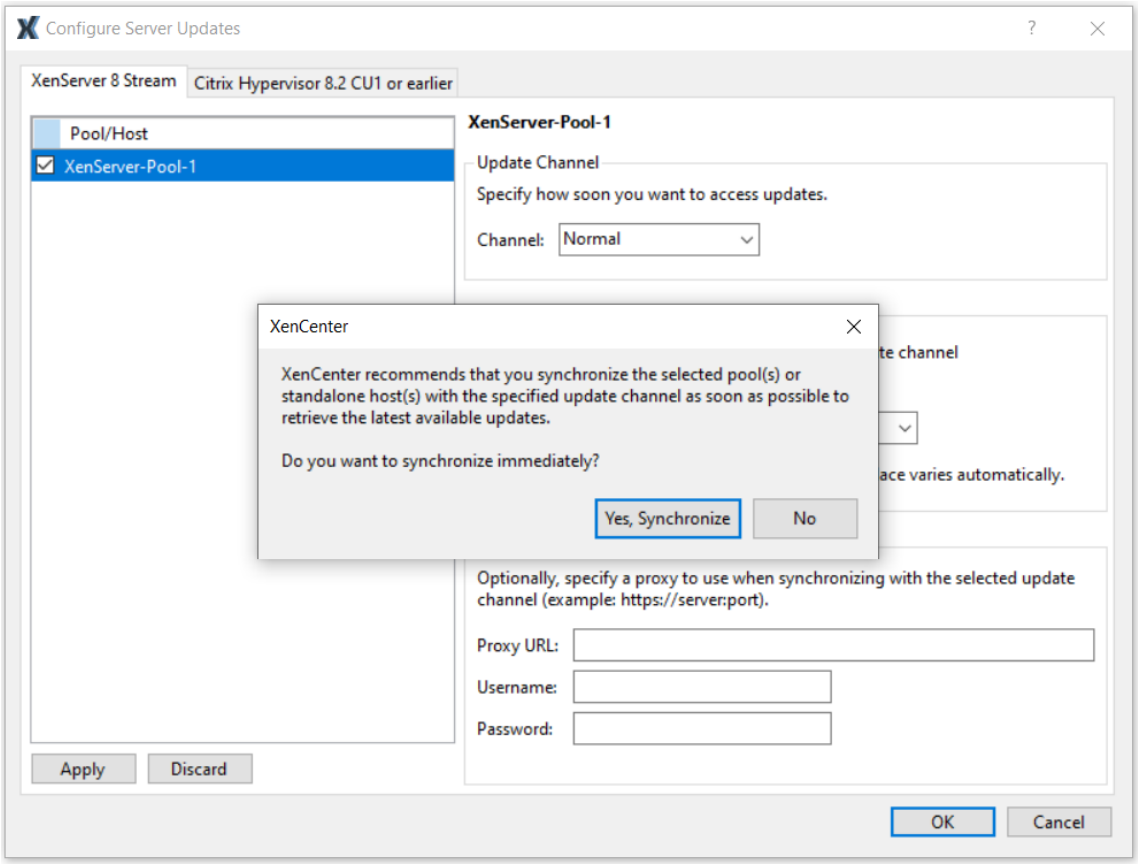
1. En XenCenter, en el menú **Herramientas**, seleccione **Configurar actualizaciones**. Como alternativa, vaya a la sección **Actualizaciones** en la ficha **General** de su grupo y seleccione **Configurar actualizaciones** o haga clic con el botón derecho en su grupo y seleccione **Actualizaciones** > **Configurar actualizaciones**. Se abre la ventana **Configurar actualizaciones del servidor** .
2. En la ficha **XenServer 8**, seleccione los grupos o hosts que desee configurar.
3. En **Canal de actualizaciones**, especifica la rapidez con la que deseas acceder a las actualizaciones. Su grupo o anfitrión puede suscribirse a uno de los siguientes canales de actualización:
   - **Acceso anticipado**
   - **Normal**
4. En **Programación de sincronización**, seleccione la frecuencia con la que desea que el grupo de XenServer se sincronice con el canal de actualización. Esto puede ser diario o semanal en un día determinado de la semana.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Tras la sincronización, aplique las actualizaciones a su grupo lo antes posible para beneficiarse de las últimas actualizaciones.
>
> Si designa a un nuevo coordinador del grupo después de la sincronización, pero antes de aplicar las actualizaciones a los anfitriones del grupo, debe volver a sincronizar con el nuevo coordinador del grupo para poder actualizar el grupo.
>
> No sincronice el grupo de XenServer mientras el grupo se esté actualizando.

5. (Opcional) En **Servidor proxy**, especifique un proxy para usar al sincronizar con el canal de actualización. Este servidor proxy se usa para la comunicación entre el host y la CDN pública.
6. Haga clic en **Aplicar** para aplicar los cambios de configuración al grupo de XenServer y, a continuación, repita los pasos anteriores para configurar las actualizaciones del resto de los grupos de XenServer.
7. Si está satisfecho con los cambios de configuración de sus grupos, haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Configurar actualizaciones del servidor** . Cuando configura su host o grupo por primera vez con un canal de actualización (o si más adelante cambia su host o grupo para sincronizarlo con un canal de actualización diferente), se le preguntará si desea sincronizar inmediatamente su host o grupo con el canal de actualización. En el cuadro de diálogo que se abre **, seleccione Sí, sincronizar** si desea sincronizar su host o grupo con el canal de actualización inmediatamente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

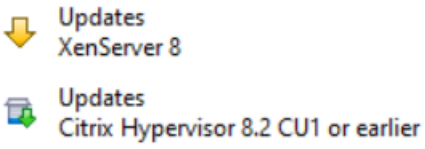


8. En cuanto su grupo se sincronice con el canal de actualizaciones, aplique las actualizaciones descargadas a su grupo mediante el asistente de **instalación de actualizaciones** . Para obtener más información, consulte Aplicar actualizaciones a su agrupación.

Después de configurar el grupo de XenServer, puede encontrar información sobre el canal de actualización al que está suscrito el grupo y la última vez que el grupo se sincronizó con el canal de actualización en la sección **Actualizaciones** de la **ficha** General del grupo en XenCenter. También puedes encontrar información sobre la última vez que se actualizó su host en la sección **Actualizaciones** de la ficha **General** de su host.

Vea las actualizaciones disponibles para su agrupación

XenCenter emite notificaciones sobre las actualizaciones disponibles para los hosts y grupos en las fichas **Actualizaciones** de la vista **Notificaciones**. **Las fichas Actualizaciones** se dividen en actualizaciones de XenServer 8 y actualizaciones de Citrix Hypervisor.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La pestaña **Actualizaciones** de XenServer 8 se actualiza cuando los hosts y grupos de XenServer 8 se sincronizan con el canal de actualización. La frecuencia de esta actualización depende de la programación de sincronización que haya configurado para su grupo (ya sea diaria o semanalmente en un día determinado de la semana).

Para ver las actualizaciones más recientes disponibles para su grupo, sincronice el grupo de XenServer con el canal de actualización. Puede hacerlo desde los siguientes lugares:

- En la vista **Por servidor** de la ficha **Actualizaciones**, puede elegir **Sincronizar todo** para sincronizar todos los grupos administrados por XenCenter o **Sincronizar seleccionados** para sincronizar los grupos seleccionados.
- Como alternativa, vaya a la sección **Actualizaciones** en la ficha **General** de su grupo y seleccione **Sincronizar ahora** o haga clic con el botón secundario en su grupo y seleccione **Actualizaciones** > **Sincronizar ahora**.

A continuación, puede revisar todas las actualizaciones disponibles para sus grupos de XenServer 8. Los tipos de actualizaciones son:

- **Correcciones de seguridad**
- **Problemas resueltos**
- **Mejoras**
- **Funciones nuevas**
- **Funciones en Tech Preview**
- **Cambios fundamentales**

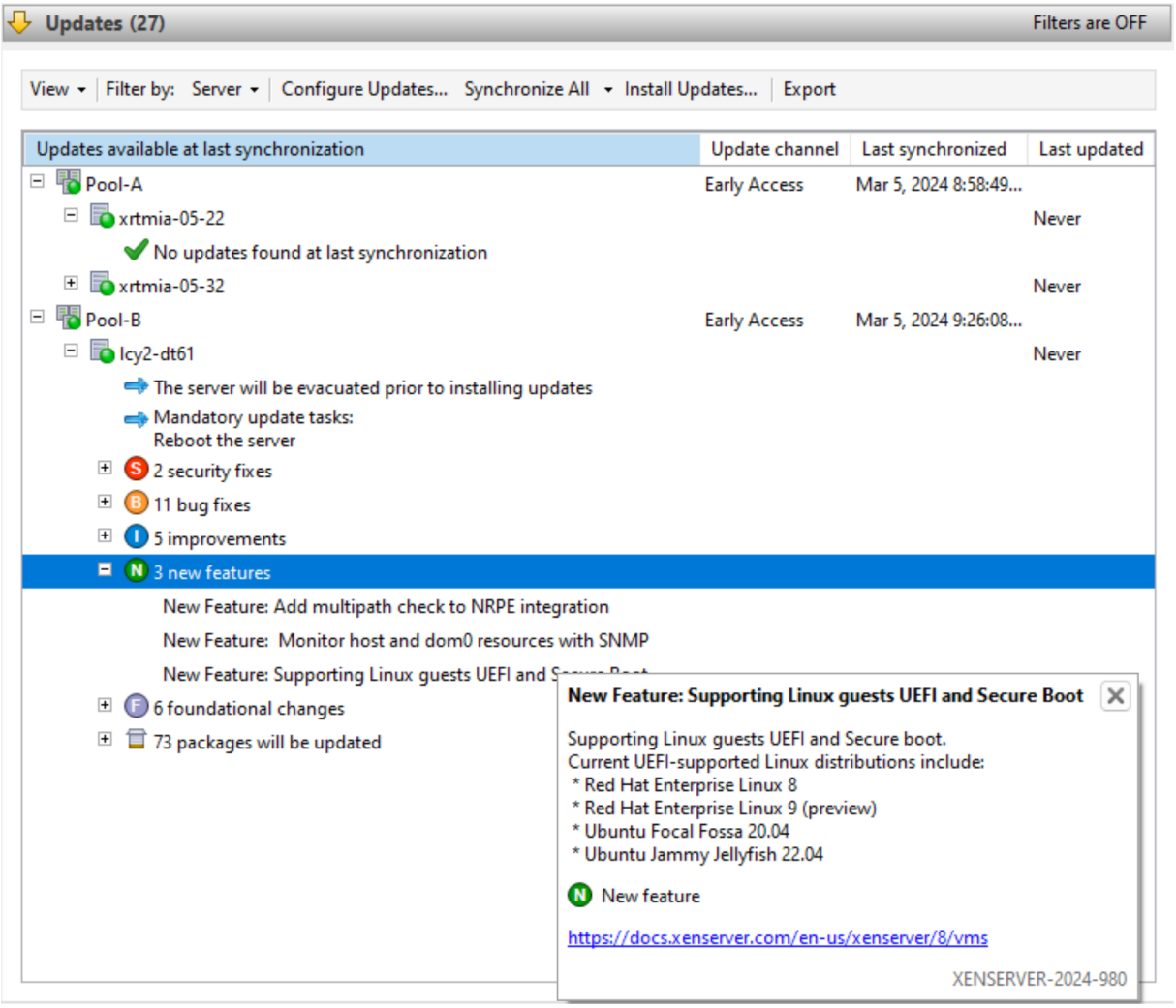
  > **Nota:**
  >
  > Los cambios fundamentales son cambios fundamentales que no son visibles por el cliente para mantener y mejorar el producto.

En el panel principal, use la opción **Ver** para elegir si las actualizaciones se muestran **Por servidor** o **Por actualización**.

Por servidor

Las actualizaciones se agrupan por host y tipo de actualización.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Puede filtrar la información de actualización por servidor. Seleccione una actualización y coloque el cursor sobre ella para ver información detallada sobre la misma.

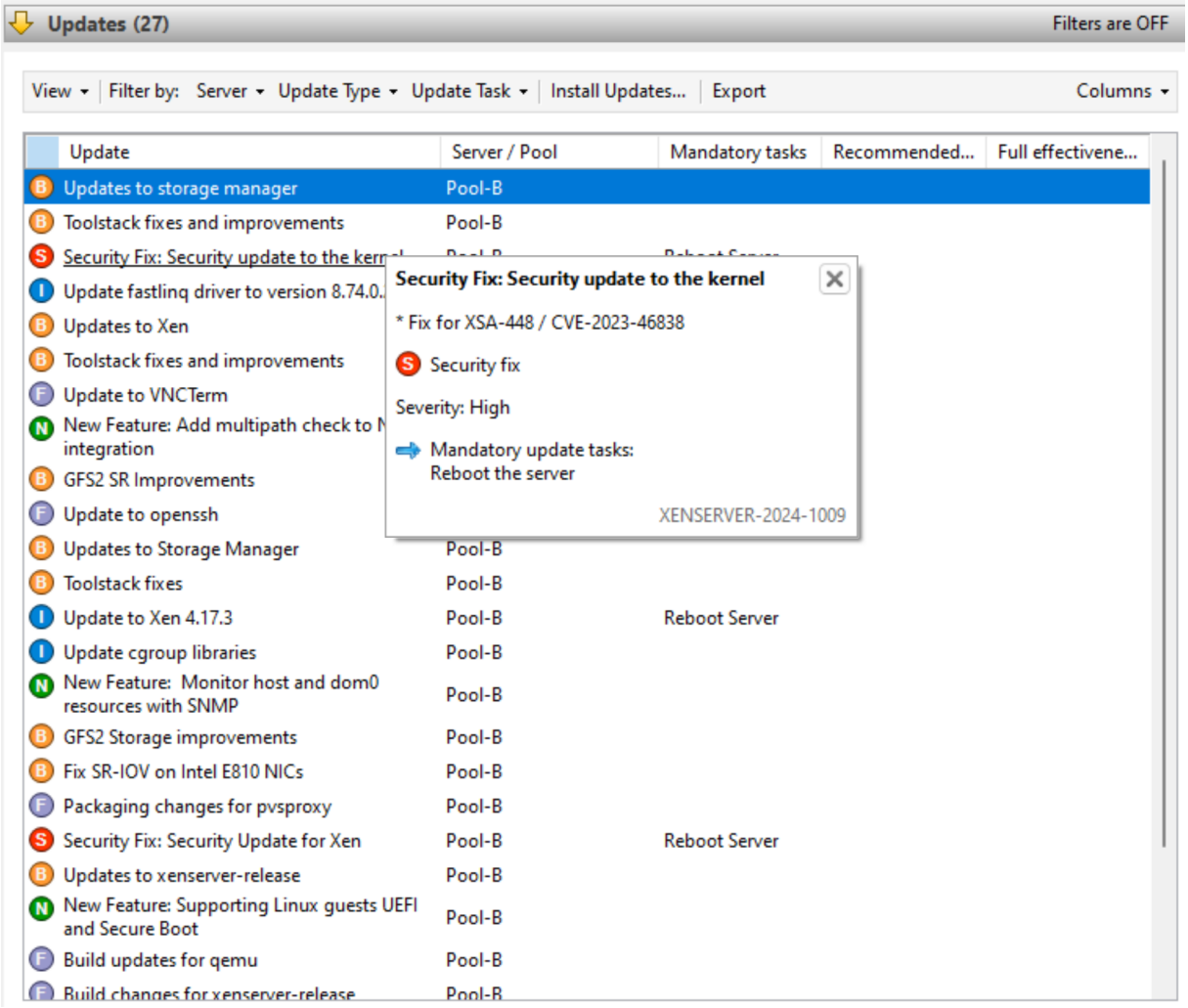
Para ver esta información sobre las actualizaciones disponibles sin conexión, seleccione **Exportar todo** para exportar la información como un `.md` archivo. El contenido del archivo `.md` se agrupa por grupo y, a continuación, por host. Para cada host, el archivo contiene la siguiente información:

- Cualquier tarea de actualización para este host o sus máquinas virtuales. Para obtener más información sobre las tareas obligatorias, recomendadas y de plena eficacia, consulte Actualizar tareas.
- Actualizaciones agrupadas por tipo de actualización
  - El nombre de la actualización
  - Descripción de la actualización
- Una lista de los RPM que se actualizarán en el host

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Por actualización

Todas las actualizaciones se enumeran cronológicamente por orden de publicación.



Puede filtrar la información de actualización por el servidor al que se puede aplicar, por el tipo de actualización y por cualquier tarea de actualización que se le aplique. Seleccione una actualización y coloque el cursor sobre ella para ver información detallada sobre la misma.

Para ver esta información sobre las actualizaciones disponibles sin conexión, seleccione **Exportar todo** para exportar la información como un `.csv` archivo. El `.csv` archivo contiene la siguiente información:

- El tipo de actualización
- El nombre de la actualización
- Los servidores a los que se puede aplicar esta actualización
- Las tareas obligatorias, recomendadas y de plena eficacia

Para obtener más información sobre las tareas obligatorias, recomendadas y de plena eficacia, con-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

sulte Actualizar tareas.

- Para aplicar las actualizaciones a sus hosts o grupos, seleccione **Instalar actualizaciones** para abrir el asistente de **instalación de actualizaciones** . Para obtener más información, consulte la siguiente sección Aplicar actualizaciones a su agrupación.

Aplicar actualizaciones a su agrupación

El mecanismo de instalación de actualizaciones de XenCenter aplica las actualizaciones a los hosts y grupos mediante **el** asistente de instalación de actualizaciones. Durante el proceso, XenCenter determina automáticamente la acción menos impactante necesaria después de aplicar todas las actualizaciones disponibles. El asistente de **instalación de actualizaciones** realiza automáticamente estos pasos:

1. Si es necesario, migra las máquinas virtuales de cada host.
2. Si es necesario, coloca el host en modo de mantenimiento.
3. Aplica las actualizaciones.
4. Si es necesario, ejecute las tareas de actualización necesarias, como reiniciar el host, reiniciar la pila de herramientas o reiniciar las máquinas virtuales.
5. Migra las máquinas virtuales de nuevo al host actualizado.

Se revierte cualquier acción que se lleve a cabo en la fase de comprobación previa para permitir la aplicación de las actualizaciones, como desactivar la alta disponibilidad.

Antes de comenzar

Antes de aplicar una actualización a los servidores, preste especial atención a lo siguiente:

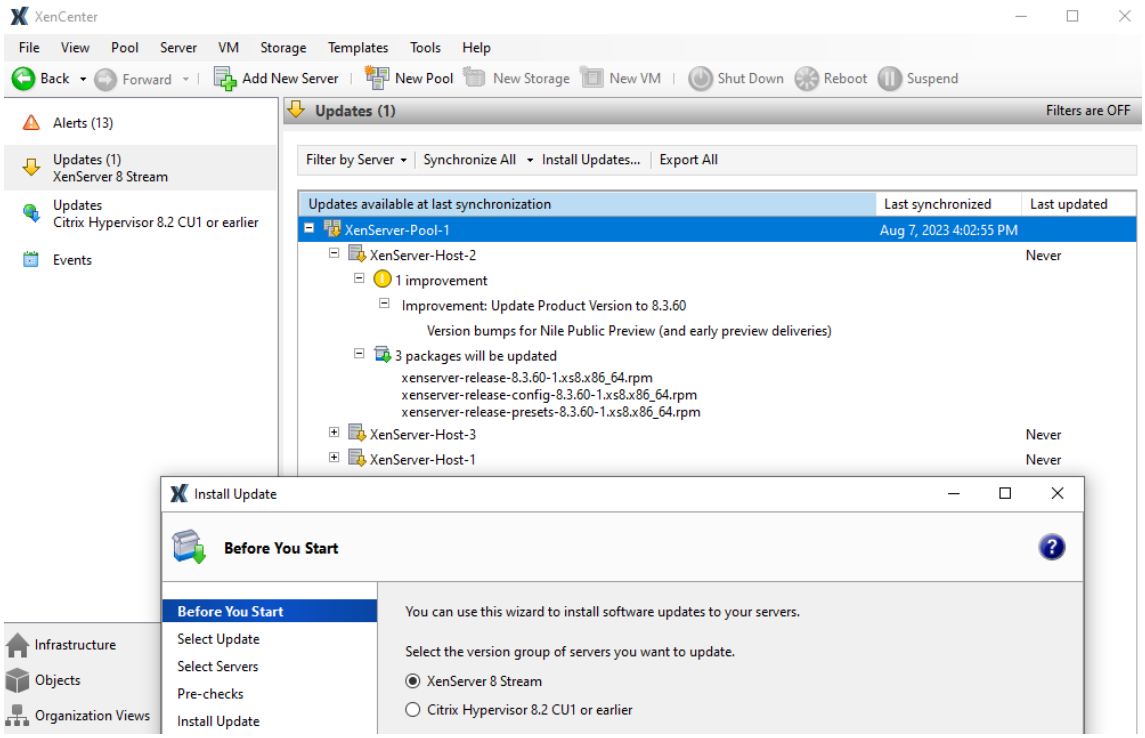
- Realice copias de seguridad de todos sus servidores
- Asegúrese de que la alta disponibilidad (HA) no esté habilitada en ningún grupo en el que desee aplicar actualizaciones.
- Asegúrese de haber iniciado sesión en XenCenter como administrador u operador de grupo, o con una cuenta raíz local.

Instalar actualizaciones

En la siguiente sección se proporcionan instrucciones paso a paso sobre cómo aplicar las actualizaciones mediante el asistente de **instalación de actualizaciones**:

1. En el menú XenCenter, seleccione **Herramientas** y, a continuación, **Instalar actualizaciones**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. En el asistente de **instalación de actualizaciones**, seleccione **XenServer 8** y revise la información de la página **Antes de empezar**. Haga clic en **Next** para continuar.
3. Selecciona **Actualizaciones automatizadas**. Haga clic en **Siguiente**.
4. Seleccione los grupos o hosts de XenServer que quiere actualizar. Haga clic en **Siguiente** para pasar a la siguiente página del asistente y comenzar las comprobaciones previas.
5. El asistente realiza varias comprobaciones previas para comprobar que las actualizaciones se pueden aplicar en el host o el grupo. Por ejemplo, debe haber sincronizado su host o grupo con el canal de actualización la semana pasada.

   Sigue las recomendaciones que aparecen en pantalla para resolver cualquier comprobación previa que haya fallado. **Si prefiere que XenCenter resuelva automáticamente todas las comprobaciones previas fallidas, seleccione Resolver todo.** Cuando se hayan resuelto las comprobaciones previas, seleccione **Siguiente** para continuar.

   > **Notas:**
   >
   > - Si el proceso de actualización no se puede completar por algún motivo, XenCenter lo detiene. Esta interrupción le permite corregir el problema y reanudar el proceso de actualización haciendo clic en el botón **Reintentar**.
   > - Si selecciona **Cancelar** en esta fase, el asistente de **instalación de actualizaciones** revierte los cambios.

6. Una vez aplicadas las actualizaciones, es posible que se requieran algunas tareas de actual-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ización (como reiniciar los hosts). En la página **Modo de actualización**, seleccione el nivel de tareas de actualización que quiere que XenCenter lleve a cabo automáticamente (como reiniciar los hosts) después de aplicar las actualizaciones al grupo. De forma predeterminada, XenCenter elige el nivel recomendado de tareas de actualización. Las tareas obligatorias no se pueden deseleccionar y XenCenter las realiza automáticamente.

Las tareas de actualización obligatorias, recomendadas y de plena eficacia se enumeran en **Tareas**. Si no se requieren tareas de actualización, la página muestra una nota que indica que **no se requiere ninguna acción**. Para obtener más información sobre los diferentes tipos de tareas de actualización y los niveles de orientación que ofrece XenCenter, consulte Tareas de actualización.

7. Haga clic en **Instalar actualizaciones** para XenCenter para empezar a instalar las actualizaciones para su host o grupo.
8. El asistente **Instalar actualizaciones** muestra el progreso de la actualización y muestra las principales operaciones que realiza XenCenter al actualizar cada host del grupo. Haga clic en **Finalizar** para completar las actualizaciones y cerrar el asistente de **instalación de actualizaciones**.

Actualizar tareas

Es posible que se requieran algunas tareas (como evacuar o reiniciar los hosts) antes y después de aplicar las actualizaciones a su grupo. A veces, no se requieren tareas de actualización.

Categorías de orientación

XenServer intenta minimizar las interrupciones en las máquinas virtuales que estas tareas de actualización pueden provocar al clasificarlas en **obligatorias**, **recomendadas**, de **plena eficacia** y **con parches activos**. Estas categorizaciones le permiten determinar si es necesaria para su entorno y perfil de riesgo una tarea de actualización que pueda provocar un tiempo de inactividad o una interrupción leve en sus hosts o máquinas virtuales.

Las actualizaciones pueden incluir tareas en más de una de estas categorías. Por ejemplo, una actualización puede requerir que reinicie el host para ser totalmente efectiva, pero se recomienda reiniciar la pila de herramientas para aprovechar al máximo los beneficios de la actualización y reducir las posibles interrupciones en el grupo.

Durante el proceso de actualización, puede elegir llevar a cabo uno de los tres niveles de tareas siguientes:

1. Obligatorio
2. Obligatorio + Recomendado

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Obligatorio + Recomendado + Plena eficacia

Obligatorio Las tareas obligatorias se *deben* realizar después de una actualización; de lo contrario, el sistema podría fallar durante el tiempo de ejecución. Estas acciones son necesarias para habilitar las correcciones críticas y garantizar que su entorno sea seguro y estable. Al aplicar actualizaciones, XenCenter realiza estas tareas. No puede omitir las tareas obligatorias.

Recomendado Las tareas recomendadas son las tareas que le recomendamos que realice para aprovechar la mayoría de las funciones y correcciones incluidas en las actualizaciones. Al aplicar actualizaciones, estas tareas se seleccionan de forma predeterminada en XenCenter, pero puede optar por no realizarlas. Si decide no realizar estas tareas ahora, se enumeran en las tareas pendientes del grupo, el host o la máquina virtual correspondiente.

Por qué realizar las tareas recomendadas:

- Estas tareas son las que garantizan un entorno de XenServer seguro y estable.

Por qué omitir las tareas recomendadas:

- Tras revisar la información detallada de las actualizaciones, considera que el riesgo de no aplicarlas por completo ahora es aceptable.
- Las tareas recomendadas ahora provocan interrupciones no deseadas en sus máquinas virtuales.

Plena eficacia Se requieren tareas de plena eficacia para obtener los beneficios de la actualización relacionada. Las actualizaciones que tienen asociadas tareas de plena eficacia suelen ser relevantes solo para los usuarios de determinado hardware o que utilizan funciones específicas.

Revise la información de actualización para saber si estas tareas son necesarias para su entorno. Al aplicar actualizaciones, estas tareas no se seleccionan de forma predeterminada en XenCenter, pero puede optar por realizarlas durante la actualización si cree que la actualización se aplica a su entorno o configuración. Si decide no realizar estas tareas ahora, se enumeran en las tareas pendientes del grupo, el host o la máquina virtual correspondiente.

Por qué realizar las tareas de plena eficacia:

- Las actualizaciones que tienen tareas de plena eficacia son relevantes para su hardware, entorno o configuración.

Por qué omitir las tareas de plena eficacia:

- Las actualizaciones que tienen una guía de plena eficacia no son relevantes para su hardware, entorno o configuración.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Las tareas de plena eficacia provocan ahora interrupciones no deseadas en sus máquinas virtuales.
- No necesita los beneficios de estas actualizaciones en este momento.

Si las tareas de plena eficacia se aplican a su entorno, pero ha optado por aplazarlas, planifique completar estas tareas durante un período de mantenimiento adecuado para mantener la estabilidad de su entorno.

Parches activos Las actualizaciones de ciertos componentes pueden incluir un parche activo, o en vivo. La posibilidad de aplicar un parche activo a los hosts depende de la versión del componente que se haya instalado la última vez que se reiniciaron los hosts. Si se puede aplicar una actualización como parche activo a sus hosts, la guía sobre parches activos reemplaza a la guía recomendada.

> **Ejemplo:**
>
> Tienes dos agrupaciones. El grupo A se ha actualizado a un nivel reciente. El grupo B no se ha actualizado durante algún tiempo. Publicamos una nueva actualización que incluye la tarea de actualización recomendada "Reiniciar el host"y la tarea de actualización de parche activo "Reiniciar la pila de herramientas".
>
> En el grupo A, el parche activo se puede aplicar a estos hosts más actualizados. La guía recomendada de XenCenter muestra "Reiniciar la pila de herramientas". La tarea menos disruptiva de la guía de parches activos anula la guía recomendada.
>
> En el grupo B, el parche activo no se puede aplicar a los hosts porque están en un nivel anterior. La guía recomendada de XenCenter muestra "Reiniciar el host". La guía recomendada sigue siendo aplicable. La guía sobre los parches en vivo, o activos, es irrelevante en este caso.

A veces, solo algunas de las correcciones de una actualización están habilitadas cuando la actualización se aplica como un parche activo. Revise los detalles de la actualización para saber si necesita todas las correcciones de la actualización o solo las habilitadas con el parche activo. A continuación, puede usar esta información para decidir si desea realizar las tareas recomendadas. Para obtener más información, consulte Ver las actualizaciones disponibles para su grupo.

Actualizar tareas

Es posible que se requieran una o más de las siguientes tareas al aplicar una actualización. Cualquier tipo de tarea de actualización se puede incluir en cualquier categoría de orientación.

Actualizar las tareas de su host Esta tarea solo se lleva a cabo *antes* de aplicar las actualizaciones y, a veces, la lleva a cabo como parte de la tarea "Reiniciar el host":

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Evacuar el servidor**: Todas las máquinas virtuales deben migrarse del host de XenServer o apagarse antes de aplicar la actualización. Para completar esta tarea, XenCenter migra todas las máquinas virtuales del host. Mientras esta tarea está en curso, el grupo de XenServer funciona a una capacidad reducida, ya que un host no está disponible temporalmente para ejecutar máquinas virtuales.

Las siguientes tareas requieren acciones en el host actualizado:

- **Reiniciar el servidor**: Se debe reiniciar el host de XenServer. Para completar esta tarea, XenCenter migra todas las máquinas virtuales del host y lo reinicia. Mientras esta tarea está en curso, el grupo de XenServer funciona a una capacidad reducida, ya que un host no está disponible temporalmente para ejecutar máquinas virtuales.
- **Reiniciar la pila de herramientas**: Se debe reiniciar la pila de herramientas del host. Cuando XenCenter reinicia la pila de herramientas en el coordinador del grupo, XenCenter pierde la conexión con el grupo e intenta volver a conectarse automáticamente. En otros miembros del grupo, no hay ningún efecto visible.

Actualizar las tareas de su máquina virtual Algunas actualizaciones proporcionan nuevas funciones para sus máquinas virtuales. Estas actualizaciones pueden requerir las siguientes tareas en las máquinas virtuales:

- **Reiniciar la máquina virtual**: La máquina virtual debe reiniciarse. En XenCenter, mientras la máquina virtual se reinicia, se muestra el icono de parada rojo (cuadrado sobre rojo). Cuando la tarea esté completa, se mostrará el icono verde de reproducción. Durante este tiempo, la máquina virtual no está disponible para el usuario final.
- **Modelo de dispositivo de reinicio**: Se debe reiniciar el modelo de dispositivo para las máquinas virtuales del host actualizado. En XenCenter, mientras el modelo de dispositivo se reinicia, la máquina virtual muestra un triángulo de advertencia amarillo. Cuando la tarea esté completa, se mostrará el icono verde de reproducción. Durante este tiempo, no puede detener, iniciar ni migrar la máquina virtual. Es posible que el usuario final de la máquina virtual experimente una pausa leve y se reanude su sesión.

  Para que la acción de reinicio del modelo de dispositivo sea compatible con una máquina virtual Windows, la máquina virtual debe tener instalado XenServer VM Tools para Windows.

Revise las tareas de actualización antes de aplicar las actualizaciones

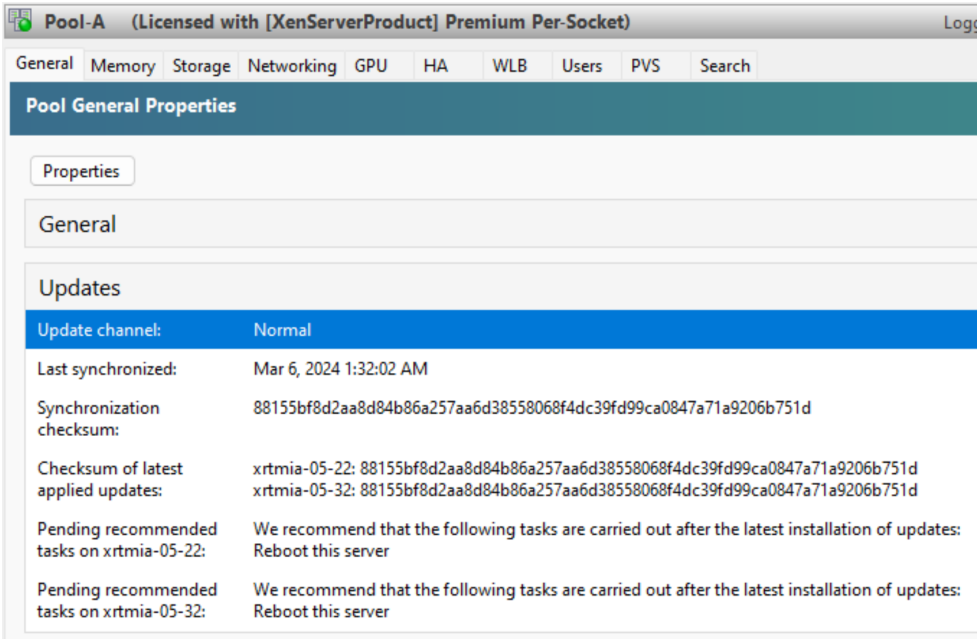
Estas tareas aparecen en la ficha **Actualizaciones** de XenServer 8, en la vista **Notificaciones** . Para obtener más información, consulte Ver las actualizaciones disponibles para su grupo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ver las tareas pendientes

Si decide no realizar todas las tareas durante una actualización, las tareas pendientes de cada grupo, host o máquina virtual se muestran en la vista **Infraestructura** de XenCenter.

En la ficha **General** del grupo, el host o la máquina virtual, consulte la sección **Actualizaciones**.

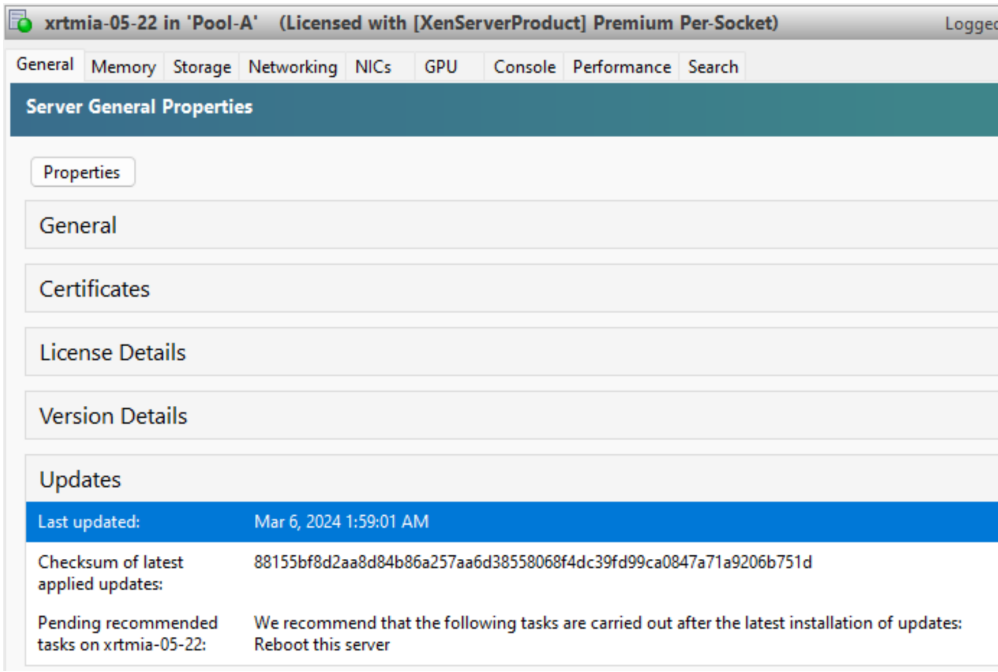


Tareas pendientes del grupo

En esta sección se muestran las tareas pendientes de todos los hosts del grupo.

También muestra una suma de comprobación que indica el nivel con el que se ha sincronizado el coordinador del grupo actual y unas sumas de comprobación para cada host que indican el nivel de las actualizaciones instaladas. Estas sumas de comprobación pueden proporcionar información útil si necesita ponerse en contacto con el servicio de asistencia técnica.

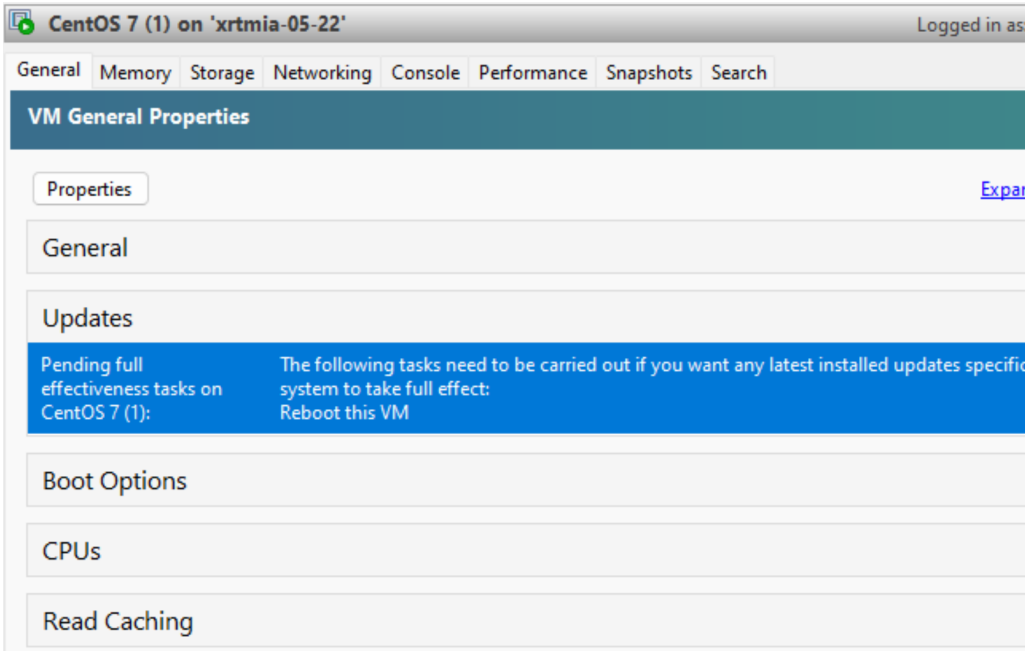
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Tareas pendientes del host

En esta sección se muestran las tareas pendientes del host de XenServer.

También muestra una suma de comprobación que indica el nivel de las actualizaciones instaladas. Esta suma de comprobación puede proporcionar información útil si necesita ponerse en contacto con el servicio de asistencia técnica.



Tareas pendientes de VM

En esta sección se muestran las tareas pendientes de una máquina virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Versión actual de XenCenter

April 10, 2024

Use XenCenter aaaa.x.x para administrar el entorno de XenServer 8 y para implementar, administrar y supervisar máquinas virtuales desde su máquina de escritorio Windows.

> **Nota:**
>
> Aún no se admite el uso de XenCenter aaaa.x.x con Citrix Hypervisor 8.2 CU1 en entornos de producción. Para administrar el entorno de producción de Citrix Hypervisor 8.2 CU1, use XenCenter 8.2.7. Para obtener más información, consulte la documentación de XenCenter 8.2.7.
>
> Puede instalar XenCenter 8.2.7 y XenCenter aaaa.x.x en el mismo sistema. La instalación de XenCenter aaaa.x.x no sobrescribe la instalación de XenCenter 8.2.7.

Puede descargar el instalador de la versión más reciente de XenCenterdesde la página de descargas de XenServer.

Uso de XenServer con productos Citrix

April 10, 2024

XenServer ofrece funciones que mejoran su interoperación con Citrix Virtual Apps and Desktops, Citrix DaaS y Citrix Provisioning.

Para obtener más información acerca de estos productos, consulte:

- Documentación del producto Citrix Virtual Apps and Desktops
- Documentación del producto Citrix DaaS
- documentación del producto Citrix Provisioning

Versiones compatibles

Puede encontrar las versiones de estos productos con los que XenServer 8 interopera en el sitio web de Citrix: Hipervisores compatibles para Citrix Virtual Apps and Desktops (MCS) y Citrix Provisioning (PVS).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Licencias

Para usar XenServer para las cargas de trabajo de Citrix Virtual Apps and Desktops o Citrix DaaS, debe tener una licencia de XenServer Premium Edition. Para obtener más información, consulte Licencias.

Si ya usa XenServer o Citrix Hypervisor para alojar sus cargas de trabajo de Citrix Virtual Apps and Desktops, puede solicitar la participación en nuestra promoción y recibir hasta 10 000 licencias de socket de XenServer Premium Edition de forma gratuita. Más información.

Puede obtener licencias de XenServer en https://xenserver.com/buy.

Funciones de XenServer para Citrix Virtual Apps and Desktops

Las siguientes funciones de XenServer están diseñadas para usarse con Citrix Virtual Apps and Desktops, Citrix DaaS y Citrix Provisioning:

- **Intellicache**: El uso de XenServer con IntelliCache hace que las implementaciones alojadas de Citrix Virtual Desktops sean más rentables, ya que permite usar una combinación de almacenamiento compartido y almacenamiento local. Resulta especialmente beneficioso cuando muchas máquinas virtuales comparten una imagen de sistema operativo común. La carga en el arreglo de almacenamiento se reduce y se mejora el rendimiento. Además, el tráfico de red hacia y desde el almacenamiento compartido se reduce a medida que el almacenamiento local almacena en caché la imagen principal del almacenamiento compartido.
- **Almacenamiento en caché de lectura**: El almacenamiento en caché de lectura mejora el rendimiento del disco de una máquina virtual al almacenar en caché los datos en la memoria libre del host. Mejora el rendimiento en un entorno de Citrix Virtual Desktops Machine Creation Services (MCS) en el que se clonan muchas máquinas virtuales de una sola máquina virtual base, ya que reduce drásticamente la cantidad de bloques leídos del disco.
- **PVS-Accelerator**: La función PVS-Accelerator de XenServer ofrece capacidades ampliadas para los clientes que usan XenServer con Citrix Provisioning. PVS-Accelerator ofrece muchos beneficios, como la localización de los datos, la mejora de la experiencia del usuario final, la aceleración de los arranques y múltiples arranques simultáneos de máquinas virtuales, la simplificación de la escalabilidad horizontal mediante la adición de más hosts de hipervisor y la reducción del coste total de propiedad y de los requisitos de infraestructura.
- **Compatibilidad fluida con itinerancia para el modo tableta de escritorio virtual**: XenServer, junto con Citrix Virtual Apps and Desktops, le permite disfrutar de la experiencia de Windows 10 Continuum en un entorno virtualizado.
- **Virtualización de gráficos**: XenServer ofrece la entrega virtual de estaciones de trabajo y aplicaciones gráficas profesionales en 3D en XenServer mediante transferencia de GPU (para GPU

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

NVIDIA, AMD e Intel) y uso compartido de GPU basado en hardware con NVIDIA vGPU™ e Intel GVT-G™.

Prácticas recomendadas

Al configurar y administrar su entorno de XenServer, puede tomar medidas para optimizar su funcionamiento con los productos Citrix.

Instalación y actualización

- Al instalar por primera vez los hosts de XenServer, puede habilitar Intellicache para almacenar en caché los datos de las máquinas virtuales de forma local y mejorar el rendimiento. Para obtener más información, consulte Intellicache.
- Si actualiza desde una versión anterior de Citrix Hypervisor o XenServer, el método que utilice para esta actualización puede depender de la carga de trabajo de Citrix Virtual Apps and Desktops. Para obtener más información, consulte Escenarios de actualización para Citrix Virtual Apps and Desktops.

Configuración del entorno

- El host XenServer viene instalado con un certificado TLS predeterminado. Sin embargo, para usar HTTPS para proteger la comunicación entre XenServer y Citrix Virtual Apps and Desktops, instale un certificado proporcionado por una entidad de certificación de confianza. Para obtener más información, consulte Instalar un certificado TLS en el host.

Uso de memoria

- Cuando XenServer se instala por primera vez, asigna una cantidad determinada de memoria al dominio de control. En muchos entornos de Citrix Virtual Apps and Desktops, se recomienda aumentar la cantidad de memoria asignada al dominio de control más allá de esta cantidad predeterminada.

  Aumente la memoria del dominio de control en los siguientes casos:

  - Está ejecutando muchas máquinas virtuales en el servidor
  - Está utilizando PVS-Accelerator
  - Está utilizando el almacenamiento en caché de lectura

  Para obtener información sobre cómo cambiar la cantidad de memoria del dominio de control y supervisar el comportamiento de la memoria, consulte Uso de memoria.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

layout: doc
description: Upgrade scenarios and recommendations for Citrix Virtual Apps and Desktops environments.—

Escenarios de actualización para XenServer y Citrix Virtual Apps and Desktops

XenServer contiene funciones y optimizaciones que lo convierten en un hipervisor ideal para su uso en el entorno de Citrix Virtual Apps and Desktops.

Si utiliza XenServer con Citrix Virtual Apps and Desktops, hay algunas consideraciones a la hora de realizar la actualización que no se tratan en el artículo principal de actualización: Actualizar desde una versión existente. Consulte este artículo y el artículo principal de actualización antes de iniciar la actualización de Citrix Hypervisor 8.2 a XenServer 8.

> **Importante:**
>
> Si usa su licencia de Citrix Virtual Apps and Desktops con sus hosts de Citrix Hypervisor 8.2 CU 1, esta licencia ya no se aplica a XenServer 8. En su lugar, debe obtener licencias de XenServer Premium Edition para cubrir todos los sockets de CPU de su grupo. Para obtener más información, consulte https://xenserver.com/buy.
>
> Los clientes actuales pueden solicitar participar en nuestra promoción y recibir hasta 10 000 licencias de socket de XenServer Premium Edition de forma gratuita. Más información.

Consideraciones al actualizar XenServer en un entorno de Citrix Virtual Apps and Desktops:

- Los hosts de XenServer se reinician dos veces como parte de una actualización. Al principio de la actualización, debe arrancar el servidor en el medio de instalación. Al final del proceso, el instalador reinicia el servidor para completar la actualización. Las máquinas virtuales de estos hosts se deben migrar o detener durante este tiempo.
- El enfoque que se utilice para actualizar XenServer depende del entorno de XenServer, del entorno de Citrix Virtual Apps and Desktops y de los tipos de máquinas y aplicaciones que aloje XenServer.
- Es posible que deba realizar algunos preparativos en el entorno de Citrix Virtual Apps and Desktops antes de iniciar la actualización de XenServer.
- Este artículo solo cubre los casos de uso en los que la carga de trabajo de Citrix Virtual Apps and Desktops se aloja en el grupo de XenServer. En este artículo no se tratan los casos en los que también aloja partes de la infraestructura de Citrix Virtual Apps and Desktops en máquinas

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

virtuales del grupo de XenServer. Tenga en cuenta estos componentes al planificar la actualización.

- Asegúrese de que la versión de Citrix Virtual Apps and Desktops que está utilizando sea compatible tanto para la versión de XenServer desde la que está actualizando como para la versión a la que está actualizando. Para obtener más información, consulte Hipervisores compatibles para Citrix Virtual Apps and Desktops (MCS) y Citrix Provisioning (PVS).
- El tiempo necesario para realizar la actualización y la posibilidad de que se produzca una interrupción del servicio dependen del enfoque de la actualización. La mejora completa de una agrupación completa puede tardar varias horas en completarse.
- En este artículo se presupone que el tiempo necesario para actualizar por completo un único host de XenServer es de 35 minutos. Este tiempo de actualización del host incluye el proceso de actualización y los reinicios necesarios.

Los enfoques descritos en este artículo tienen como objetivo guiarlo hacia un método de actualización que reduzca la posibilidad de interrupciones del servicio y permita que el proceso de actualización se ajuste a su período de mantenimiento. Sin embargo, en algunos casos, las interrupciones del servicio son inevitables. Si el proceso de actualización de XenServer no cabe en el período de mantenimiento, puede ejecutar el grupo en modo mixto durante un breve período de tiempo entre las ventanas de mantenimiento. Sin embargo, esto no se recomienda. Para obtener más información, consulte Grupos de modo mixto.

Durante el período de actualización y mantenimiento planificado de XenServer, siga estas restricciones:

- No intente reconfigurar la infraestructura del grupo que se está actualizando. Por ejemplo, no añada ni expulse anfitriones del grupo.
- No agregue, inicie ni detenga ninguna máquina virtual del grupo que se está actualizando.
- No actualice el catálogo durante la ventana.

Actualización gradual de versiones de grupos

Rolling Pool Upgrade es una función de XenServer diseñada para facilitar el proceso de actualización y minimizar el tiempo de inactividad.

El asistente **Rolling Pool Upgrade** de XenCenter lo guía a través del procedimiento de actualización y organiza la ruta de actualización automáticamente. Para los grupos, cada uno de los servidores del grupo se actualiza sucesivamente, empezando por el coordinador del grupo. Antes de iniciar una actualización, el asistente lleva a cabo una serie de comprobaciones previas. Estas comprobaciones previas garantizan que ciertas funciones de todo el grupo, como la alta disponibilidad, estén deshabilitadas temporalmente y que cada servidor del grupo esté preparado para la actualización. Solo hay un servidor fuera de línea a la vez. Todas las máquinas virtuales en ejecución se migran automáticamente fuera de cada servidor antes de que se instale la actualización en ese servidor.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puede usar Rolling Pool Upgrade para muchos de los casos de uso de Citrix Virtual Apps and Desktops que se describen en este artículo. Para cada uno, el tiempo de actualización es el mismo: el número de hosts del grupo multiplicado por el tiempo de actualización de un solo host. (**N x 35 minutos**). La posibilidad de que se produzca una interrupción de la máquina virtual depende de la carga de trabajo de Citrix Virtual Apps and Desktops y de la configuración del grupo de XenServer.

Incluso si tiene la intención de utilizar Rolling Pool Upgrade para actualizar su grupo de XenServer, revise la información de su entorno específico para asegurarse de que comprende las acciones previas de Citrix Virtual Apps and Desktops, cualquier consideración especial y el comportamiento esperado.

Casos de uso

En este artículo se identifican varios casos de uso generales. Para cada uno de estos casos de uso, asumimos que el grupo de XenServer aloja solo un tipo de carga de trabajo de Citrix Virtual Apps and Desktops. Si su grupo contiene una combinación de diferentes tipos de carga de trabajo, revise todos los casos que se aplican a su grupo para decidir cuál es su enfoque de actualización preferido.

En primer lugar, tenga en cuenta cómo está configurado su entorno de XenServer:

- Grupo de XenServer con almacenamiento compartido

  En un grupo de XenServer con uno o más repositorios de almacenamiento compartido (SR), los discos de máquina virtual se pueden alojar en este almacenamiento compartido, lo que permite que las máquinas virtuales migren de un host a otro durante la actualización. Esta configuración puede reducir o eliminar la necesidad de tiempo de inactividad de las máquinas virtuales.

- Grupo de XenServer sin almacenamiento compartido ni host independiente

  En un grupo de XenServer sin almacenamiento compartido o en un host de XenServer independiente, las máquinas virtuales no pueden migrar durante el proceso de actualización. Cuando el host se reinicie como parte de la actualización, debe apagar las máquinas virtuales.

Grupo de XenServer con almacenamiento compartido

Si va a actualizar un grupo en el que los discos de máquina virtual se encuentran en un almacenamiento compartido, puede evacuar las máquinas virtuales de cada host de XenServer del grupo mientras se actualiza.

La mayoría de los casos de uso de este tipo de grupos se pueden actualizar mediante Rolling Pool Upgrade. Sin embargo, las acciones previas necesarias en Citrix Virtual Apps and Desktops y el comportamiento de las interrupciones varían según la carga de trabajo.

Tenga en cuenta qué tipo de carga de trabajo de Citrix Virtual Apps and Desktops está alojada en su grupo:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Escritorios de sesión única sin asignar
- Otras cargas de trabajo

Grupo de XenServer sin almacenamiento compartido ni host independiente

Si está actualizando un grupo en el que los discos de máquina virtual están ubicados en el almacenamiento local o si tiene un solo host en su grupo, las máquinas virtuales no se pueden migrar de los hosts de XenServer mientras se actualizan. En estos casos, las máquinas virtuales deben apagarse mientras dure la actualización del host o del grupo. En estos casos, es inevitable que se produzcan algunas interrupciones en sus aplicaciones y escritorios virtuales.

Tenga en cuenta qué tipo de carga de trabajo de Citrix Virtual Apps and Desktops está alojada en su grupo:

- Escritorios asignados
- Otras cargas de trabajo

Caso 1: Escritorios de sesión única que se ejecutan en un grupo con almacenamiento compartido

Este caso de uso abarca grupos de XenServer con almacenamiento compartido cuya carga de trabajo principal son escritorios virtuales de sesión única con el tipo de asignación de máquinas aleatorias. Las máquinas de este tipo deben administrarse mediante Citrix Provisioning o Machine Creation Services.

Para cualquier carga de trabajo que administre Citrix Virtual Apps and Desktops, incluidas las que son administradas por Citrix Provisioning and Machine Creation Services, no puede mantener una carga de trabajo completa mientras se realiza la actualización. La administración de energía de las máquinas puede resultar problemática durante el proceso de actualización y no se puede deshabilitar la administración de energía sin deshabilitar también la creación de nuevas sesiones.

Opciones recomendadas para la actualización:

- Actualización gradual de versiones de grupos
  - Tiempo estimado de actualización: el número de hosts del grupo multiplicado por el tiempo de actualización de un solo host. (**N x 35 minutos**)
  - Comportamiento de interrupción: todas las máquinas están en modo de mantenimiento de Citrix Virtual Apps and Desktops durante todo el tiempo de actualización.

Si es posible, haga que la carga de trabajo esté disponible en otros grupos de XenServer con capacidad durante la actualización de este grupo. Este enfoque puede provocar una reducción de la capacidad durante la actualización. Si no tiene capacidad para la carga de trabajo en los otros hosts y grupos

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de XenServer, le recomendamos que declare una interrupción en todas las máquinas de su carga de trabajo.

Mejora de la agrupación rodante (1)

Revisa los pasos y las instrucciones de Antes de empezar.

1. Pon todas las máquinas de la agrupación en modo de mantenimiento. Si todas las máquinas utilizan la misma conexión, puede poner todo el catálogo de máquinas en modo de mantenimiento.
2. Notifique a todos los usuarios afectados de la interrupción inminente.
   - Si las sesiones siguen ejecutándose en las máquinas de este grupo, pida a los usuarios que cierren sesión o fuerce la finalización de sus sesiones.
   - Informe a los usuarios de que, una vez que cierren la sesión, no podrán volver a iniciar sesión hasta que se reanude el servicio completo.
3. En XenCenter, inicie el asistente de actualización gradual de grupos y elija el modo automático. Para obtener más información, consulte Actualización gradual de grupos mediante XenCenter.

   Una vez finalizada la actualización, se reinician todas las máquinas virtuales que se suspendieron como parte de la actualización continua de la agrupación.
4. Saque las máquinas del modo de mantenimiento.

   Ahora se pueden iniciar nuevas sesiones y reanudar el servicio completo.

Caso 2: Otras cargas de trabajo que se ejecutan en un grupo con almacenamiento compartido

Este caso de uso abarca grupos de XenServer con almacenamiento compartido cuya carga de trabajo principal son escritorios virtuales de sesión única con el tipo de asignación de máquinas asignado o aplicaciones virtuales de sesión múltiple con el tipo de asignación de máquinas aleatorias.

Opciones recomendadas para la actualización:

- Actualización gradual de versiones de grupos
  - Tiempo estimado de actualización: el número de hosts del grupo multiplicado por el tiempo de actualización de un solo host. (**N x 35 minutos**)
  - Comportamiento de interrupción: sin interrupción del servicio

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Mejora de la agrupación rodante (2)

Revisa los pasos y las instrucciones de Antes de empezar.

1. Asegúrese de que el grupo tenga suficiente capacidad para ejecutar su carga de trabajo con un host menos en el grupo. Durante el proceso de actualización, cada host se elimina de uno en uno. Los hosts restantes deben poder ejecutar todas las máquinas virtuales necesarias.

   Si no hay suficiente capacidad en el grupo, es posible que algunas máquinas no estén disponibles durante el proceso de actualización. Si es posible, puede suspender cualquier máquina virtual que no sea crítica durante el proceso de actualización.

2. Asegúrese de que todas las máquinas proporcionadas por el grupo de XenServer estén encendidas y registradas en Citrix Virtual Apps and Desktops en los grupos de entrega correspondientes.

   - Para máquinas no administradas:
     - Use XenCenter para confirmar que todas las máquinas virtuales están encendidas.
     - No realice ninguna acción manual de alimentación durante el proceso de actualización.
   - Para máquinas con administración de energía:
     - Asegúrese de que todas las máquinas estén encendidas (mediante XenCenter, Citrix Studio o Web Studio).
     - **Para permitir que se inicien nuevas sesiones durante el proceso de actualización:**
       * No ponga las máquinas en modo de mantenimiento.
       * No realice ninguna acción manual de alimentación durante el proceso de actualización.
       * Deshabilite cualquier esquema de administración de energía que pueda suspender las máquinas.
       * Asegúrese de que no haya otros procesos que puedan apagar o suspender las máquinas.
     - **Si es aceptable que las sesiones nuevas no puedan iniciarse durante la actualización:**
       * Pon la conexión de alojamiento en modo de mantenimiento. Para obtener más información, consulte Activar o desactivar el modo de mantenimiento para una conexión.
       * Informe a los usuarios finales de que, si cierran sesión, no podrán volver a conectarse durante la actualización.

     Para obtener más información, consulte Máquinas administradas de energía en un grupo de entrega.
   - Para máquinas administradas por Machine Creation Services

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Siga las mismas instrucciones que para las máquinas con administración de energía del elemento de la lista anterior.
  - Además, no intente crear máquinas nuevas durante todo el período de actualización.

3. En XenCenter, inicie el asistente de actualización gradual de grupos y elija el modo automático. Para obtener más información, consulte Actualización gradual de grupos mediante XenCenter.
4. Restaure las operaciones de su entorno a su configuración habitual.

   - Elimine todos los indicadores del modo de mantenimiento establecidos en los pasos anteriores.
   - Revierta cualquier ajuste del esquema de administración de energía realizado en los pasos anteriores.

Caso 3: Escritorios asignados que se ejecutan en un grupo con almacenamiento local o en un host independiente

Este caso de uso abarca los hosts o grupos independientes de XenServer que no tienen almacenamiento compartido y cuya carga de trabajo principal son escritorios virtuales de sesión única con el tipo de asignación de máquinas asignado.

Opciones recomendadas para la actualización:

- Rolling Pool Upgrade Utilice la RPU en modo automático en una sola ventana de mantenimiento. Esto requiere que todos los usuarios tengan una interrupción durante toda la actualización, pero supone una menor sobrecarga de administración para un grupo
  - Tiempo estimado de actualización: el número de hosts del grupo multiplicado por el tiempo de actualización de un solo host. (**N x 35 minutos**)
  - Comportamiento de interrupción: todas las máquinas están en modo de mantenimiento de Citrix Virtual Apps and Desktops durante todo el tiempo de actualización.
- Actualización manual: Este modo proporciona la menor interrupción para cada usuario durante la actualización, pero es más complicado para el administrador
  - Tiempo estimado de actualización: dos veces el tiempo de actualización de un solo host. (**Aproximadamente 70 minutos**)
  - Comportamiento de interrupción: cada escritorio no está disponible durante el tiempo de actualización para su host individual. Este tiempo suele ser de 35 minutos.

Mejora de la agrupación rodante (3)

Revisa los pasos y las instrucciones de Antes de empezar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Coloque todos los grupos de entrega o catálogos que proporcionan máquinas del grupo en modo de mantenimiento.

   Mientras las máquinas estén en modo de mantenimiento, no se pueden iniciar nuevas sesiones en las máquinas del grupo. Las sesiones existentes se mantienen hasta que las máquinas se apaguen o suspendan.

   Para obtener más información, consulte Impedir que los usuarios se conecten a una máquina de un grupo de entrega.

2. Notifique a todos los usuarios afectados de la interrupción inminente. Indique una hora en la que deben finalizar sus sesiones e indique cuándo se restablecerá el servicio.

3. Compruebe si hay sesiones restantes en las máquinas afectadas y tome las medidas adecuadas para estas sesiones.

4. En XenCenter, inicie el asistente de actualización gradual de grupos y elija el modo automático. Para obtener más información, consulte Actualización gradual de grupos mediante XenCenter.

   Una vez finalizada la actualización, se reinician todas las máquinas virtuales que se suspendieron como parte de la actualización continua de la agrupación.

5. Saque las máquinas del modo de mantenimiento.

   Ahora se pueden iniciar nuevas sesiones y reanudar el servicio completo.

Actualización manual (3)

Puede usar este proceso manual para actualizar primero el coordinador del grupo y luego todos los demás hosts en paralelo, a fin de reducir significativamente el tiempo total de interrupción.

> **Nota:**
>
> Con el enfoque de actualización paralela, el perfil de riesgo cambia. Si hay algún problema durante la actualización, es posible que no se detecte hasta que todos los hosts se hayan actualizado y estén experimentando el problema. Mientras que si actualiza sus hosts de forma secuencial, puede comprobar que la actualización se ha realizado correctamente en cada host antes de pasar al siguiente.

Revisa los pasos y las instrucciones de Antes de empezar.

1. Asegúrese de que todas las máquinas proporcionadas por el grupo o el host de XenServer estén encendidas y registradas en Citrix Virtual Apps and Desktops en los grupos de entrega correspondientes.

   - Para máquinas no administradas:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Use XenCenter para confirmar que todas las máquinas virtuales están encendidas.
  - No realice ninguna acción manual de alimentación durante el proceso de actualización.

- Para máquinas con administración de energía:

  - Asegúrese de que todas las máquinas estén encendidas (mediante XenCenter o Studio).
  - **Para permitir que se inicien nuevas sesiones durante el proceso de actualización:**
    * No ponga las máquinas en modo de mantenimiento.
    * No realice ninguna acción manual de alimentación durante el proceso de actualización.
    * Deshabilite cualquier esquema de administración de energía que pueda suspender las máquinas.
    * Asegúrese de que no haya otros procesos que puedan apagar o suspender las máquinas.
  - **Si es aceptable que las sesiones nuevas no puedan iniciarse durante la actualización:**
    * Pon la conexión de alojamiento en modo de mantenimiento. Para obtener más información, consulte Activar o desactivar el modo de mantenimiento para una conexión.
    * Informe a los usuarios finales de que, si cierran sesión, no podrán volver a conectarse durante la actualización.

  Para obtener más información, consulte Máquinas administradas de energía en un grupo de entrega.

- Para máquinas administradas por Machine Creation Services

  - Siga las mismas instrucciones que para las máquinas con administración de energía del elemento de la lista anterior.
  - Además, no intente crear máquinas durante todo el período de actualización.

2. Identifique al coordinador del grupo y las máquinas virtuales asociadas.
3. Coloque las máquinas del catálogo del host del coordinador de grupos en modo de mantenimiento.
4. Use Director, Citrix Studio o Web Studio para enviar mensajes a los usuarios que aún están conectados a las sesiones activas, avisándoles de que su escritorio se quedará sin conexión durante un período. Este período es el tiempo de actualización de este host individual (aproximadamente 35 minutos).
5. Actualice el coordinador del grupo mediante la CLI xe:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a) Desactiva el coordinador de la agrupación. Esto impide que cualquier máquina virtual nueva se inicie o se migre al host especificado.

```
xe host-disable host=<uuid_or_name_label>
```

b) Asegúrese de que no haya máquinas virtuales ejecutándose en el coordinador del grupo. Cierre, suspenda o migre las máquinas virtuales a otros hosts del grupo.

- Para apagar una máquina virtual, utilice el siguiente comando:

```
xe vm-shutdown
```

- Para suspender una máquina virtual, utilice el siguiente comando:

```
xe vm-suspend
```

- Para migrar una máquina virtual específica, utilice el siguiente comando:

```
xe vm-migrate
```

La migración de máquinas virtuales específicas a hosts específicos le proporciona un control total sobre la distribución de las máquinas virtuales migradas a otros hosts del grupo.

- Para evacuar el anfitrión, utilice el siguiente comando:

```
xe host-evacuate
```

Al evacuar todas las máquinas virtuales de un host, se deja la distribución de las máquinas virtuales migradas a XenServer.

c) Cierre el coordinador de agrupaciones.

```
xe host-shutdown
```

> **Importante:**
>
> No puede ponerse en contacto con el coordinador de la agrupación hasta que se complete la actualización del coordinador de la agrupación. Al cerrar el coordinador de la agrupación, los demás anfitriones de la agrupación entran en *modo de emergencia.* Los anfitriones pueden entrar en modo de emergencia cuando se encuentran en un grupo cuyo coordinador de grupo ha desaparecido de la red y no se puede contactar con ellos tras varios intentos. Las VM siguen ejecutándose en hosts en modo de emergencia, pero las operaciones de control no están disponibles.

d) Arranque el coordinador del grupo mediante el medio de instalación de XenServer y el método que prefiera (por ejemplo, USB o red).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

e) Siga el procedimiento de instalación de XenServer hasta que el instalador le ofrezca la opción de actualizar. Elija actualizar.

Cuando el coordinador de la agrupación se reinicia, los demás anfitriones de la agrupación abandonan el modo de emergencia y el servicio normal se restablece después de unos minutos.

f) Inicie o reanude cualquier máquina virtual apagada o suspendida.

g) Migre las máquinas virtuales que quiera volver al coordinador del grupo.

Si algo interrumpe la actualización del coordinador del grupo o si la actualización falla por algún motivo, no intente continuar con la actualización. Reinicie el coordinador del grupo y restaure a una versión funcional.

6. Una vez actualizado el coordinador de grupos, saque las máquinas del coordinador de grupos del modo de mantenimiento en Citrix Studio o Web Studio.

7. Complete los siguientes pasos en paralelo para todos los hosts restantes del grupo:

a) Coloque las máquinas del catálogo del host en modo de mantenimiento.

b) Use Director, Citrix Studio o Web Studio para enviar mensajes a los usuarios que aún están conectados a las sesiones activas, avisándoles de que su escritorio se quedará sin conexión durante un período. Este período es el tiempo de actualización de este host individual (aproximadamente 35 minutos).

c) Inhabilite el host mediante la CLI xe.

```
xe host-disable host-selector=<host_selector_value>
```

d) Asegúrese de que no se ejecuten máquinas virtuales en el host. Cierre, suspenda o migre las máquinas virtuales a otros hosts del grupo.

- Para apagar una máquina virtual, utilice el siguiente comando:

```
xe vm-shutdown
```

- Para suspender una máquina virtual, utilice el siguiente comando:

```
xe vm-suspend
```

- Para migrar una máquina virtual específica, utilice el siguiente comando:

```
xe vm-migrate
```

La migración de máquinas virtuales específicas a hosts específicos le proporciona un control total sobre la distribución de las máquinas virtuales migradas a otros hosts del grupo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Para evacuar el anfitrión, utilice el siguiente comando:

```
xe host-evacuate
```

Al evacuar todas las máquinas virtuales de un host, se deja la distribución de las máquinas virtuales migradas a XenServer.

e) Apaga el host.

```
xe host-shutdown
```

f) Arranque el host mediante el medio de instalación de XenServer y el método que prefiera (por ejemplo, USB o red).

g) Siga el procedimiento de instalación de XenServer hasta que el instalador le ofrezca la opción de actualizar. Elija actualizar.

h) Una vez completada la actualización del host, inicie o reanude las máquinas virtuales apagadas o suspendidas.

i) Migre las máquinas virtuales que quiera volver al host.

Si la actualización de un host subordinado falla o se interrumpe, no es necesario revertirla. Ejecuta el comando `xe host-forget` en la agrupación para olvidar ese anfitrión. Vuelva a instalar XenServer en el host y, a continuación, únalo, como un nuevo host, al grupo mediante el comando. `xe pool-join`

8. Una vez actualizados los hosts de XenServer, saque las máquinas del modo de mantenimiento en Citrix Studio o Web Studio.

Caso 4: Otras cargas de trabajo que se ejecutan en un grupo con almacenamiento local o en un host independiente

Este caso de uso abarca grupos de XenServer con almacenamiento compartido cuya carga de trabajo principal son escritorios virtuales de sesión única o aplicaciones virtuales de sesión múltiple con el tipo de asignación de máquinas aleatorias.

Para cualquier carga de trabajo que administre Citrix Virtual Apps and Desktops, incluidas las que son administradas por Citrix Provisioning and Machine Creation Services, no puede mantener una carga de trabajo completa mientras se realiza la actualización. La administración de energía de las máquinas puede resultar problemática durante el proceso de actualización y no se puede deshabilitar la administración de energía sin deshabilitar también la creación de nuevas sesiones.

Opciones recomendadas para la actualización:

- Actualización gradual de versiones de grupos

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Tiempo estimado de actualización: el número de hosts del grupo multiplicado por el tiempo de actualización de un solo host. (**N x 35 minutos**)
  - Comportamiento de interrupción: todas las máquinas están en modo de mantenimiento de Citrix Virtual Apps and Desktops durante todo el tiempo de actualización.

- Actualización manual

  - Tiempo estimado de actualización: dos veces el tiempo de actualización de un solo host. (**Aproximadamente 70 minutos**)
  - Comportamiento de interrupción: todas las máquinas están en modo de mantenimiento de Citrix Virtual Apps and Desktops durante todo el tiempo de actualización.

Si es posible, haga que la carga de trabajo esté disponible en otros grupos de XenServer con capacidad durante la actualización de este grupo. Este enfoque puede provocar una reducción de la capacidad durante la actualización. Si no tiene capacidad para la carga de trabajo en los otros hosts y grupos de XenServer, le recomendamos que declare una interrupción en todas las máquinas de su carga de trabajo.

Mejora de la agrupación rodante (4)

Revisa los pasos y las instrucciones de Antes de empezar.

1. Pon todas las máquinas de la agrupación en modo de mantenimiento. Si todas las máquinas utilizan la misma conexión, puede poner todo el catálogo de máquinas en modo de mantenimiento.
2. Notifique a todos los usuarios afectados de la interrupción inminente.

   - Si las sesiones siguen ejecutándose en las máquinas de este grupo, pida a los usuarios que cierren sesión o fuerce la finalización de sus sesiones.
   - Informe a los usuarios de que, una vez que cierren la sesión, no podrán volver a iniciar sesión hasta que se reanude el servicio completo.

3. En XenCenter, inicie el asistente de actualización gradual de grupos y elija el modo automático. Para obtener más información, consulte Actualización gradual de grupos mediante XenCenter.

   Una vez finalizada la actualización, se reinician todas las máquinas virtuales que se suspendieron como parte de la actualización continua de la agrupación.

4. Saque las máquinas del modo de mantenimiento.

   Ahora se pueden iniciar nuevas sesiones y reanudar el servicio completo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Actualización manual (4)

Puede usar este proceso manual para actualizar primero el coordinador del grupo y luego todos los demás hosts en paralelo, a fin de reducir significativamente el tiempo total de interrupción.

> **Nota:**
>
> Con el enfoque de actualización paralela, el perfil de riesgo cambia. Si hay algún problema durante la actualización, es posible que no se detecte hasta que todos los hosts se hayan actualizado y estén experimentando el problema. Mientras que si actualiza sus hosts de forma secuencial, puede comprobar que la actualización se ha realizado correctamente en cada host antes de pasar al siguiente.

Revisa los pasos y las instrucciones de Antes de empezar.

1. Asegúrese de que todas las máquinas proporcionadas por el grupo o el host de XenServer estén encendidas y registradas en Citrix Virtual Apps and Desktops en los grupos de entrega correspondientes.

    - Para máquinas no administradas:
        - Use XenCenter para confirmar que todas las máquinas virtuales están encendidas.
        - No realice ninguna acción manual de alimentación durante el proceso de actualización.
    - Para máquinas con administración de energía:
        - Asegúrese de que todas las máquinas estén encendidas (mediante XenCenter o Studio).
        - **Para permitir que se inicien nuevas sesiones durante el proceso de actualización:**
            * No ponga las máquinas en modo de mantenimiento.
            * No realice ninguna acción manual de alimentación durante el proceso de actualización.
            * Deshabilite cualquier esquema de administración de energía que pueda suspender las máquinas.
            * Asegúrese de que no haya otros procesos que puedan apagar o suspender las máquinas.
        - **Si es aceptable que las sesiones nuevas no puedan iniciarse durante la actualización:**
            * Pon la conexión de alojamiento en modo de mantenimiento. Para obtener más información, consulte Activar o desactivar el modo de mantenimiento para una conexión.
            * Informe a los usuarios finales de que, si cierran sesión, no podrán volver a conectarse durante la actualización.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para obtener más información, consulte Máquinas administradas de energía en un grupo de entrega.

- Para máquinas administradas por Machine Creation Services
  - Siga las mismas instrucciones que para las máquinas con administración de energía del elemento de la lista anterior.
  - Además, no intente crear máquinas durante todo el período de actualización.

2. Identifique al coordinador del grupo y las máquinas virtuales asociadas.
3. Coloque las máquinas del catálogo del host del coordinador de grupos en modo de mantenimiento.
4. Use Director, Citrix Studio o Web Studio para enviar mensajes a los usuarios que aún están conectados a las sesiones activas, avisándoles de que su escritorio se quedará sin conexión durante un período. Este período es el tiempo de actualización de este host individual (aproximadamente 35 minutos).
5. Actualice el coordinador del grupo mediante la CLI xe:

   a) Desactiva el coordinador de la agrupación. Esto impide que cualquier máquina virtual nueva se inicie o se migre al host especificado.

   ```
   1 xe host-disable host=<uuid_or_name_label>
   ```

   b) Asegúrese de que no haya máquinas virtuales ejecutándose en el coordinador del grupo. Cierre, suspenda o migre las máquinas virtuales a otros hosts del grupo.

   - Para apagar una máquina virtual, utilice el siguiente comando:

     ```
     1 xe vm-shutdown
     ```

   - Para suspender una máquina virtual, utilice el siguiente comando:

     ```
     1 xe vm-suspend
     ```

   - Para migrar una máquina virtual específica, utilice el siguiente comando:

     ```
     1 xe vm-migrate
     ```

     La migración de máquinas virtuales específicas a hosts específicos le proporciona un control total sobre la distribución de las máquinas virtuales migradas a otros hosts del grupo.

   - Para evacuar el anfitrión, utilice el siguiente comando:

     ```
     1 xe host-evacuate
     ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Al evacuar todas las máquinas virtuales de un host, se deja la distribución de las máquinas virtuales migradas a XenServer.

c) Cierre el coordinador de agrupaciones.

```
xe host-shutdown
```

> **Importante:**
>
> No puede ponerse en contacto con el coordinador de la agrupación hasta que se complete la actualización del coordinador de la agrupación. Al cerrar el coordinador de la agrupación, los demás anfitriones de la agrupación entran en *modo de emergencia.* Los anfitriones pueden entrar en modo de emergencia cuando se encuentran en un grupo cuyo coordinador de grupo ha desaparecido de la red y no se puede contactar con ellos tras varios intentos. Las VM siguen ejecutándose en hosts en modo de emergencia, pero las operaciones de control no están disponibles.

d) Arranque el coordinador del grupo mediante el medio de instalación de XenServer y el método que prefiera (por ejemplo, USB o red).

e) Siga el procedimiento de instalación de XenServer hasta que el instalador le ofrezca la opción de actualizar. Elija actualizar.

Cuando el coordinador de la agrupación se reinicia, los demás anfitriones de la agrupación abandonan el modo de emergencia y el servicio normal se restablece después de unos minutos.

f) Inicie o reanude cualquier máquina virtual apagada o suspendida.

g) Migre las máquinas virtuales que quiera volver al coordinador del grupo.

Si algo interrumpe la actualización del coordinador del grupo o si la actualización falla por algún motivo, no intente continuar con la actualización. Reinicie el coordinador del grupo y restaure a una versión funcional.

6. Una vez actualizado el coordinador de grupos, saque las máquinas del coordinador de grupos del modo de mantenimiento en Citrix Studio o Web Studio.

7. Complete los siguientes pasos en paralelo para todos los hosts restantes del grupo:

a) Coloque las máquinas del catálogo del host en modo de mantenimiento.

b) Use Director, Citrix Studio o Web Studio para enviar mensajes a los usuarios que aún están conectados a las sesiones activas, avisándoles de que su escritorio se quedará sin conexión durante un período. Este período es el tiempo de actualización de este host individual (aproximadamente 35 minutos).

c) Inhabilite el host mediante la CLI xe.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe host-disable host-selector=<host_selector_value>
```

d) Asegúrese de que no se ejecuten máquinas virtuales en el host. Cierre, suspenda o migre las máquinas virtuales a otros hosts del grupo.

- Para apagar una máquina virtual, utilice el siguiente comando:

```
xe vm-shutdown
```

- Para suspender una máquina virtual, utilice el siguiente comando:

```
xe vm-suspend
```

- Para migrar una máquina virtual específica, utilice el siguiente comando:

```
xe vm-migrate
```

La migración de máquinas virtuales específicas a hosts específicos le proporciona un control total sobre la distribución de las máquinas virtuales migradas a otros hosts del grupo.

- Para evacuar el anfitrión, utilice el siguiente comando:

```
xe host-evacuate
```

Al evacuar todas las máquinas virtuales de un host, se deja la distribución de las máquinas virtuales migradas a XenServer.

e) Apaga el host.

```
xe host-shutdown
```

f) Arranque el host mediante el medio de instalación de XenServer y el método que prefiera (por ejemplo, USB o red).

g) Siga el procedimiento de instalación de XenServer hasta que el instalador le ofrezca la opción de actualizar. Elija actualizar.

h) Una vez completada la actualización del host, inicie o reanude las máquinas virtuales apagadas o suspendidas.

i) Migre las máquinas virtuales que quiera volver al host.

Si la actualización de un host subordinado falla o se interrumpe, no es necesario revertirla. Ejecuta el comando `xe host-forget` en la agrupación para olvidar ese anfitrión. Vuelva a instalar XenServer en el host y, a continuación, únalo, como un nuevo host, al grupo mediante el comando. `xe pool-join`

8. Una vez actualizados los hosts de XenServer, saque las máquinas del modo de mantenimiento en Citrix Studio o Web Studio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Piscinas de modo mixto

Un grupo de modo mixto es aquel en el que los hosts del grupo utilizan diferentes versiones de XenServer. No opere el grupo en modo mixto (con varias versiones de XenServer) durante más tiempo del necesario, ya que el grupo funciona en un estado degradado durante la actualización. En este estado degradado, se bloquean determinadas operaciones de VM, SR, VDI y host. Las máquinas virtuales que se han ejecutado en un host en la versión superior de XenServer no se pueden migrar ni iniciar en un host en la versión inferior de XenServer.

Los grupos de modo mixto no se admiten para el uso estándar y solo se admiten como estado de transición durante la actualización de un grupo. Si tiene algún problema mientras ejecuta en modo mixto, el soporte técnico le pedirá que complete la actualización de su grupo y, a continuación, reproduzca el problema en un grupo no mixto.

Tras revisar las opciones de actualización del entorno de Citrix Virtual Apps and Desktops, la ruta de actualización de XenServer planificada puede tardar más que el período de mantenimiento disponible. Si es posible, amplíe el período de mantenimiento para permitir que la actualización de XenServer se complete dentro de él. Si esto no es posible, puede optar por ejecutar la agrupación en modo mixto hasta la próxima ventana de mantenimiento. Sin embargo, el funcionamiento de su agrupación en modo mixto aumenta la probabilidad de que se produzcan comportamientos o problemas inesperados que podrían hacer que, en su lugar, necesite un período de mantenimiento de emergencia. Planifique minimizar el tiempo que su agrupación pasa en modo mixto.

Si su entorno de Citrix Virtual Apps and Desktops se ejecuta temporalmente sobre un grupo de XenServer de modo mixto, tenga en cuenta los siguientes comportamientos:

- En el caso de las cargas de trabajo de escritorios agrupados que requieren que las máquinas virtuales se reinicien antes de volver a utilizarse, las máquinas virtuales se reinician solo en los hosts que ejecutan la versión más reciente de XenServer. La capacidad efectiva de la agrupación está restringida. Según el número de hosts de su grupo que se hayan actualizado, es posible que no haya capacidad suficiente para reiniciar todas las máquinas virtuales necesarias. Este comportamiento puede provocar errores y es posible que algunos usuarios de Citrix Virtual Apps and Desktops no puedan acceder a las sesiones necesarias.
- Si tiene máquinas dedicadas que utilizan almacenamiento local y están ubicadas en hosts que ejecutan la versión anterior de XenServer, estas máquinas virtuales se pueden detener, pero no se pueden reiniciar hasta que se complete la actualización y el grupo deje de estar en modo mixto.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

IntelliCache

April 10, 2024

> **Nota:**
>
> Esta función solo se admite cuando se usa XenServer Premium Edition con Citrix Virtual Desktops.
>
> Intellicache no es compatible con las máquinas virtuales que utilizan un SR de GFS2 o XFS.

El uso de XenServer con *IntelliCache* hace que las implementaciones de infraestructura de escritorios virtuales alojados sean más rentables al permitirle usar una combinación de almacenamiento compartido y almacenamiento local. Resulta especialmente beneficioso cuando muchas máquinas virtuales (VM) comparten una imagen de sistema operativo común. La carga en el arreglo de almacenamiento se reduce y se mejora el rendimiento. Además, el tráfico de red hacia y desde el almacenamiento compartido se reduce a medida que el almacenamiento local almacena en caché la imagen principal del almacenamiento compartido.

IntelliCache funciona almacenando en caché los datos de una VDI principal de VM en el almacenamiento local en el host de la VM. Esta memoria caché local se rellena a medida que se leen los datos de la VDI principal. Cuando muchas VM comparten una VDI principal común, una VM puede usar los datos leídos en la memoria caché desde otra VM. No se requiere más acceso a la imagen principal en el almacenamiento compartido.

Se requiere un SR local de aprovisionamiento fino para IntelliCache. El aprovisionamiento controlado es una forma de optimizar el uso del almacenamiento disponible. Este enfoque le permite hacer más uso del almacenamiento local en lugar del almacenamiento compartido. Se basa en la asignación bajo demanda de bloques de datos. En otros enfoques, todos los bloques se asignan por adelantado.

> **Importante:**
>
> Thin Provisioning cambia el tipo de almacenamiento local predeterminado del host de LVM a EXT4. El aprovisionamiento ligero **debe estar** habilitado para que el almacenamiento en caché local de Citrix Virtual Desktops funcione correctamente.

El aprovisionamiento controlado permite al administrador presentar más espacio de almacenamiento a las máquinas virtuales que se conectan al repositorio de almacenamiento (SR) del que está disponible en el SR. No hay garantías de espacio y la asignación de un LUN no reclama ningún bloque de datos hasta que la VM escribe datos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Advertencia:**
>
> Los SR con aprovisionamiento fino pueden quedarse sin espacio físico, ya que las máquinas virtuales que contienen pueden crecer hasta consumir capacidad de disco a pedido. Las máquinas virtuales de IntelliCache gestionan esta condición recurriendo automáticamente al almacenamiento compartido cuando la memoria caché de SR local está llena. No mezcle máquinas virtuales tradicionales y máquinas virtuales de IntelliCache en la misma SR, ya que las máquinas virtuales de IntelliCache pueden aumentar rápidamente de tamaño.

Implementación de IntelliCache

IntelliCache debe habilitarse durante la instalación del host o habilitarse manualmente en un host en ejecución mediante la CLI.

Le recomendamos que utilice un dispositivo de almacenamiento local de alto rendimiento para garantizar la transferencia de datos lo más rápida posible. Por ejemplo, utilice un disco de estado sólido o una matriz RAID de alto rendimiento. Tenga en cuenta el rendimiento de datos y la capacidad de almacenamiento al dimensionar los discos locales El tipo de almacenamiento compartido, utilizado para alojar la imagen de disco virtual (VDI) de origen, debe basarse en NFS o EXT3/EXT4.

Habilitar la instalación en host

Para habilitar IntelliCache durante la instalación del host, en la pantalla **Almacenamiento de máquinas virtuales**, seleccione **Habilitar aprovisionamiento ligero**. Esta opción selecciona el SR local del host para que sea el que se utilizará para el almacenamiento en caché local de los VDI de VM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Convertir un host existente para usar aprovisionamiento controlado

Para eliminar un SR local de LVM existente y sustituirlo por un SR EXT3/EXT4 de aprovisionamiento fino, introduzca los siguientes comandos.

> **Advertencia:**
>
> Estos comandos eliminan el SR local existente y las VM del SR se eliminan permanentemente.

```
    localsr=`xe sr-list type=lvm host=hostname params=uuid --minimal`
        echo localsr=$localsr
        pbd=`xe pbd-list sr-uuid=$localsr params=uuid --minimal`
        echo pbd=$pbd
        xe pbd-unplug uuid=$pbd
        xe pbd-destroy uuid=$pbd
        xe sr-forget uuid=$localsr
        sed -i "s/'lvm'/'ext'/" /etc/firstboot.d/data/default-storage.
           conf
        rm -f /var/lib/misc/ran-storage-init
        systemctl restart storage-init.service
        xe sr-list type=ext
<!--NeedCopy-->
```

Para habilitar el almacenamiento en caché local, introduzca los siguientes comandos:

```
    xe host-disable host=hostname
        localsr=`xe sr-list type=ext host=hostname params=uuid --
           minimal`
        xe host-enable-local-storage-caching host=hostname sr-uuid=
           $localsr
        xe host-enable host=hostname
<!--NeedCopy-->
```

Comportamiento de las máquinas virtuales con Intellicache

El indicador VDI dicta `on-boot`el comportamiento de una VDI de máquina virtual cuando se arranca la máquina virtual y el indicador VDI dicta `allow-caching`el comportamiento del almacenamiento en caché.

Los valores que se deben usar para estos parámetros dependen del tipo de máquina virtual que esté creando y de su uso previsto:

- **Para máquinas compartidas o asignadas de forma aleatoria:**
  - Establezca el parámetro `on-boot` en `reset`.
  - Establezca el `allow-caching`parámetro en **`true`**

  Por ejemplo:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe vdi-param-set uuid=vdi_uuid on-boot=reset allow-caching=true
<!--NeedCopy-->
```

En el arranque de la VM, la VDI se revierte al estado en el que se encontraba en el arranque anterior. Todos los cambios durante la ejecución de la máquina virtual se pierden la próxima vez que se inicia la máquina virtual. Los datos de las nuevas VM se escriben solo en el almacenamiento local. No hay escrituras en el almacenamiento compartido. Este enfoque significa que se reduce la carga en el almacenamiento compartido. Sin embargo, la VM no se puede migrar entre hosts.

Seleccione esta opción si planea entregar escritorios estandarizados en los que los usuarios no puedan realizar cambios permanentes.

- **Para máquinas estáticas o dedicadas:**
  - Establezca el parámetro `on-boot` en `persist`.
  - Establezca el `allow-caching`parámetro en **`true`**

Por ejemplo:

```
xe vdi-param-set uuid=vdi_uuid on-boot=persist allow-caching=true
<!--NeedCopy-->
```

En el arranque de la VM, la VDI se encuentra en el estado en que se quedó en el último apagado. Los nuevos datos de VM se escriben tanto en el almacenamiento local como en el compartido. Las lecturas de datos almacenados en caché no requieren tráfico de E/S para el almacenamiento compartido, por lo que se reduce la carga en el almacenamiento compartido. Se permite la migración de máquinas virtuales a otro host y la caché local del nuevo host se rellena a medida que se leen los datos.

Seleccione esta opción si va a permitir que los usuarios realicen cambios permanentes en sus escritorios.

> **Nota:**
>
> En el caso de las máquinas virtuales cuyos VDI se encuentran en un SR de GFS2, el comportamiento de la máquina virtual durante el arranque es diferente al de las máquinas virtuales con VDI en otros tipos de SR. Para los VDI de una SR de GFS2, la opción de arranque se aplica al apagar la máquina virtual, no al iniciar la máquina virtual.

Detalles de implementación y solución de problemas

P: ¿ IntelliCache es compatible con la migración en vivo y la alta disponibilidad?

R: Puede utilizar la migración en vivo y la alta disponibilidad con IntelliCache cuando los escritorios virtuales están en modo privado, es decir, cuando `on-boot=persist`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Advertencia:**
>
> No se puede migrar una máquina virtual si cualquiera de sus VDI tiene indicadores de comportamiento de almacenamiento en caché establecidos en `on-boot=reset` y `allow-caching=true`. Los intentos de migración de máquinas virtuales con estas propiedades fallan.

P: ¿Dónde se encuentra la memoria caché local en el disco local?

R: La memoria caché vive en un repositorio de almacenamiento (SR). Cada host tiene un parámetro de configuración (denominado local-cache-sr) que indica qué SR (local) se va a utilizar para los archivos de caché. Normalmente, esta SR es una SR de tipo EXT3/EXT4. Cuando ejecuta máquinas virtuales con IntelliCache, ve archivos dentro del SR con nombres `uuid.vhdcache`. Este archivo es el archivo de caché para la VDI con el UUID dado. Estos archivos no se muestran en XenCenter; la única forma de verlos es iniciando sesión en dom0 y enumerando el contenido de `/var/run/sr-mount/sr-uuid`

P: ¿Cómo especifico un SR concreto para usarlo como caché?

A: El campo de objeto de host `local-cache-sr` hace referencia a un SR local. Puede ver su valor ejecutando el siguiente comando:

```
1 xe sr-list params=local-cache-sr,uuid,name-label
2 <!--NeedCopy-->
```

Este campo se establece:

- Tras la instalación del host, si ha elegido la opción “Habilitar aprovisionamiento delgado”en el instalador del host, o
- Corriendo `xe host-enable-local-storage-caching host=host sr-uuid=sr`. El comando requiere que el host especificado esté inhabilitado. Apague las máquinas virtuales cuando use este comando.

La primera opción utiliza el SR local de tipo EXT3/EXT4 y se crea durante la instalación del host. La segunda opción usa el SR que se especifica en la línea de comandos.

> **Advertencia:**
>
> Estos pasos solo son necesarios para los usuarios que han configurado más de una SR local.

P: ¿ Cuándo se elimina la memoria caché local?

R: Un archivo de caché de VDI solo se elimina cuando se elimina la propia VDI. La memoria caché se restablece cuando se conecta una VDI a una VM (por ejemplo, al iniciarse la VM). Si el host está fuera de línea cuando elimina la VDI, la sincronización de SR que se ejecuta en la basura de inicio recopila el archivo de caché.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> El archivo de caché no se elimina del host cuando una máquina virtual migra a un host diferente o se cierra.

---

layout: doc
description: If you use Citrix Provisioning for image management and hosting for Citrix Virtual Apps and Desktops or Citrix DaaS, PVS-Accelerator dramatically improves the already excellent combination of XenServer and Citrix Provisioning.—

PVS-Accelerator

La función PVS-Accelerator de XenServer ofrece capacidades ampliadas para los clientes que utilizan XenServer con Citrix Provisioning. Citrix Provisioning es una opción popular para la administración y el alojamiento de imágenes para Citrix Virtual Apps and Desktops o Citrix DaaS. PVS-Accelerator mejora drásticamente la ya excelente combinación de XenServer y Citrix Provisioning. Algunas de las ventajas que ofrece esta nueva función son:

- **Localidad de datos:** utilice el rendimiento y la localidad de los dispositivos de memoria, SSD y NVM para las solicitudes de lectura, a la vez que reduce sustancialmente la utilización de la red.
- **Experiencia de usuario final mejorada:** la localidad de los datos permite reducir la latencia de E/S de lectura para los dispositivos de destino (VM) almacenados en caché, lo que acelera aún más las aplicaciones de los usuarios finales.
- Arranques**y tormentas de arranque acelerados de VM:** La reducción de la latencia de E/S de lectura y la eficiencia mejorada pueden acelerar los tiempos de arranque de la VM y permitir un rendimiento más rápido cuando muchos dispositivos se inician en un marco de tiempo limitado
- **Escalamiento horizontal simplificado mediante la adición de más hosts de hipervisores:** es posible que se necesiten menos servidores Citrix Provisioning, ya que la carga de almacenamiento se distribuye de manera eficiente en todos los hosts de XenServer. Las cargas pico se manejan mediante la memoria caché dentro de los hosts de origen.
- **Reducción del coste total de propiedad y requisitos de infraestructura simplificados:** menos servidores de Citrix Provisioning significa una reducción de los requisitos de hardware y licencia, además de una reducción de la sobrecarga de administración. La capacidad liberada está disponible para las cargas de trabajo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Notas:**
>
> PVS-Accelerator está disponible para los clientes de XenServer Premium Edition. Para usar la función PVS-Accelerator, actualice el servidor de licencias de Citrix a la versión 11.14 o posterior.
>
> Para usar PVS-Accelerator con máquinas virtuales habilitadas para UEFI, asegúrese de usar Citrix Provisioning 1906 o posterior.

Cómo funciona PVS-Accelerator

PVS-Accelerator emplea un mecanismo de proxy que reside en el dominio de control (dom0) de XenServer. Cuando esta función está habilitada, las solicitudes de lectura del dispositivo (VM) de destino de Citrix Provisioning se almacenan en caché directamente en la máquina host de XenServer. Estas solicitudes se almacenan en caché en la memoria física o en un repositorio de almacenamiento. Cuando las máquinas virtuales posteriores de ese host de XenServer realizan la misma solicitud de lectura, el disco virtual se transmite directamente desde la memoria caché, no desde el servidor Citrix Provisioning. La eliminación de la necesidad de transmitir desde el servidor de Citrix Provisioning reduce considerablemente la utilización y el procesamiento de la red en el servidor. Este enfoque da como resultado una mejora sustancial en el rendimiento de la VM.

Consideraciones

Tenga en cuenta lo siguiente cuando utilice la función PVS-Accelerator:

- Los dispositivos de destino de Citrix Provisioning conocen su estado de proxy. No se requiere ninguna configuración adicional una vez que se instala la capacidad.
- En entornos en los que varios servidores de Citrix Provisioning se implementan con el mismo VHD, pero tienen marcas de tiempo diferentes en el sistema de archivos, los datos pueden almacenarse en caché varias veces. Debido a esta limitación, recomendamos usar el formato VHDX en lugar de VHD para los discos virtuales.
- No utilice un rango de puertos grande para la comunicación con el servidor PVS. Rara vez es necesario configurar un rango de más de 20 puertos en el servidor PVS. Un amplio rango de puertos puede ralentizar el procesamiento de paquetes y aumentar el tiempo de arranque del dominio de control de XenServer cuando se usa PVS-Accelerator.
- Después de iniciar una VM con PVS-Accelerator habilitado, el estado de almacenamiento en caché de la VM se muestra en XenCenter:
  - En la ficha **PVS** del grupo o el host
  - En la ficha **General** de la VM

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- No puede ejecutar más de 200 máquinas virtuales habilitadas para PVS-Accelerator en un host de XenServer.
- Los clientes pueden confirmar el funcionamiento correcto del PVS-Accelerator mediante métricas de RRD en la ficha **Rendimiento** del host en XenCenter. Para obtener más información, consulte Supervisar y administrar su implementación.
- PVS-Accelerator requiere Citrix Provisioning 7.13 o posterior.
- Para usar PVS-Accelerator con máquinas virtuales habilitadas para UEFI, asegúrese de usar Citrix Provisioning 1906 o posterior.
- PVS-Accelerator está disponible para los clientes de XenServer Premium Edition.
- PVS-Accelerator requiere el servidor de licencias 11.14 o posterior.
- PVS-Accelerator utiliza las capacidades de OVS y, por lo tanto, no está disponible en hosts que usan Linux Bridge como back-end de red.
- PVS-Accelerator funciona en la primera interfaz de red virtual (VIF) de una VM en caché. Por lo tanto, conecte la primera VIF a la red de almacenamiento de Citrix Provisioning para que el almacenamiento en caché funcione.
- Actualmente, PVS-Accelerator no se puede usar en puertos de red que obligan a que las IP estén enlazadas a ciertas direcciones MAC. Esta funcionalidad del conmutador puede denominarse "IP Source Guard"o similar. En tales entornos, los destinos de PVS no se inician con el error "Tiempo de espera de solicitud de inicio de sesión agotado"después de activar PVS-Accelerator.

Habilitar PVS-Accelerator

Los clientes deben completar los siguientes parámetros de configuración en XenServer y Citrix Provisioning para habilitar la función PVS-Accelerator:

1. Configure PVS-Accelerator en XenServer mediante XenCenter o la CLI xe. Esta configuración incluye agregar un sitio de Citrix Provisioning y especificar la ubicación del almacenamiento en caché de Citrix Provisioning.
    - Para obtener instrucciones de la CLI, consulte *Configuración de PVS-Accelerator en XenServer mediante la CLI en la siguiente* sección.
    - Para obtener información sobre cómo configurar PVS-Accelerator mediante XenCenter, consulte PVS-Accelerator en la documentación de XenCenter.
2. Después de configurar PVS-Accelerator en XenServer, complete la configuración de la caché del sitio de PVS mediante la interfaz de usuario de PVS. Para obtener instrucciones detalladas, consulte Completar la configuración de caché en Citrix Provisioning.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuración de puertos

Citrix Provisioning Services usa los siguientes puertos:

- 6901, 6902, 6905: Se utilizan para la comunicación saliente del servidor de aprovisionamiento (paquetes destinados al dispositivo de destino)
- 6910: Se utiliza para el inicio de sesión del dispositivo de destino con Citrix Provisioning Services
- Puerto de dispositivo de destino configurable. El valor predeterminado es el puerto 6901.
- Intervalo de puertos de servidor configurable. El rango predeterminado es 6910-6930.

Para obtener información sobre los puertos que usa Citrix Provisioning Services, consulte Puertos de comunicación utilizados por XenServer .

El rango de puertos configurado en XenServer debe incluir todos los puertos en uso. Por ejemplo, use 6901-6930 para la configuración predeterminada.

> **Nota:**
>
> No utilice un rango de puertos grande para la comunicación con el servidor PVS. Rara vez es necesario configurar un rango de más de 20 puertos en el servidor PVS. Un amplio rango de puertos puede ralentizar el procesamiento de paquetes y aumentar el tiempo de arranque del dominio de control de XenServer cuando se usa PVS-Accelerator.

Configurar PVS-Accelerator en XenServer mediante la CLI

1. Ejecute el siguiente comando para crear una configuración de sitio de Citrix Provisioning en XenServer:

```
PVS_SITE_UUID=$(xe pvs-site-introduce name-label=My PVS Site)
```

2. Para cada host del grupo, especifique la memoria caché que se va a utilizar. Puede elegir almacenar la memoria caché en un repositorio de almacenamiento (SR) o en la memoria de dominio de control.

Configurar el almacenamiento en caché en un repositorio de almacenamiento Tenga en cuenta las siguientes funciones al elegir un repositorio de almacenamiento (SR) para el almacenamiento en caché:

Ventajas:

- Los datos leídos más recientemente se almacenan en caché en la memoria según el mejor esfuerzo posible. El acceso a los datos puede ser tan rápido como usar la memoria de dominio de control.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- La memoria caché puede ser mucho mayor cuando está en un SR. El coste del espacio de SR es normalmente una fracción del coste del espacio de memoria. El almacenamiento en caché en un SR puede quitarle más carga al servidor de Citrix Provisioning.
- No tiene que modificar la configuración de memoria del dominio de control. La memoria caché utiliza automáticamente la memoria disponible en el dominio de control y nunca provoca que el dominio de control se quede sin memoria.
- Los VDI de caché se pueden almacenar en almacenamiento compartido. Sin embargo, esta elección de almacenamiento rara vez tiene sentido. Este enfoque solo tiene sentido cuando el almacenamiento compartido es significativamente más rápido que el servidor de Citrix Provisioning.
- Puede usar un SR basado en archivos o en bloques para el almacenamiento en caché.

Desventajas:

- Si el SR es lento y los datos solicitados no están en el nivel de memoria, el proceso de almacenamiento en caché puede ser más lento que en un servidor de Citrix Provisioning remoto.
- Los VDI almacenados en caché que se almacenan en almacenamiento compartido no se pueden compartir entre hosts. Un VDI almacenado en caché es específico de un host.

Realice los siguientes pasos para configurar el almacenamiento en caché en un repositorio de almacenamiento:

1. Ejecute el siguiente comando para encontrar el UUID del SR que se va a usar para el almacenamiento en caché:

```
xe sr-list name-label=Local storage host=host-name-label --minimal
    )
<!--NeedCopy-->
```

2. Crea el almacenamiento en caché.

```
xe pvs-cache-storage-create host=host-name-label pvs-site-uuid=
    PVS_SITE_UUID \
          sr-uuid=SR_UUID size=10GiB
<!--NeedCopy-->
```

> **Nota:**
>
> Al seleccionar un repositorio de almacenamiento (SR), la función utiliza hasta el tamaño de caché especificado en el SR. También utiliza implícitamente la memoria de dominio de control disponible como nivel de caché de mejor esfuerzo.

Configuración del almacenamiento en caché en la memoria del dominio de control Tenga en cuenta las siguientes funciones al elegir la memoria de dominio de control para el almacenamiento en caché:

Ventajas:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El uso de memoria significa un rendimiento de lectura/escritura constantemente rápido al acceder o llenar la memoria caché.

Desventajas:

- El tamaño del hardware debe ser adecuado, ya que la RAM utilizada para el almacenamiento en caché no está disponible para las VM.
- La memoria del dominio de control debe ampliarse **antes de** configurar el almacenamiento en caché.

  > **Nota:**
  >
  > Si elige almacenar la memoria caché en la memoria de Control Domain, la función utiliza hasta el tamaño de caché especificado en la memoria de Control Domain. Esta opción solo está disponible después de que se haya asignado memoria adicional al dominio de control. Para obtener información sobre cómo aumentar la memoria del dominio de control, consulte Cambiar la cantidad de memoria asignada al dominio de control.

  Después de aumentar la cantidad de memoria asignada al dominio de control del host, la memoria adicional se puede asignar explícitamente para PVS-Accelerator.

  Realice los siguientes pasos para configurar el almacenamiento en caché en la memoria del dominio de control:

  1. Ejecute el siguiente comando para encontrar el UUID del host para configurarlo para el almacenamiento en caché:

     ```
     xe host-list name-label=host-name-label --minimal
     <!--NeedCopy-->
     ```

  2. Cree una SR del tipo especial `tmpfs`:

     ```
     xe sr-create type=tmpfs name-label=MemorySR host-uuid=
        HOST_UUID device-config:uri=""
     <!--NeedCopy-->
     ```

     > **Nota:**
     >
     > Para los SR del tipo especial `tmpfs`, el valor del parámetro requerido `name-label` no se tiene en cuenta y, en su lugar, se usa un nombre fijo.

  3. Ejecute el siguiente comando para crear el almacenamiento en caché:

     ```
     xe pvs-cache-storage-create host-uuid=HOST_UUID
     pvs-site-uuid=PVS_SITE_UUID sr-uuid=SR_UUID size=1GiB
     <!--NeedCopy-->
     ```

     Donde `SR_UUID` es el UUID del SR creado en el paso b

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Completar la configuración de caché en Citrix Provisioning

Tras configurar PVS-Accelerator en XenServer, lleve a cabo los siguientes pasos para completar la configuración de la caché del sitio de Citrix Provisioning.

En la consola de administrador de Citrix Provisioning, utilice Citrix Virtual Desktops Setup Wizard o Streaming VM Wizard (según el tipo de implementación) para acceder a la capacidad de proxy. Aunque ambos asistentes son similares y comparten muchas de las mismas pantallas, existen las siguientes diferencias:

- El **asistente de configuración de Citrix Virtual Desktops** se utiliza para configurar las máquinas virtuales que se ejecutan en el hipervisor XenServer que se controla mediante Citrix Virtual Desktops.
- El **asistente Streaming VM Wizard** se usa para crear máquinas virtuales en un host. No implica Citrix Virtual Desktops.

Inicie la consola de administrador de Citrix Provisioning:

1. Navegue hasta el sitio de Citrix Provisioning.
2. Seleccione el sitio de Citrix Provisioning y haga clic con el botón secundario para ver un menú
3. Elija el asistente adecuado en función de la implementación. Seleccione la opción **Habilitar PVS-Accelerator para todas las máquinas virtuales** para habilitar la función PVS-Accelerator.
4. Si habilita el almacenamiento en caché de discos virtuales por primera vez, aparecerá la pantalla **XenServer** en el asistente Streamed Virtual Machine Setup Wizard. Este muestra la lista de todos los sitios de Citrix Provisioning configurados en XenServer que aún no se han asociado a ningún sitio de Citrix Provisioning. Seleccione en la lista un sitio de Citrix Provisioning al que aplicar PVS-Accelerator. Esta pantalla no aparece cuando ejecuta el asistente para el mismo sitio de Citrix Provisioning con el mismo host de XenServer.
5. Haga clic en **Next** para completar la configuración de almacenamiento en caché.
6. Haga clic en **Finalizar** para aprovisionar Citrix Virtual Desktops o máquinas virtuales transmitidas y asociar el sitio de Citrix Provisioning seleccionado al PVS Accelerator de XenServer. Cuando se completa este paso, el botón **Ver servidores PVS** en la ventana de **configuración de PVS-Accelerator** se habilita en XenCenter. Al hacer clic en el botón **Ver servidores PVS**, se muestran las direcciones IP de todos los servidores PVS asociados al sitio de Citrix Provisioning.

Operación de almacenamiento en caché

La funcionalidad PVS-Accelerator almacena en caché:

- **Lee** desde discos virtuales pero no escribe ni lee desde una memoria caché de escritura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Basado en versiones de imágenes**. Varias VM comparten bloques en caché cuando usan la misma versión de imagen
- Dispositivos con cualquier tipo de memoria caché de escritura **no persistente**
- Discos virtuales con el **modo de acceso Imagen estándar**. No funciona para discos virtuales con el modo de acceso Private Image
- Dispositivos marcados como **de tipo Producción o Prueba**. Los dispositivos marcados como de tipo Mantenimiento no se almacenan en caché

Operaciones CLI del acelerador de PVS

La siguiente sección describe las operaciones que los clientes pueden realizar cuando utilizan PVS-Accelerator mediante la CLI. Los clientes también pueden realizar estas operaciones con XenCenter. Para obtener más información, consulte PVS-Accelerator en la documentación de XenCenter.

Ver las direcciones y puertos del servidor de Citrix Provisioning configurados por Citrix Provisioning

PVS-Accelerator funciona optimizando el tráfico de red entre una VM y el servidor de Citrix Provisioning. Al completar la configuración en el servidor de Citrix Provisioning, el servidor de Citrix Provisioning rellena los objetos de XenServer con sus `pvs-server` direcciones IP y puertos. Posteriormente, PVS-Accelerator utiliza esta información para optimizar específicamente el tráfico entre una máquina virtual y sus servidores de Citrix Provisioning. Los servidores de Citrix Provisioning configurados se pueden enumerar mediante el siguiente comando:

```
xe pvs-server-list pvs-site-uuid=PVS_SITE_UUID params=all
<!--NeedCopy-->
```

Configurar una VM para el almacenamiento en caché

PVS-Accelerator se puede habilitar para la VM mediante cualquiera de las siguientes herramientas:

- CLI Citrix Provisioning
- Asistente de configuración de Citrix Virtual Desktops
- Asistente Streamed VM Setup Wizard
- XenCenter
- La CLI xe

La CLI xe configura PVS-Accelerator mediante el VIF de una VM. Crea un proxy de Citrix Provisioning que vincula el VIF de la VM con un sitio de Citrix Provisioning.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para configurar una VM:

1. Busque el primer VIF de la VM para habilitar el almacenamiento en caché en él:

```
VIF_UUID=$(xe vif-list vm-name-label=pvsdevice_1 device=0 --
    minimal)
<!--NeedCopy-->
```

2. Cree el proxy de Citrix Provisioning

```
xe pvs-proxy-create pvs-site-uuid=PVS_SITE_UUID vif-uuid=$VIF_UUID
<!--NeedCopy-->
```

Inhabilitar el almacenamiento en caché de una VM

PVS-Accelerator se puede inhabilitar para una VM destruyendo el proxy de Citrix Provisioning que vincula el VIF de la VM con un `pvs-site`.

1. Busque el primer VIF de la VM:

```
VIF_UUID=$(xe vif-list vm-name-label=pvsdevice_1 device=0 --
    minimal)
<!--NeedCopy-->
```

2. Busque el proxy de Citrix Provisioning de la VM:

```
PVS_PROXY_UUID=$(xe pvs-proxy-list vif-uuid=$VIF_UUID --minimal)
<!--NeedCopy-->
```

3. Destruya el proxy Citrix Provisioning

```
xe pvs-proxy-destroy uuid=$PVS_PROXY_UUID
<!--NeedCopy-->
```

Eliminar el almacenamiento de PVS-Accelerator de un host o un sitio

Para eliminar el almacenamiento de PVS-Accelerator de un host o un sitio:

1. Encuentre el host para el que quiere destruir el almacenamiento:

```
HOST_UUID=$(xe host-list name-label=HOST_NAME --minimal)
<!--NeedCopy-->
```

2. Encuentre el UUID del objeto:

```
PVS_CACHE_STORAGE_UUID=$(xe pvs-cache-storage-list host-uuid=
    $HOST_UUID --minimal)
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Destruye el objeto:

```
xe pvs-cache-storage-destroy uuid=$PVS_CACHE_STORAGE_UUID
<!--NeedCopy-->
```

Olvídese de la configuración del acelerador de PVS para un sitio

Para olvidar la configuración del acelerador de PVS para un sitio:

1. Busque el sitio de Citrix Provisioning:

```
PVS_SITE_UUID=$(xe pvs-site-list name-label=My PVS Site)
<!--NeedCopy-->
```

2. Ejecute el siguiente comando para olvidar el sitio de Citrix Provisioning:

```
xe pvs-site-forget uuid=$PVS_SITE_UUID
<!--NeedCopy-->
```

---

layout: doc
description: Create resource pools to group your XenServer hosts and shared storage into a single managed entity.—

Hosts y grupos de recursos

En esta sección se describe cómo se pueden crear grupos de recursos mediante una serie de ejemplos utilizando la interfaz de línea de comandos (CLI) xe. Se presenta una configuración de almacenamiento compartido simple basada en NFS y se analizan varios ejemplos sencillos de administración de VM. También contiene procedimientos para tratar los fallos de los nodos físicos.

Descripción general de los hosts y grupos de recursos de XenServer

Un *grupo de recursos* comprende varias instalaciones host de XenServer, unidas a una sola entidad administrada que puede alojar máquinas virtuales. Si se combina con el almacenamiento compartido, un grupo de recursos permite iniciar las máquinas virtuales en *cualquier* host de XenServer que tenga suficiente memoria. Luego, las máquinas virtuales se pueden mover dinámicamente entre los hosts de XenServer mientras se ejecutan con un tiempo de inactividad mínimo (migración en vivo). Si un host de XenServer individual sufre un error de hardware, el administrador puede reiniciar las máquinas virtuales con errores en otro host de XenServer del mismo grupo de recursos. Cuando se

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

habilita la alta disponibilidad en el grupo de recursos, las máquinas virtuales se mueven automáticamente a otro host cuando su host falla. Se admiten hasta 64 hosts por grupo de recursos, aunque esta restricción no se aplica.

Un grupo siempre tiene al menos un nodo físico, conocido como *coordinador del grupo* (anteriormente "maestro del grupo"). El nodo coordinador expone una interfaz de administración (utilizada por XenCenter y la interfaz de línea de comandos de XenServer, conocida como CLI xe). El coordinador envía las órdenes a los miembros individuales según sea necesario.

> **Nota:**
>
> Cuando el coordinador del grupo fracasa, la reelección del coordinador se lleva a cabo solo si se habilita la alta disponibilidad.

Requisitos para crear grupos de recursos

Una agrupación de recursos es un agregado homogéneo (o heterogéneo con restricciones) de uno o más hosts XenServer, hasta un máximo de 64. La definición de homogéneo es:

- Las CPU del host que se une al grupo son las mismas (en términos de proveedor, modelo y funciones) que las CPU de los hosts que ya están en el grupo.
- El host que se une al grupo ejecuta la misma versión del software XenServer, con el mismo nivel de parche, que los hosts que ya están en el grupo.

El software impone restricciones adicionales al unir un anfitrión a un grupo. En concreto, XenServer comprueba que se cumplan las siguientes condiciones para el host que se une al grupo:

- El anfitrión no es miembro de un grupo de recursos existente.
- El host no tiene ningún almacenamiento compartido configurado.
- El host no aloja ninguna máquina virtual suspendida o en ejecución.
- No hay operaciones activas en curso en las máquinas virtuales del host, como el cierre de una máquina virtual.
- El reloj del host se sincroniza a la misma hora que el coordinador del grupo (por ejemplo, mediante NTP).
- La interfaz de administración del host no está vinculada. Puede configurar la interfaz de administración cuando el host se una correctamente al grupo.
- La dirección IP de administración es estática, ya sea configurada en el propio host o mediante una configuración adecuada en el servidor DHCP.

Los hosts de XenServer de los grupos de recursos pueden contener diferentes números de interfaces de red físicas y tener repositorios de almacenamiento local de distintos tamaños. En la práctica, a

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

menudo es difícil obtener varios hosts con exactamente las mismas CPU, por lo que se permiten pequeñas variaciones. Si es aceptable tener hosts con diferentes CPU como parte del mismo grupo, puede forzar la operación de unión de grupos pasando el parámetro `--force`.

Todos los hosts del grupo deben estar en el mismo sitio y conectados mediante una red de baja latencia.

> **Nota:**
>
> Los servidores que proporcionan almacenamiento NFS o iSCSI compartido para el grupo deben tener una dirección IP estática.

Un grupo debe contener repositorios de almacenamiento compartidos para seleccionar en qué host XenServer ejecutar una máquina virtual y para mover una máquina virtual entre los hosts de XenServer de forma dinámica. Si es posible, cree un grupo después de que haya almacenamiento compartido disponible. Le recomendamos que mueva las VM existentes con discos ubicados en el almacenamiento local al almacenamiento compartido después de agregar almacenamiento compartido. Puede usar el comando `xe vm-copy` o usar XenCenter para mover las máquinas virtuales.

Crear un grupo de recursos

Los grupos de recursos se pueden crear mediante XenCenter o la CLI. Cuando un nuevo host se une a un grupo de recursos, el host que se une sincroniza su base de datos local con la de todo el grupo y hereda algunos ajustes del grupo:

- La configuración de almacenamiento de VM, local y remoto se agrega a la base de datos de todo el grupo. Esta configuración se aplica al host que se une al grupo, a menos que haga que los recursos se compartan explícitamente después de que el host se una al grupo.
- El host que se une hereda los repositorios de almacenamiento compartidos existentes en el grupo. Se crean registros PBD apropiados para que el nuevo host pueda acceder automáticamente al almacenamiento compartido existente.
- La información de red se hereda parcialmente al host que se une: todos los detalles *estructurales* de las NIC, las VLAN y las interfaces enlazadas se heredan, pero la información de *directivas* no. Esta información de directiva, que debe reconfigurarse, incluye:
  - Las direcciones IP de las NIC de administración, que se conservan de la configuración original.
  - La ubicación de la interfaz de administración, que sigue siendo la misma que la configuración original. Por ejemplo, si los otros hosts del grupo tienen interfaces de administración en una interfaz enlazada, el host que se une se debe migrar al enlace después de unirse.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- NIC de almacenamiento dedicado, que deben reasignarse al host que se une desde XenCenter o la CLI, y los PBD se deben volver a conectar para redirigir el tráfico en consecuencia. Esto se debe a que las direcciones IP no se asignan como parte de la operación de unión de grupo y la NIC de almacenamiento solo funciona cuando está configurada correctamente. Para obtener más información sobre cómo dedicar una NIC de almacenamiento desde la CLI, consulte Administrar redes.

> **Nota:**
>
> Solo puede unir un nuevo host a un grupo de recursos cuando la interfaz de administración del host está en la misma VLAN etiquetada que la del grupo de recursos.

Agregar un host a una agrupación mediante la CLI xe

> **Nota:**
>
> Le recomendamos actualizar su grupo y el host que se une al mismo nivel antes de intentar unirse.

1. Abra una consola en el host de XenServer que quiera unir a un grupo.
2. Para unir el host de XenServer al grupo, ejecute el comando:

```
xe pool-join master-address=<address of pool coordinator> master-
   username=<administrator username> master-password=<password>
<!--NeedCopy-->
```

   `master-address` debe configurarse en el nombre de dominio completo del coordinador de la agrupación. `password` Debe ser la contraseña de administrador establecida cuando se instaló el coordinador de la agrupación.

> **Nota:**
>
> Al unir un anfitrión a un grupo, la contraseña de administrador del host que se une se cambia automáticamente para que coincida con la contraseña de administrador del coordinador del grupo.

De forma predeterminada, los hosts de XenServer pertenecen a un grupo sin nombre. Para crear su primer grupo de recursos, cambie el nombre del grupo sin nombre existente. Use tab-complete para encontrar `pool_uuid`:

```
xe pool-param-set name-label="New Pool" uuid=pool_uuid
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Crear grupos de recursos heterogéneos

XenServer simplifica la expansión de las implementaciones a lo largo del tiempo al permitir que hardware de host dispares se una a un grupo de recursos, conocido como grupos de recursos heterogéneos. Los grupos de recursos heterogéneos son posibles mediante el uso de tecnologías en las CPU Intel (FlexMigration) y AMD (migración extendida) que proporcionan "enmascaramiento"o "nivelación"de la CPU. Las funciones de enmascaramiento y nivelación de CPU permiten configurar una CPU para que *parezca* que proporciona una marca, modelo o funcionalidad diferente a la que realmente ofrece. Esta función le permite crear grupos de hosts con CPU diferentes, pero aun así admitir la migración en vivo de forma segura.

> **Nota:**
>
> Las CPU de los hosts XenServer que se unen a grupos heterogéneos deben ser del mismo proveedor (es decir, AMD o Intel) que las CPU de los hosts que ya están en el grupo. Sin embargo, no es necesario que los anfitriones sean del mismo tipo a nivel de familia, modelo o números escalonados.

XenServer simplifica el soporte de grupos heterogéneos. Los hosts ahora se pueden agregar a los grupos de recursos existentes, independientemente del tipo de CPU subyacente (siempre que la CPU pertenezca a la misma familia de proveedores). El conjunto de funciones del grupo se calcula dinámicamente cada vez:

- Un nuevo anfitrión se une al grupo
- Un miembro del grupo abandona el grupo
- Un miembro del grupo se vuelve a conectar después de reiniciar

Cualquier cambio en el conjunto de funciones del grupo no afecta a las máquinas virtuales que se ejecutan actualmente en el grupo. Una máquina virtual en ejecución sigue utilizando el conjunto de funciones que se aplicó cuando se inició. Este conjunto de funciones se corrige en el arranque y persiste en las operaciones de migración, suspensión y reanudación. Si el nivel del grupo disminuye cuando un host con menos capacidad se une al grupo, una VM en ejecución se puede migrar a cualquier host del grupo, excepto al host recién agregado. Al mover o migrar una máquina virtual a un host diferente dentro o entre grupos, XenServer compara el conjunto de funciones de la máquina virtual con el conjunto de funciones del host de destino. Si se determina que los conjuntos de funciones son compatibles, se permite la migración de la máquina virtual. Esto permite que la máquina virtual se mueva libremente dentro de los grupos y entre ellos, independientemente de las funciones de CPU que esté utilizando la máquina virtual. Si usa Equilibrio de carga de trabajo para seleccionar un host de destino óptimo para migrar su VM, no se recomendará un host con un conjunto de funciones incompatible como host de destino.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Agregar almacenamiento compartido

Para obtener una lista completa de los tipos de almacenamiento compartido admitidos, consulte Formatos de repositorio de almacenamiento. En esta sección se muestra cómo se puede crear el almacenamiento compartido (representado como un repositorio de almacenamiento) en un servidor NFS existente.

Para agregar almacenamiento compartido NFS a un grupo de recursos mediante la CLI

1. Abra una consola en cualquier host XenServer del grupo.
2. Cree el repositorio de almacenamiento en server: /path emitiendo el siguiente comando:

```
xe sr-create content-type=user type=nfs name-label="Example SR"
    shared=true \
     device-config:server=server \
     device-config:serverpath=path
<!--NeedCopy-->
```

   `device-config:server` es el nombre de host del servidor NFS y `device-config:serverpath` es la ruta del servidor NFS. Si `shared` se establece en true, el almacenamiento compartido se conecta automáticamente a todos los hosts de XenServer del grupo. Todos los hosts de XenServer que se unan más adelante también están conectados al almacenamiento. El identificador único universal (UUID) del repositorio de almacenamiento se imprime en la pantalla.

3. Busque el UUID del grupo ejecutando el siguiente comando:

```
xe pool-list
<!--NeedCopy-->
```

4. Establezca el almacenamiento compartido como el valor predeterminado de todo el grupo con el siguiente comando:

```
xe pool-param-set uuid=pool_uuid default-SR=sr_uuid
<!--NeedCopy-->
```

   Como el almacenamiento compartido se estableció como el valor predeterminado para todo el grupo, todas las máquinas virtuales futuras tendrán sus discos creados en almacenamiento compartido de forma predeterminada. Para obtener información sobre la creación de otros tipos de almacenamiento compartido, consulte Formatos de repositorio de almacenamiento.

Eliminar los hosts de XenServer de un grupo de recursos

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Antes de eliminar cualquier host de XenServer de un grupo, asegúrese de cerrar todas las máquinas virtuales que se ejecutan en ese host. De lo contrario, puede ver una advertencia que indica que el host no se puede eliminar.

Cuando elimina (*expulsa*) un host de una agrupación, la máquina se reinicia, se reinicializa y se deja en un estado similar al de una instalación nueva. No expulse los hosts XenServer de un grupo si hay datos importantes en los discos locales.

Para eliminar un host de un grupo de recursos mediante la CLI

1. Abra una consola en cualquier host del grupo.
2. Busque el UUID del host ejecutando el siguiente comando:

   ```
   xe host-list
   <!--NeedCopy-->
   ```

3. Expulse el host requerido del grupo:

   ```
   xe pool-eject host-uuid=host_uuid
   <!--NeedCopy-->
   ```

   El host XenServer se expulsa y se deja en un estado recién instalado.

   > **Advertencia:**
   >
   > *No* expulse un host de un grupo de recursos si contiene datos importantes almacenados en sus discos locales. Todos los datos se borran cuando se expulsa un host del grupo. Si quiere conservar estos datos, copie la máquina virtual en el almacenamiento compartido del grupo mediante XenCenter o el comando `xe vm-copy` de la CLI.

Cuando los hosts XenServer que contienen máquinas virtuales almacenadas localmente se expulsan de un grupo, las máquinas virtuales estarán presentes en la base de datos del grupo. Las máquinas virtuales almacenadas localmente también son visibles para los demás hosts de XenServer. Las máquinas virtuales no se inician hasta que los discos virtuales asociados a ellas se hayan cambiado para que apunten al almacenamiento compartido visto por otros hosts de XenServer del grupo o se hayan eliminado. Por lo tanto, le recomendamos que traslade cualquier almacenamiento local a un almacenamiento compartido cuando se una a un grupo. Pasar a un almacenamiento compartido permite expulsar (o fallar físicamente) los hosts individuales de XenServer sin pérdida de datos.

> **Nota:**
>
> Cuando se elimina un host de un grupo que tiene su interfaz de administración en una red VLAN

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> etiquetada, la máquina se reinicia y su interfaz de administración estará disponible en la misma red.

Prepare un grupo de hosts de XenServer para el mantenimiento

Antes de realizar operaciones de mantenimiento en un host que forma parte de un grupo de recursos, debe inhabilitarlo. La desactivación del host impide que las máquinas virtuales se inicien en él. A continuación, debe migrar sus máquinas virtuales a otro host de XenServer del grupo. Para ello, coloque el host de XenServer en modo de mantenimiento mediante XenCenter. Para obtener más información, consulte Ejecutar en modo de mantenimiento en la documentación de XenCenter.

La sincronización de reserva se produce cada 24 horas. Al poner el coordinador del grupo en modo de mantenimiento, se pierden las últimas 24 horas de actualizaciones de RRD para las máquinas virtuales sin conexión.

> **Advertencia:**
>
> Recomendamos encarecidamente reiniciar todos los hosts de XenServer antes de instalar una actualización y comprobar su configuración. Algunos cambios de configuración solo se aplican cuando se reinicia el host de XenServer, por lo que el reinicio puede detectar problemas de configuración que pueden provocar un error en la actualización.

Para preparar un host en un grupo para las operaciones de mantenimiento mediante la CLI

1. Ejecute este comando:

   ```
   xe host-disable uuid=XenServer_host_uuid
   xe host-evacuate uuid=XenServer_host_uuid
   <!--NeedCopy-->
   ```

   Este comando inhabilita el host de XenServer y, a continuación, migra las máquinas virtuales en ejecución a otros hosts de XenServer del grupo.

2. Realice la operación de mantenimiento deseada.

3. Habilite el host XenServer cuando se complete la operación de mantenimiento:

   ```
   xe host-enable
   <!--NeedCopy-->
   ```

4. Reinicie las máquinas virtuales detenidas y reanude las máquinas virtuales suspendidas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Exportar datos de la agrupación de recursos

La opción Exportar datos de recursos le permite generar un informe de datos de recursos para su grupo y exportar el informe a un archivo XLS o CSV. Este informe proporciona información detallada sobre varios recursos del grupo, como hosts, redes, almacenamiento, máquinas virtuales, VDI y GPU. Esta función permite a los administradores realizar un seguimiento, planificar y asignar recursos en función de diversas cargas de trabajo, como la CPU, el almacenamiento y la red.

> **Nota:**
>
> La exportación de datos de la agrupación de recursos está disponible para los clientes de XenServer Premium Edition.

La lista de recursos y varios tipos de datos de recursos que se incluyen en el informe:

Servidor:

- Nombre
- Coordinador de agrupaciones
- UUID
- Dirección
- Uso de CPU
- Red (kBs promedio/máximo)
- Memoria usada
- Almacenamiento
- Tiempo de actividad
- Descripción

Redes:

- Nombre
- Estado del enlace
- MAC
- MTU
- VLAN
- Tipo
- Ubicación

VDI:

- Nombre
- Tipo
- UUID
- Tamaño

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Almacenamiento
- Descripción

Almacenamiento:

- Nombre
- Tipo
- UUID
- Tamaño
- Ubicación
- Descripción

VM:

- Nombre
- Estado de energía
- Se ejecuta en
- Dirección
- MAC
- NIC
- Sistema operativo
- Almacenamiento
- Memoria usada
- Uso de CPU
- UUID
- Tiempo de actividad
- Plantilla
- Descripción

GPU:

- Nombre
- Servidores
- Ruta de bus PCI
- UUID
- Uso de energía
- Temperatura
- Memoria usada
- Utilización de equipos

> **Nota:**
>
> La información sobre las GPU solo está disponible si hay GPU conectadas al host de XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para exportar datos de recursos

1. En el panel de navegación de XenCenter, seleccione **Infraestructura** y, a continuación, seleccione la agrupación.
2. Seleccione el menú **Agrupación** y luego **Exportar datos de recursos**.
3. Vaya a la ubicación en la que quiera guardar el informe y, a continuación, haga clic en **Guardar**.

Encendido del host

Encender hosts de forma remota

Puede usar la función de encendido del host de XenServer para encender y apagar un host de forma remota, ya sea desde XenCenter o mediante la CLI.

Para habilitar la alimentación del host, el host debe tener una de las siguientes soluciones de control de energía:

- **Tarjeta de red habilitada para Wake on LAN**.
- **Tarjetas de acceso remoto de Dell (DRAC)**. Para usar XenServer con DRAC, debe instalar el paquete complementario de Dell para obtener soporte para DRAC. La compatibilidad con la DRAC requiere instalar la utilidad de línea de comandos RACADM en el host con la controladora de acceso remoto y habilitar la DRAC y su interfaz. RACADM se incluye a menudo en el software de administración de la DRAC. Para obtener más información, consulte la documentación de DRAC de Dell.
- Un script personalizado basado en la API de administración que le permite encender y apagar la alimentación a través de XenServer. Para obtener más información, consulte *Configuración de un script personalizado para la función de encendido del host* en la siguiente sección.

El uso de la función Host Power On requiere dos tareas:

1. Asegúrese de que los hosts del grupo admitan el control de la energía de forma remota. Por ejemplo, tienen la funcionalidad Wake on LAN o una tarjeta DRAC, o usted ha creado un script personalizado.
2. Habilite la funcionalidad de encendido del host mediante la CLI o XenCenter.

Usar la CLI para administrar el encendido del host

Puede administrar la función Host Power On mediante la CLI o XenCenter. En esta sección se proporciona información sobre cómo administrarlo con la CLI.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El encendido del host está habilitado en el nivel de host (es decir, en cada XenServer).

Después de habilitar el encendido del host, puede activar los hosts mediante la CLI o XenCenter.

Para habilitar el encendido del host mediante la CLI Ejecute el comando:

```
xe host-set-power-on-mode host=<host uuid> \
    power-on-mode=("" , "wake-on-lan", "DRAC","custom") \
    power-on-config=key:value
<!--NeedCopy-->
```

Para DRAC, las claves `power_on_ip` deben especificar la contraseña si está utilizando la función secreta. Para obtener más información, consulte Secretos.

Para activar hosts de forma remota mediante la CLI Ejecute el comando:

```
xe host-power-on host=<host uuid>
<!--NeedCopy-->
```

Configurar un script personalizado para la función Host Power On

Si la solución de alimentación remota de su anfitrión utiliza un protocolo que no es compatible de forma predeterminada (como Wake-On-Ring o la tecnología Intel Active Management), puede crear un script Python de Linux personalizado para encender los equipos XenServer de forma remota. Sin embargo, también puede crear scripts personalizados para las soluciones de energía remota DRAC y Wake on LAN.

En esta sección se proporciona información sobre la configuración de un script personalizado para Host Power On mediante los pares clave/valor asociados a la llamada a la API de XenServer. `host.power_on`

Cuando cree un script personalizado, ejecútelo desde la línea de comandos cada vez que quiera controlar la alimentación de forma remota en un host de XenServer. Como alternativa, puede especificarlo en XenCenter y usar las funciones de la interfaz de usuario de XenCenter para interactuar con él.

La API de XenServer está documentada en la API de administración de XenServer.

> **Advertencia:**
>
> No cambie los scripts proporcionados de forma predeterminada en el directorio `/etc/xapi.d/plugins/`. Puede incluir nuevos scripts en este directorio, pero nunca debe cambiar los scripts contenidos en ese directorio después de la instalación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pares clave/valor Para usar Host Power On, configure las teclas `host.power_on_mode` y `host.power_on_config`. Consulte la siguiente sección para obtener información sobre los valores.

También hay una llamada a la API que le permite configurar estos campos simultáneamente:

```
void host.set_host_power_on_mode(string mode, Dictionary<string,string>
    config)
<!--NeedCopy-->
```

host.power_on_mode

- **Definición**: contiene pares clave/valor para especificar el tipo de solución de alimentación remota (por ejemplo, DRAC de Dell).
- **Valores posibles**:
  - Una cadena vacía, que representa el control de potencia desactivado.
  - "DRAC": Le permite especificar Dell DRAC. Para usar la DRAC, ya debe haber instalado el paquete complementario de Dell.
  - "wake-on-lan": permite especificar Wake on LAN.
  - Cualquier otro nombre (utilizado para especificar un script de encendido personalizado). Esta opción se usa para especificar un script personalizado para la administración de energía.
- **Tipo**: cuerda

host.power_on_config

- **Definición**: contiene pares clave/valor para la configuración de modo. Proporciona información adicional para la DRAC.
- **Valores posibles:**
  - Si configuró la DRAC como el tipo de solución de energía remota, también debe especificar una de las siguientes claves:
    - "power_on_ip": La dirección IP que especificó configuró para comunicarse con la tarjeta de control de alimentación. Como alternativa, puede escribir el nombre de dominio de la interfaz de red en la que está configurada la DRAC.
    - "power_on_user": El nombre de usuario de la DRAC asociado al procesador de administración, que puede haber cambiado de su configuración predeterminada de fábrica.
    - "power_on_password_secret": Especifica el uso de la función de secretos para proteger su contraseña.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Para utilizar la función de secretos para almacenar su contraseña, especifique la clave "power_on_password_secret". Para obtener más información, consulte Secretos.

- **Tipo**: Asignación (cadena, cadena)

Script de ejemplo El script de ejemplo importa la API de XenServer, se define como un script personalizado y, a continuación, pasa parámetros específicos del host que quiere controlar de forma remota. Debe definir los parámetros `session` en todos los scripts personalizados.

El resultado aparece cuando el script no es correcto.

```
import XenAPI
def custom(session,remote_host,
power_on_config):
result="Power On Not Successful"
for key in power_on_config.keys():
result=result+''
key=''+key+''
value=''+power_on_config[key]
return result
<!--NeedCopy-->
```

> **Nota:**
>
> Después de crear el script, guárdelo en /etc/xapi.d/plugins con una extensión .py.

Comuníquese con los hosts y grupos de recursos de XenServer

TLS

XenServer usa el protocolo TLS 1.2 para cifrar el tráfico de la API de administración. Cualquier comunicación entre XenServer y los clientes (o dispositivos) de la API de administración utiliza el protocolo TLS 1.2.

> **Importante:**
>
> No admitimos modificaciones por parte de los clientes en la funcionalidad criptográfica del producto.

XenServer usa el siguiente conjunto de cifrado:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Además, los siguientes conjuntos de cifrado también se admiten para la compatibilidad con versiones anteriores de algunas versiones de Citrix Virtual Apps and Desktops:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

SSH

Cuando se utiliza un cliente SSH para conectarse directamente al host de XenServer, se pueden utilizar los siguientes algoritmos:

Cifrados:

- aes128-ctr
- aes256-ctr
- aes128-gcm@openssh.com
- aes256-gcm@openssh.com

MAC:

- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1

KexAlgorithms:

- curve25519-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group14-sha1

HostKeyAlgorithms:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-ed25519
- ssh-rsa

Si quiere inhabilitar el acceso SSH a su host de XenServer, puede hacerlo en. `xsconsole`

1. Desde XenCenter, abra la consola host e inicie sesión como. `root`
2. Escriba `xsconsole`.
3. En `xsconsole`, vaya a **Configuración de servicio remoto** > **Habilitar/inhabilitar Shell remoto**.

   La consola muestra si el shell remoto está habilitado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Para cambiar si el shell remoto está habilitado o inhabilitado, presione **Entrar**.

> **Importante:**
>
> No admitimos modificaciones por parte de los clientes en la funcionalidad criptográfica del producto.

Instale un certificado TLS en su host

El host XenServer viene instalado con un certificado TLS predeterminado. Sin embargo, para usar HTTPS para proteger la comunicación entre XenServer y Citrix Virtual Apps and Desktops, instale un certificado proporcionado por una entidad de certificación de confianza.

En esta sección se describe cómo instalar certificados mediante la CLI de xe. Para obtener información sobre cómo trabajar con certificados mediante XenCenter, consulte la documentación de XenCenter.

Asegúrese de que su certificado TLS y su clave cumplan con los siguientes requisitos:

- El par de certificados y claves son una clave RSA.
- La clave coincide con el certificado.
- La clave se proporciona en un archivo independiente del certificado.
- El certificado se proporciona en un archivo independiente de los certificados intermedios.
- El archivo de claves debe ser de uno de los siguientes tipos: `.pem` o `.key`.
- Los archivos de certificados deben ser de uno de los siguientes tipos: `.pem`, `.cer` o `.crt`.
- La clave es mayor o igual a 2048 bits y menor o igual a 4096 bits de longitud.
- La clave es una clave PKCS #8 sin cifrar y no tiene una clave de paso.
- La clave y el certificado están en formato 'PEM'codificado en base 64.
- El certificado es válido y no ha caducado.
- El algoritmo de firma es SHA-2 (SHA256).

La CLI de xe le avisa cuando el certificado y la clave que elija no cumplen con estos requisitos.

¿Dónde puedo obtener un certificado TLS?

- Es posible que ya tenga un certificado de confianza que quiera instalar en el host de XenServer.
- Como alternativa, puede crear un certificado en su servidor y enviarlo a la entidad de certificación que prefiera para que lo firme. Este método es más seguro, ya que la clave privada puede permanecer en el host de XenServer y no copiarse de un sistema a otro.

  La creación de un certificado TLS tiene los siguientes pasos:

  1. Generar una solicitud de firma de certificado

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Enviar la solicitud de firma del certificado a una autoridad certificadora
3. Instale el certificado firmado en el host de XenServer

1. Generar una solicitud de firma de certificado En primer lugar, genere una solicitud de firma de certificado y clave privada. En el host de XenServer, complete los siguientes pasos:

1. Para crear un archivo de clave privada, ejecute el siguiente comando:

```
openssl genrsa -des3 -out privatekey.pem 2048
<!--NeedCopy-->
```

   Se le pedirá que introduzca una contraseña. Esta frase de contraseña se elimina en un paso siguiente.

2. Elimine la contraseña de la clave:

```
openssl rsa -in privatekey.pem -out privatekey.nop.pem
<!--NeedCopy-->
```

3. Cree la solicitud de firma de certificado mediante la clave privada:

```
openssl req -new -key privatekey.nop.pem -out csr
<!--NeedCopy-->
```

4. Siga las instrucciones para proporcionar la información necesaria para generar la solicitud de firma de certificado.

   - **Nombre del país**. Introduzca los códigos de país del certificado TLS para su país. Por ejemplo, CA para Canadá o JM para Jamaica. Puede encontrar una lista de códigos de países de certificados TLS en la web.
   - Nombre del**estado o provincia (nombre completo)**. Introduzca el estado o la provincia donde se encuentra la agrupación. Por ejemplo, Massachusetts o Alberta.
   - **Nombre de la localidad**. Nombre de la ciudad donde se encuentra la agrupación.
   - **Nombre de la organización**. El nombre de su empresa u organización.
   - **Nombre de la unidad organizativa**. Introduzca el nombre del departamento. Este campo es opcional.
   - **Nombre común**. Introduzca el FQDN del host de XenServer. Recomendamos especificar un FQDN o una dirección IP que no caduque.
   - **Dirección de correo**. Esta dirección de correo electrónico se incluye en el certificado cuando lo genera.

   La solicitud de firma de certificado se guarda en el directorio actual y se denomina `csr`.

5. Para mostrar la solicitud de firma de certificados en la ventana de la consola, ejecute el siguiente comando:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
cat csr
<!--NeedCopy-->
```

6. Copie la solicitud de firma de certificado completa y use esta información para solicitar el certificado a la entidad de certificación.

   Ejemplo de solicitud de firma de certificado:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDBDCCAewCAQAwgYsxCzAJBgNVBAYTAlVLMRcwFQYDVQQIDA5DYW1icmlkZ2Vz
aGlyZTESMBAGA1UEBwwJQ2FtYnJpZGdlMRIwEAYDVQQKDAlYZW5TZXJ2ZXIxFTAT
...
SdYCkFdo+85z8hBULFzSH6jgSP0UGQU0PcfIy7KPKyI4jnFQqeCDvLdWyhtAx9gq
Fu40qMSm1dNCFfnACRwYQkQgqCt/RHeUtl8srxyZC+odbunnV+ZyQdmLwLuQySUk
ZL8naumG3yU=
-----END CERTIFICATE REQUEST-----
<!--NeedCopy-->
```

2. Enviar la solicitud de firma del certificado a una autoridad certificadora Ahora que ha generado la solicitud de firma del certificado, puede enviarla a la entidad de certificación preferida de su organización.

Una entidad de certificación es un tercero de confianza que proporciona certificados digitales. Algunas autoridades de certificación exigen que los certificados estén alojados en un sistema al que se pueda acceder desde Internet. Recomendamos no utilizar una entidad de certificación con este requisito.

La entidad de certificación responde a su solicitud de firma y proporciona los siguientes archivos:

- el certificado firmado
- un certificado raíz
- si procede, un certificado intermedio

Ahora puede instalar todos estos archivos en el host de XenServer.

3. Instale el certificado firmado en el host de XenServer Una vez que la entidad de certificación haya respondido a la solicitud de firma del certificado, complete los siguientes pasos para instalar el certificado en el host de XenServer:

1. Obtenga el certificado firmado, el certificado raíz y, si la entidad de certificación tiene uno, el certificado intermedio de la entidad de certificación.
2. Copie la clave y los certificados en el host de XenServer.
3. Ejecute el siguiente comando en el host:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe host-server-certificate-install certificate=<
    path_to_certificate_file> private-key=<path_to_private_key>
    certificate-chain=<path_to_chain_file>
```

El parámetro `certificate-chain` es opcional.

Para mayor seguridad, puede eliminar el archivo de clave privada después de instalar el certificado.

Administrar la contraseña de administrador

Cuando instala por primera vez un host de XenServer, establece una contraseña de administrador o *root*. Use esta contraseña para conectar XenCenter a su host o (con el `root`nombre de usuario) para iniciar sesión **en**xsconsole, la consola de configuración del sistema.

Si une un anfitrión a un grupo, la contraseña de administrador del host se cambia automáticamente para que coincida con la contraseña de administrador del coordinador del grupo.

> **Nota:**
>
> Las contraseñas de administrador de XenServer solo deben contener caracteres ASCII.

Cambiar la contraseña

Puede usar XenCenter, la CLI de xe o **xsconsole** para cambiar la contraseña del administrador.

XenCenter Para cambiar la contraseña de administrador de un grupo o un host independiente mediante XenCenter, complete los siguientes pasos:

1. En el panel **Recursos**, seleccione el grupo o cualquier host del grupo.
2. En el menú **Agrupación** o en el menú **Servidor**, seleccione **Cambiar contraseña del servidor**.

Para cambiar la contraseña raíz de un host independiente, seleccione el host en el panel **Recursos**, haga clic en **Contraseña** y, a continuación, en **Cambiar** en el menú **Servidor**.

Si XenCenter está configurado para guardar las credenciales de inicio de sesión del host entre sesiones, se recuerda la nueva contraseña. Para obtener más información, consulte Almacenar el estado de la conexión del host.

Después de cambiar la contraseña de administrador, rote el secreto del grupo. Para obtener más información, consulte Rotar el secreto de la agrupación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

CLI de xe Para cambiar la contraseña de administrador mediante la CLI xe, ejecute el siguiente comando en un host del grupo:

```
  xe user-password-change new=<new_password>
<!--NeedCopy-->
```

> **Nota:**
>
> Asegúrese de anteponer un espacio al comando para evitar almacenar la contraseña de texto sin formato en el historial de comandos.

Después de cambiar la contraseña de administrador, rote el secreto del grupo. Para obtener más información, consulte Rotar el secreto de la agrupación.

xsconsole Para cambiar la contraseña de administrador de un grupo o un host independiente mediante **xsconsole**, complete los siguientes pasos:

1. En el coordinador de la agrupación, vaya a la consola.
2. Inicie sesión como `root`.
3. Escriba `xsconsole`. Presiona **Entrar**. Se muestra **xsconsole**.
4. En **xsconsole**, utilice las flechas para ir a la opción **Autenticación**. Presiona **Entrar**.
5. Vaya a **Cambiar contraseña**. Presione **Intro**.
6. Autentíquese con la contraseña de administrador.
7. En el cuadro de diálogo **Cambiar contraseña**:

   a) Introduzca su contraseña actual.
   b) Introduzca una contraseña nueva.
   c) Escriba de nuevo la nueva contraseña para confirmarla.

   Aparecerá la pantalla **Cambio de contraseña correcto**. Presione **Entrar** para cerrarla.

Si el anfitrión es el coordinador del grupo, esta contraseña actualizada ahora se propaga a los demás hosts del grupo.

Después de cambiar la contraseña de administrador, rote el secreto del grupo. Para obtener más información, consulte Rotar el secreto de la agrupación.

Restablecer una contraseña root perdida

Si pierde la contraseña de administrador (root) del host de XenServer, puede restablecerla accediendo directamente al host.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Reinicie el host de XenServer.
2. Cuando aparezca el menú de GRUB, presione **e** para modificar la entrada del menú de arranque.
3. Agregue `init=/sysroot/bin/sh` a la línea que comienza con `module2`.
4. Presione **Ctrl-X** para un arranque en un shell raíz.
5. En el shell de comandos, ejecute los siguientes comandos:

```
chroot /sysroot
passwd

(type the new password twice)

sync
/sbin/reboot -f
<!--NeedCopy-->
```

Si el anfitrión es el coordinador del grupo, esta contraseña actualizada ahora se propaga a los demás hosts del grupo.

Después de cambiar la contraseña de administrador, rote el secreto del grupo.

Gira el secreto de la agrupación

El secreto de la agrupación es un secreto compartido entre los anfitriones de una agrupación que permite al anfitrión demostrar su pertenencia a una agrupación.

Dado que los usuarios con la función de administrador del grupo pueden descubrir este secreto, se recomienda cambiar el secreto del grupo si uno de estos usuarios abandona la organización o pierde su función de administrador de grupo.

Puede rotar el secreto del grupo mediante XenCenter o la CLI de xe.

XenCenter

Para rotar el secreto del grupo de un grupo mediante XenCenter, siga estos pasos:

1. En el panel **Recursos**, seleccione el grupo o cualquier host del grupo.
2. En el menú **Agrupación**, seleccione **Rotar secreto de agrupación**.

Al rotar el secreto del grupo, también se le pide que cambie la contraseña de root. Si ha rotado el secreto del grupo porque cree que su entorno se ha visto comprometido, asegúrese de cambiar también la contraseña de root. Para obtener más información, consulte Cambiar la contraseña.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

CLI de xe

Para rotar el secreto del grupo mediante la CLI xe, ejecute el siguiente comando en un host del grupo:

```
xe pool-secret-rotate
<!--NeedCopy-->
```

Si ha rotado el secreto del grupo porque cree que su entorno se ha visto comprometido, asegúrese de cambiar también la contraseña de root. Para obtener más información, consulte Cambiar la contraseña.

Habilite el espionaje IGMP en su grupo de XenServer

XenServer envía tráfico de multidifusión a todas las máquinas virtuales invitadas, lo que genera una carga innecesaria en los dispositivos host al obligarlos a procesar paquetes que no han solicitado. La habilitación de la indagación IGMP evita que los hosts de una red local reciban tráfico para un grupo de multidifusión al que no se hayan unido explícitamente y mejora el rendimiento de la multidifusión. La indagación IGMP es especialmente útil para aplicaciones de multidifusión IP con uso intensivo de ancho de banda, como IPTV.

> **Notas:**
>
> - La indagación IGMP solo está disponible cuando el back-end de la red usa Open vSwitch.
> - Al habilitar esta función en un grupo, también puede ser necesario habilitar la consulta IGMP en uno de los conmutadores físicos. De lo contrario, la multidifusión en la subred recurre a la transmisión y puede reducir el rendimiento de XenServer.
> - Al habilitar esta función en un grupo que ejecuta IGMP v3, la migración de VM o la conmutación por error de enlace de red da como resultado que la versión IGMP cambie a v2.
> - Para habilitar esta función con una red GRE, los usuarios deben configurar un solicitante IGMP en la red GRE. Como alternativa, puede reenviar el mensaje de consulta IGMP desde la red física a la red GRE. O bien, se puede bloquear el tráfico de multidifusión en la red GRE.

Puede habilitar la detección de IGMP en un grupo mediante XenCenter o la CLI xe.

XenCenter

1. Navegue hasta **Propiedades del grupo**.
2. Seleccione **Opciones de red**. Aquí puede habilitar o inhabilitar la detección de IGMP.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

CLI de xe

1. Obtenga el UUID del grupo:

   ```
   xe pool-list
   ```

2. Habilitar/inhabilitar la detección de IGMP para la agrupación:

   ```
   xe pool-param-set [uuid=pool-uuid] [igmp-snooping-enabled=true|
   false]
   ```

Después de habilitar la detección de IGMP, puede ver la tabla de detección de IGMP mediante la CLI xe.

Ver la tabla de espionaje de IGMP

Utilice el siguiente comando para ver la tabla de detección de IGMP:

```
ovs-appctl mdb/show [bridge name]
```

> **Nota:**
>
> Puede obtener el nombre del puente usando `xe network-list`. Los nombres de estos puentes pueden ser `xenbr0`, `xenbr1`, `xenapi` o `xapi0`.

Esto genera una tabla con cuatro columnas:

- puerto: El puerto del conmutador (OVS).
- VLAN: El ID de VLAN del tráfico.
- GRUPO: El grupo de multidifusión que solicitó el puerto.
- Edad: la antigüedad de este registro en segundos.

Si el **GRUPO** es una dirección de grupo de multidifusión, significa que se recibió un mensaje de informe IGMP en el puerto del conmutador asociado. Esto significa que un receptor (miembro) del grupo de multidifusión está escuchando en este puerto.

Tomemos el ejemplo siguiente, que contiene dos registros:

port	VLAN	GRUPO	Edad
14	0	227.0.0.1	15
1	0	querier	24

El primer registro muestra que hay un receptor que escucha en el puerto 14 para el grupo de multidifusión 227.0.0.1. El Open vSwitch reenvía el tráfico destinado al grupo de multidifusión 227.0.0.1 a

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

los puertos de escucha únicamente para este grupo (en este ejemplo, el puerto 14), en lugar de transmitirlo a todos los puertos. El registro que vincula el puerto 14 y el grupo 227.0.0.1 se creó hace 15 segundos. De forma predeterminada, el intervalo de tiempo de espera es de 300 segundos. Esto significa que si el conmutador no recibe ningún otro mensaje de informe IGMP en el puerto 14 durante 300 segundos después de agregar el registro, el registro caducará y se eliminará de la tabla.

En el segundo registro, el **GROUP realizaconsultas**, lo que significa que los mensajes de consulta IGMP se han recibido en el puerto asociado. Un consultador envía periódicamente mensajes de consulta IGMP, que se transmiten a todos los puertos del conmutador, para determinar qué nodos de red están escuchando en un grupo de multidifusión. Al recibir un mensaje de consulta de IGMP, el receptor responde con un mensaje de informe de IGMP, que hace que el registro de multidifusión del receptor se actualice y evite su caducidad.

La columna **VLAN** indica a la VLAN que vive un receptor/consultador. '0'significa VLAN nativa. Si quiere ejecutar la multidifusión en alguna VLAN etiquetada, asegúrese de que haya registros en la VLAN.

> **Nota:**
>
> Para el caso de VLAN, debe tener un registro de consulta con un valor de columna de VLAN igual al ID de VLAN de la red; de lo contrario, la multidifusión no funcionará en la red VLAN.

Habilite la compresión del flujo de migración en su grupo de XenServer

Durante la migración en vivo de una máquina virtual, su memoria se transfiere como un flujo de datos entre dos hosts que utilizan la red. La función de compresión del flujo de migración comprime este flujo de datos, lo que acelera la transferencia de memoria en redes lentas. Esta función está inhabilitada de forma predeterminada, pero se puede cambiar mediante XenCenter o la CLI xe. Para obtener más información, consulte Propiedades de la agrupación: Opciones avanzadas y Parámetros de la agrupación. Como alternativa, puede habilitar la compresión al migrar una máquina virtual mediante la línea de comandos. Para obtener más información, consulte el comando `vm-migrate` en Comandos de máquina virtual.

Verificación de certificados

August 24, 2023

Cuando se habilita la verificación de certificados para un grupo, todos los puntos finales de comunicación TLS de su red de administración utilizan certificados para validar la identidad de sus pares antes de transmitir información confidencial.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Comportamiento

Las conexiones iniciadas por un host de XenServer en la red de administración requieren que el punto final de destino proporcione un certificado TLS para verificar su identidad. Este requisito afecta a los siguientes elementos que forman parte del grupo o interactúan con él:

- Anfitriones en la piscina
- XenCenter
- Clientes de terceros que utilizan la API

La verificación de certificados es compatible tanto con los certificados autofirmados proporcionados por XenServer como con los certificados instalados por el usuario y firmados por una autoridad de confianza. Para obtener más información, consulte Instalar un certificado TLS en el host.

Cada host XenServer de un grupo tiene dos certificados que lo identifican:

- *Los certificados de identidad internos del grupo* se utilizan para proteger las comunicaciones entre los hosts del grupo. Para la comunicación dentro del grupo, XenServer siempre usa certificados autofirmados.
- Los*certificados de identidad del servidor* se utilizan para verificar la identidad de un host de XenServer ante cualquier aplicación cliente que se comunique con el grupo de la red de administración. Para la comunicación entre el host y una aplicación cliente, puede usar certificados autofirmados o puede instalar sus propios certificados TLS en sus hosts.

Cuando un host se une al grupo por primera vez o un cliente establece una conexión al grupo por primera vez, el grupo confía en la conexión. Durante esta primera conexión, los certificados se intercambian entre el grupo y el host que se une o el cliente que se conecta. Para todas las comunicaciones posteriores de este host o cliente en la red de administración, los certificados se utilizan para verificar la identidad de las partes involucradas en la comunicación.

Le recomendamos que habilite la verificación de certificados en todos sus hosts y grupos. Para que un host XenServer se una correctamente a un grupo, tanto el host como el grupo deben tener habilitada o deshabilitada la verificación de certificados. Si la verificación de certificados está habilitada en uno y no en el otro, la operación de unión no se realiza correctamente. XenCenter proporciona un mensaje de advertencia en el que se le indica que habilite la verificación de certificados en el grupo o en el host que se une.

Cuando un host abandona un grupo con la verificación de certificados habilitada, tanto el host como el grupo eliminan los certificados relacionados con el otro.

El dispositivo virtual Workload Balancing se puede utilizar con la verificación de certificados. Debe asegurarse de que los certificados autofirmados de Workload Balancing estén instalados en el host de XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El dispositivo virtual XenServer Conversion Manager no se conecta a los hosts de XenServer y, por lo tanto, está exento del requisito de verificación de certificación cuando actúa como punto final de un cliente TLS.

Habilitar la verificación de certificados para su grupo

La verificación de certificados está habilitada de forma predeterminada en las instalaciones nuevas de XenServer 8 y versiones posteriores. Si actualiza desde una versión anterior de XenServer o Citrix Hypervisor, la verificación de certificados no se habilita automáticamente y debe habilitarla. XenCenter le pedirá que habilite la verificación de certificados la próxima vez que se conecte al grupo actualizado.

Antes de habilitar la verificación de certificados en un grupo, asegúrese de que no se estén ejecutando operaciones en el grupo.

Habilitar mediante XenCenter

XenCenter ofrece varias formas de habilitar la verificación de certificados.

- La primera vez que conecte XenCenter a un grupo sin la verificación de certificados habilitada, se le pedirá que la habilite. Haga clic en **Sí, habilitar la verificación de certificados**.
- En el menú **Agrupación**, seleccione **Habilitar verificación de certificados**.
- En la ficha **General** del grupo, haga clic con el botón derecho en la entrada **Verificación de certificados** y seleccione **Habilitar verificación de certificados** en el menú.

Habilitar mediante la CLI xe

Para habilitar la verificación de certificados para un grupo, ejecute el siguiente comando en la consola de un host del grupo:

```
1 xe pool-enable-tls-verification
```

Administración de certificados

Puede instalar, ver información y restablecer los certificados que se utilizan para verificar la identidad de un host.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Instalación de certificados

Puede instalar su propio certificado TLS para que el host lo presente como certificado de identidad cuando reciba conexiones de aplicaciones cliente en la red de administración.

Para obtener más información, consulte Instalar un certificado TLS en el host.

Ver la información del certificado

Para saber si un grupo tiene habilitada la verificación de certificados:

- En XenCenter, busque el grupo en **la** pestaña General. La sección **General** tiene una entrada para **Verificación de certificados** que muestra si la verificación de certificados está habilitada o inhabilitada. Esta ficha también contiene una sección **Certificados** que enumera el nombre, la validez y la huella digital de los certificados de CA.
- Con la CLI xe, puede ejecutar el siguiente comando:

```
xe pool-param-get uuid=<pool_uuid> param-name=tls-verification-
    enabled
```

  Si la verificación de certificados está habilitada, la línea `tls-verification-enabled ( RO): true` aparece en el resultado del comando.

Para ver información sobre los certificados en un host de XenServer:

- En XenCenter, vaya a **la pestaña General de ese** host. La sección **Certificados** muestra la huella digital y las fechas de validez del certificado de identidad del servidor y el certificado de identidad interno del grupo.
- Con la CLI xe, puede ejecutar el siguiente comando:

```
xe certificate-list
```

Actualización de certificados de identidad internos del grupo

Puede actualizar el certificado de identidad interno del grupo mediante la CLI xe:

1. Busque el UUID del host cuyo certificado desea restablecer ejecutando el siguiente comando:

```
xs host-list
```

2. Para restablecer el certificado, ejecute el siguiente comando:

```
xe host-refresh-server-certificate host=<host_uuid>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Se puede usar cualquier parámetro del selector de host con este comando para indicar el host en el que se debe restablecer el certificado.

Restablecer los certificados de identidad del servidor

Puede restablecer el certificado de identidad del servidor desde XenCenter o la CLI xe. Al restablecer un certificado, se elimina el certificado del host y se instala un nuevo certificado autofirmado en su lugar.

Para restablecer un certificado en XenCenter:

1. Ve a la pestaña **General** del anfitrión.
2. En la sección **Certificados**, haga clic con el botón derecho en el certificado que desea restablecer.
3. En el menú, selecciona **Restablecer certificado**.
4. En el cuadro de diálogo que aparece, haga clic en **Sí** para confirmar el restablecimiento del certificado.

Como alternativa, en el menú **Servidor**, puede ir a **Certificados > Restablecer certificado**.

Al restablecer un certificado, se desconectan todas las conexiones existentes al host de XenServer, incluida la conexión entre XenCenter y el host. XenCenter se vuelve a conectar automáticamente al host tras restablecer el certificado.

Para restablecer un certificado mediante la CLI xe:

1. Busque el UUID del host cuyo certificado desea restablecer ejecutando el siguiente comando:

```
xs host-list
```

2. Para restablecer el certificado, ejecute el siguiente comando:

```
xe host-reset-server-certificate host=<host_uuid>
```

> **Nota:**
>
> Se puede usar cualquier parámetro del selector de host con este comando para indicar el host de XenServer en el que se debe restablecer el certificado.

Al restablecer un certificado, se desconectan todas las conexiones existentes al host de XenServer, incluida la conexión entre XenCenter y el host. XenCenter se vuelve a conectar automáticamente al host tras restablecer el certificado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Alertas de caducidad

XenCenter muestra alertas en **la vista de notificaciones cuando los** certificados de identidad del servidor, los certificados de identidad internos del grupo o los certificados de CA del grupo están cerca de su fecha de caducidad.

Desactivación temporal de la verificación de certificados

No se recomienda deshabilitar la verificación de certificados después de haberla habilitado en un host o grupo. Sin embargo, XenServer proporciona comandos que se pueden usar para deshabilitar la verificación de certificados por host al solucionar problemas con los certificados.

Para deshabilitar temporalmente la verificación de certificados, ejecute el siguiente comando en la consola host:

```
1 xe host-emergency-disable-tls-verification
```

XenCenter muestra una alerta en **la vista de notificaciones cuando la** verificación del certificado está deshabilitada en un host de un grupo en el que la función está habilitada.

Una vez que haya resuelto cualquier problema con los certificados del host, asegúrese de volver a habilitar la verificación de certificados en él. Para volver a habilitar la verificación de certificados, ejecute el siguiente comando en la consola host:

```
1 xe host-emergency-reenable-tls-verification
```

---

layout: doc
description: Create, manage, or destroy a clustered pool of XenServer hosts. Understand the constraints and requirements associated with setting up a clustered pool.—

Agrupaciones en clúster

La agrupación en clústeres proporciona funciones adicionales necesarias para los grupos de recursos que utilizan SRs de GFS2. Para obtener más información sobre GFS2, consulte Configurar el almacenamiento.

Un clúster es un grupo de hasta 16 hosts de XenServer que están más estrechamente conectados y coordinados que los hosts de grupos no agrupados en clústeres. Los hosts del clúster mantienen una comunicación constante entre sí en una red seleccionada. Todos los hosts del clúster conocen el estado de todos los hosts del clúster. Esta coordinación de host permite que el clúster controle el acceso al contenido de GFS2 SR.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> La función de agrupamiento en clústeres solo beneficia a los grupos que contienen un SR de GFS2. Si su grupo no contiene un SR de GFS2, no habilite la agrupación en clústeres en su grupo.

Quórum

Cada host de un clúster debe estar siempre en comunicación con la mayoría de los hosts del clúster (incluido él mismo). Este estado se conoce como anfitrión que tiene quórum. Si un host no tiene quórum, ese host se autocerca.

La cantidad de hosts que deben estar en comunicación para alcanzar inicialmente el quórum puede ser diferente de la cantidad de hosts que un clúster necesita para mantener el quórum.

En la tabla siguiente se resume este comportamiento. El valor de n es la cantidad total de hosts del grupo agrupado.

	Número de hosts necesarios para lograr el quórum	Número de hosts necesarios para mantener el quórum
Número impar de anfitriones en la piscina	(n+1) /2	(n+1) /2
Número par de anfitriones en la piscina	(n/2) +1	n/2

Grupos de números impares

Para alcanzar el valor de quórum para un grupo de números impares, necesitará la mitad de uno más que el número total de hosts del clúster: (n+1) /2. Este es también el número mínimo de hosts a los que se debe poder contactar para que el grupo mantenga el quórum.

Por ejemplo, en un grupo agrupado en clústeres de 5 hosts, se debe poder contactar con 3 hosts para que el clúster se active y permanezca en quórum [(5+1) /2 = 3].

Siempre que sea posible, se recomienda utilizar un número impar de hosts en un grupo agrupado, ya que esto garantiza que los hosts siempre puedan determinar si tienen un conjunto de quóratos.

Grupos pares

Cuando un grupo agrupado en clúster con número par se enciende desde un inicio en frío, (n/2) +1 hosts deben estar disponibles antes de que los hosts tengan quórum. Una vez que los hosts tienen quórum, el clúster se activa.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sin embargo, un grupo de números pares activo puede permanecer en quórum si el número de hosts con los que se puede contactar es al menos n/2. Como resultado, es posible que un clúster en ejecución con un número par de hosts se divida exactamente por la mitad. El clúster en ejecución decide qué mitad del clúster se autocierra y qué mitad del clúster tiene quórum. La mitad del clúster que contiene el nodo con el ID más bajo que se consideraba activo antes de la división del clúster permanece activa y la otra mitad del clúster se autocierra.

Por ejemplo, en un grupo agrupado en clústeres de 4 hosts, se debe poder contactar con 3 hosts para que el clúster se active [4/2 + 1 = 3]. Una vez que el clúster esté activo, para mantener el quórum, solo se debe poder contactar con 2 hosts [4/2 = 2] y ese conjunto de hosts debe incluir el host con el ID de nodo más bajo que se sepa que está activo.

Autocercas

Si un host detecta que no tiene quórum, se autocierra en unos segundos. Cuando un host se autocerca, se reinicia inmediatamente. Todas las máquinas virtuales que se ejecutan en el host se detienen inmediatamente porque el host se apaga por completo. En un grupo agrupado que usa alta disponibilidad, XenServer reinicia las máquinas virtuales según su configuración de reinicio en otros miembros del grupo. El host que se autodelimitó se reinicia e intenta volver a unirse al clúster.

Si la cantidad de hosts activos en el clúster es inferior al valor de quórum, todos los hosts restantes pierden el quórum.

En un escenario ideal, su grupo agrupado en clústeres siempre tiene más hosts activos de los necesarios para el quórum y XenServer nunca lo impide. Para que este caso sea más probable, tenga en cuenta las siguientes recomendaciones al configurar su grupo agrupado en clústeres:

- Asegúrese de tener una buena redundancia de hardware.
- Use una red enlazada dedicada para la red de clústeres. Asegúrese de que las NIC enlazadas estén en el mismo segmento L2. Para obtener más información, consulte Redes.
- Configure las rutas múltiples de almacenamiento entre el grupo y GFS2 SR. Para obtener más información, consulte Múltiples rutas de almacenamiento.

Crea un grupo agrupado

Antes de empezar, asegúrese de que se cumplen los siguientes requisitos previos:

- Todos los hosts XenServer del grupo agrupado deben tener al menos 2 GiB de memoria en el dominio de control.

  Según el entorno, es posible que los hosts requieran más memoria de dominio de control que esta. Si no tiene suficiente memoria de dominio de control en sus hosts, su agrupación puede

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

experimentar inestabilidad en la red. La inestabilidad de la red puede causar problemas a una agrupación en clústeres con la SR de GFS2. Para obtener información sobre cómo cambiar la cantidad de memoria del dominio de control y supervisar el comportamiento de la memoria, consulte Uso de memoria.

- Todos los hosts del clúster deben usar direcciones IP estáticas para la red del clúster.
- Le recomendamos que utilice la agrupación en clústeres solo en grupos que contengan al menos tres hosts, ya que los grupos de dos hosts son sensibles a la posibilidad de que se autoproteja todo el grupo.
- Los grupos agrupados solo admiten hasta 16 hosts por grupo.
- Si tiene un firewall entre los hosts de su grupo, asegúrese de que los hosts puedan comunicarse en la red del clúster mediante los siguientes puertos:
  - TCP: 8892, 8896, 21064
  - UDP: 5404, 5405

  Para obtener más información, consulte Puertos de comunicación utilizados por XenServer.
- Si está agrupando un grupo existente, asegúrese de que la alta disponibilidad esté inhabilitada. Puede volver a habilitar la alta disponibilidad después de habilitar la agrupación en clústeres.
- Le recomendamos encarecidamente que utilice una red enlazada para su grupo agrupado que no se utilice para ningún otro tráfico.

Si lo prefiere, puede configurar la agrupación en clústeres en su grupo mediante XenCenter. Para obtener más información, consulte la documentación del producto XenCenter.

Para usar la CLI xe para crear un grupo en clúster:

1. Cree una red enlazada para usarla como red de agrupación en clústeres.

   > **Nota:**
   >
   > Le recomendamos encarecidamente que utilice una red enlazada dedicada para su grupo agrupado en clústeres. No utilice esta red para ningún otro tipo de tráfico.

   En el host de XenServer en el que quiere que coordine el grupo, complete los siguientes pasos:

   a) Abra una consola en el host de XenServer.

   b) Cree una red para usarla con la NIC enlazada mediante el siguiente comando:

   ```
   xe network-create name-label=bond0
   <!--NeedCopy-->
   ```

   Se devuelve el UUID de la nueva red.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

c) Encuentre los UUID de los PIF que se van a usar en el enlace mediante el siguiente comando:

```
xe pif-list
<!--NeedCopy-->
```

d) Cree su red enlazada en modo activo-activo, modo activo-pasivo o modo enlace LACP. Según el modo de enlace que quiera usar, realice una de las siguientes acciones:

- Para configurar el enlace en modo activo-activo (predeterminado), utilice el comando `bond-create` para crear el enlace. Con comas para separar los parámetros, especifique el UUID de red recién creado y los UUID de los PIF que se van a unir:

```
xe bond-create network-uuid=<network_uuid> /
     pif-uuids=<pif_uuid_1>,<pif_uuid_2>,<pif_uuid_3>,<
        pif_uuid_4>
<!--NeedCopy-->
```

  Escriba dos UUID cuando vincule dos NIC y cuatro UUID cuando vincule cuatro NIC. El UUID del enlace se devuelve después de ejecutar el comando.

- Para configurar el enlace en modo activo-pasivo o enlace LACP, utilice la misma sintaxis, agregue el parámetro `mode` opcional y especifique `lacp` o `active-backup`:

```
xe bond-create network-uuid=<network_uuid> pif-uuids=<
   pif_uuid_1>, /
     <pif_uuid_2>,<pif_uuid_3>,<pif_uuid_4> /
     mode=balance-slb | active-backup | lacp
<!--NeedCopy-->
```

Una vez creada la red enlazada en el coordinador del grupo, al unir otros hosts de XenServer al grupo, la información de red y enlace se replica automáticamente en el servidor que se une.

Para obtener más información, consulte Redes.

2. Cree un grupo de recursos de al menos tres hosts de XenServer.

   Repita los siguientes pasos en cada host de XenServer que sea miembro del grupo (no principal):

   a) Abra una consola en el host de XenServer.

   b) Une el host de XenServer al grupo en el coordinador del grupo mediante el siguiente comando:

```
xe pool-join master-address=master_address master-username=
   administrators_username master-password=password
<!--NeedCopy-->
```

   El valor del `master-address` parámetro debe establecerse en el nombre de dominio completo del host de XenServer que es el coordinador del grupo. `password` Debe ser

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

la contraseña de administrador establecida cuando se instaló el coordinador de la agrupación.

Para obtener más información, consulte Hosts y grupos de recursos.

3. Para cada PIF que pertenezca a esta red, defina `disallow-unplug=true`.

   a) Busque los UUID de los PIF que pertenecen a la red mediante el siguiente comando:

   ```
   xe pif-list
   <!--NeedCopy-->
   ```

   b) Ejecute el siguiente comando en un host de XenServer de su grupo de recursos:

   ```
   xe pif-param-set disallow-unplug=true uuid=<pif_uuid>
   <!--NeedCopy-->
   ```

4. Habilite la agrupación en clústeres en su grupo. Ejecute el siguiente comando en un host de XenServer de su grupo de recursos:

   ```
   xe cluster-pool-create network-uuid=<network_uuid>
   <!--NeedCopy-->
   ```

   Proporcione el UUID de la red enlazada que creó en un paso anterior.

Destruye una agrupación agrupada

Puede destruir una agrupación agrupada. Después de destruir un grupo agrupado, el grupo sigue existiendo, pero ya no está agrupado en clústeres y ya no puede usar SR de GFS2.

Para destruir un grupo agrupado, ejecute el siguiente comando:

```
xe cluster-pool-destroy cluster-uuid=<uuid>
```

Administre su grupo agrupado

Al administrar su grupo en clúster, las siguientes prácticas pueden disminuir el riesgo de que el grupo pierda quórum.

Agregar o quitar un host en una agrupación en clúster

Al agregar un host a una agrupación en clúster o quitarlo de ella, asegúrese de que todos los hosts del clúster estén en línea.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puede agregar un host a una agrupación en clúster o quitarlo de ella mediante XenCenter. Para obtener más información, consulte Agregar un servidor a una agrupación y Quitar un servidor de una agrupación.

También puede agregar un host a una agrupación en clúster o quitarlo de ella mediante la CLI xe. Para obtener más información, consulte Agregar un host a un grupo mediante la CLI xe y Quitar los hosts de XenServer de un grupo de recursos.

Asegúrese de que los hosts se cierren de forma limpia

Cuando un host se cierra de forma limpia, se elimina temporalmente del clúster hasta que se inicia de nuevo. Mientras el host está cerrado, no cuenta para el valor de quórum del clúster. La ausencia del anfitrión no provoca que otros anfitriones pierdan quórum.

Sin embargo, si un host se cierra de forma forzada o inesperada, no se elimina del clúster antes de que se desconecte. Este host cuenta para el valor de quórum del clúster. Su cierre puede provocar que otros hosts pierdan quórum.

Si es necesario cerrar un host por la fuerza, compruebe primero cuántos hosts activos hay en el clúster. Puede hacerlo con el comando `corosync-quorumtool`. En el resultado del comando, la cantidad de hosts en vivo es el valor de `Total votes:` y la cantidad de hosts en vivo necesarios para retener el quórum es el valor de `Quorum:`.

- Si la cantidad de hosts activos es la misma que la cantidad de hosts necesarios para mantener el quórum, no apague el host por la fuerza. Si lo hace, todo el grupo se cercará.

  En su lugar, intente recuperar otros hosts y aumentar el número de hosts activos antes de cerrar el host por la fuerza.

- Si la cantidad de anfitriones activos se acerca a la cantidad de hosts necesarios para mantener el quórum, puede cerrar el host por la fuerza. Sin embargo, esto hace que el clúster sea más vulnerable a la protección total si otros hosts del grupo tienen problemas.

Intente siempre reiniciar el host apagado lo antes posible para aumentar la resiliencia del clúster.

Usar el modo de mantenimiento

Antes de hacer algo en un host que pueda provocar que ese host pierda quórum, ponga el host en modo de mantenimiento. Cuando un host está en modo de mantenimiento, las máquinas virtuales en ejecución se migran desde él a otro host del grupo. Además, si ese host era el coordinador del grupo, esa función se pasa a otro host del grupo. Si sus acciones hacen que un host en modo de mantenimiento se autobloquee, no pierde ninguna VM ni pierde la conexión de XenCenter al grupo.

Los hosts en modo de mantenimiento siguen contando para el valor de quórum del clúster.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Solo puede cambiar la dirección IP de un host que forma parte de un grupo en clúster cuando ese host está en modo de mantenimiento. Cambiar la dirección IP de un host provoca que el host abandone el clúster. Cuando la dirección IP se ha cambiado correctamente, el host se vuelve a unir al clúster. Cuando el host se vuelva a unir al clúster, puede sacarlo del modo de mantenimiento.

Recuperar hosts que se han cerrado automáticamente o están fuera de línea

Es importante recuperar los hosts que tienen autoprotección. Mientras estos miembros del clúster están desconectados, cuentan para el número de quórum del clúster y disminuyen el número de miembros del clúster con los que se puede contactar. Esta situación aumenta el riesgo de que una falla posterior del host provoque que el clúster pierda el quórum y se cierre por completo.

Tener hosts sin conexión en su clúster también le impide realizar ciertas acciones. En un grupo agrupado, todos los miembros del grupo deben aceptar cada cambio de membresía del grupo antes de que el cambio pueda tener éxito. Si no se puede contactar con un miembro del clúster, XenServer impide las operaciones que cambien la pertenencia al clúster (como agregar o quitar un host).

Marcar los hosts como irrecuperables

Si no se pueden recuperar uno o más hosts sin conexión, puede decirle al grupo agrupado en clústeres que los olvide. Estos anfitriones se eliminan permanentemente del grupo. Una vez que los hosts se eliminan del grupo agrupado en clústeres, ya no cuentan para el valor del quórum.

Para marcar un host como irrecuperable, utilice el siguiente comando:

```
1 xe host-forget uuid=<host_uuid>
```

Recuperar un host olvidado

Cuando se le dice a un grupo agrupado que olvide un anfitrión, este no podrá volver a añadirse al grupo.

Para volver a unirse al grupo agrupado, debe volver a instalar XenServer en el host para que aparezca como un host nuevo en el grupo. A continuación, puede unir al anfitrión al grupo agrupado de la forma habitual.

Solucione los problemas de su grupo agrupado

Si tiene problemas con su grupo agrupado, consulte Solucionar problemas de grupos agrupados.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Limitaciones

- Los grupos agrupados solo admiten hasta 16 hosts por grupo.
- Para habilitar la alta disponibilidad en su agrupación en clústeres, la SR de latido debe ser una SR de GFS2.
- Para el tráfico de clústeres, le recomendamos encarecidamente que utilice una red enlazada que utilice al menos dos conmutadores de red diferentes. No utilice esta red para ningún otro propósito.
- Para cambiar la dirección IP de la red de clústeres mediante XenCenter, es necesario inhabilitar temporalmente la agrupación en clústeres y GFS2.
- No cambie la vinculación de la red de clústeres mientras el clúster está activo y tiene máquinas virtuales en ejecución. Esta acción puede provocar que los hosts del clúster se reinicien por completo (valla).
- Si tiene un conflicto de direcciones IP (varios hosts que tienen la misma dirección IP) en su red de clústeres que implica al menos un host con la agrupación en clústeres habilitada, el clúster no se forma correctamente y los hosts no pueden cercarlo cuando es necesario. Para solucionar este problema, resuelva el conflicto de direcciones IP.

Solucionar problemas de grupos agrupados

January 17, 2024

Los grupos de XenServer que utilizan GFS2 para aprovisionar de forma reducida su almacenamiento en bloque compartido se agrupan en clústeres. Estos grupos se comportan de forma diferente a los grupos que utilizan almacenamiento compartido basado en archivos o LVM con almacenamiento en bloques compartido. Como resultado, se pueden producir algunos problemas específicos en los grupos agrupados en clústeres de XenServer y en los entornos de GFS2.

Utilice la siguiente información para solucionar problemas menores que pueden producirse al utilizar esta función.

Todos mis hosts pueden hacer ping entre sí, pero no puedo crear un clúster. ¿Por qué?

El mecanismo de agrupamiento utiliza puertos específicos. Si sus hosts no pueden comunicarse en estos puertos (incluso si pueden comunicarse en otros puertos), no puede habilitar la agrupación en clústeres para el grupo.

Asegúrese de que los hosts del grupo puedan comunicarse en los siguientes puertos:

- TCP: 8892, 8896, 21064

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- UDP: 5404, 5405 (no multidifusión)

Si hay firewalls o similares entre los hosts del grupo, asegúrese de que estos puertos estén abiertos.

Si ya configuró HA en el grupo, deshabilite la HA antes de habilitar la agrupación en clústeres.

¿Por qué aparece un error cuando intento unir un nuevo host a un grupo agrupado en clústeres existente?

Cuando se habilita la agrupación en clústeres en un grupo, todos los miembros del clúster deben acordar cada cambio en la membresía del grupo antes de que pueda realizarse correctamente. Si no se puede contactar con un miembro del clúster, se produce un error en las operaciones que cambian la pertenencia al clúster (como agregar o eliminar un host).

Para añadir tu nuevo host al grupo agrupado:

1. Asegúrate de que todos tus anfitriones estén en línea y puedan contactar con ellos.
2. Asegúrese de que los hosts del grupo puedan comunicarse en los siguientes puertos:
    - TCP: 8892, 8896, 21064
    - UDP: 5404, 5405 (no multidifusión)
3. Asegúrese de que el host que se une tenga una dirección IP asignada en la NIC que se une a la red de clústeres del grupo.
4. Asegúrese de que ningún host del grupo esté desconectado cuando un nuevo host intente unirse al grupo agrupado en clústeres.
5. Si no se puede recuperar un host sin conexión, márquelo como inactivo para eliminarlo del clúster. Para obtener más información, consulte Un host de mi grupo agrupado está desconectado y no puedo recuperarlo. ¿Cómo elimino el host de mi clúster?

¿Qué hago si algunos miembros del grupo agrupado no se unen al clúster automáticamente?

Este problema puede deberse a que los miembros del grupo agrupado pierden la sincronización.

Para volver a sincronizar los miembros del grupo agrupado, utilice el siguiente comando:

```
xe cluster-pool-resync cluster-uuid=<cluster_uuid>
```

Si el problema persiste, puede intentar volver a conectar la GFS2 SR. Puede realizar esta tarea mediante la CLI xe o mediante XenCenter.

Vuelva a conectar el GFS2 SR mediante la CLI xe:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Separe la GFS2 SR de la piscina. En cada host, ejecute el comando `xe pbd-unplug uuid=<uuid_of_pbd>`xe de la CLI.
2. Deshabilite el grupo agrupado mediante el comando `xe cluster-pool-destroy cluster-uuid=<cluster_uuid>`

   Si el comando anterior no se ejecuta correctamente, puede deshabilitar forzosamente un grupo agrupado ejecutándolo `xe cluster-host-force-destroy uuid=<cluster_host>` en todos los hosts del grupo.
3. Vuelva a habilitar el grupo agrupado mediante el comando `xe cluster-pool-create network-uuid=<network_uuid> [cluster-stack=cluster_stack] [token-timeout=token_timeout] [token-timeout-coefficient=token_timeout_coefficien ]`
4. Vuelva a conectar el GFS2 SR ejecutando el comando `xe pbd-plug uuid=<uuid_of_pbd>` en cada host.

Como alternativa, para usar XenCenter para volver a conectar el GFS2 SR:

1. **En la pestaña**Almacenamiento**del grupo, haga clic con el botón derecho en la GFS2 SR y seleccione Separar**….
2. En la barra de herramientas, seleccione **Grupo > Propiedades**.
3. En la pestaña Clústeres, deselecciona **Habilitarclústeres**.
4. Haga clic en **Aceptar** para aplicar el cambio.
5. En la barra de herramientas, seleccione **Grupo > Propiedades**.
6. En la pestaña **Clústeres**, selecciona **Habilitar clústeres** y elige la red que quieres usar para la agrupación en clústeres.
7. Haga clic en **Aceptar** para aplicar el cambio.
8. **En la pestaña**Almacenamiento de**la piscina, haga clic con el botón derecho en la GFS2 SR y seleccione Reparar.**

¿Cómo puedo saber si mi anfitrión tiene autoprotección?

Si el host se autodelimitó, es posible que se haya vuelto a unir al clúster cuando se reinició. Para comprobar si un host se ha autodelimitado y se ha recuperado, puede comprobar el `/var/opt/xapi-clusterd/boot-times` archivo para ver las horas en que se inició el host. Si hay horas de inicio en el archivo que no esperaba ver, el anfitrión se ha autodelimitado.

¿Por qué mi anfitrión está desconectado? ¿Cómo puedo recuperarlo?

Hay muchas razones posibles para que un anfitrión se desconecte. Dependiendo del motivo, el host puede recuperarse o no.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Los siguientes motivos por los que un host está fuera de línea son más comunes y se pueden solucionar recuperando el host:

- Cierre limpio
- Cierre forzado
- Fallo eléctrico temporal
- Reiniciar

Los siguientes motivos por los que un host está fuera de línea son menos frecuentes:

- Fallo permanente del hardware del host
- Fallo permanente de la fuente de alimentación del host
- Partición de red
- Fallo del conmutador de red

Estos problemas se pueden solucionar sustituyendo el hardware o marcando los hosts que han fallado como inactivos.

Un host de mi grupo agrupado está desconectado y no puedo recuperarlo. ¿Cómo elimino el host de mi clúster?

Puede decirle al clúster que olvide el host. Esta acción elimina el host del clúster de forma permanente y reduce la cantidad de hosts activos necesarios para el quórum.

Para eliminar un host irrecuperable, utilice el siguiente comando:

```
xe host-forget uuid=<host_uuid>
```

Este comando elimina el host del clúster de forma permanente y reduce la cantidad de hosts activos necesarios para el quórum.

> **Nota:**
>
> Si el host no está desconectado, este comando puede provocar la pérdida de datos. Se te pedirá que confirmes que estás seguro antes de continuar con el comando.

Una vez olvidado un host, no se puede volver a agregar al clúster. Para volver a agregar este host al clúster, debe realizar una instalación nueva de XenServer en el host.

He reparado un huésped que estaba marcado como muerto. ¿Cómo lo vuelvo a añadir a mi clúster?

Un host de XenServer marcado como inactivo no se puede volver a agregar al clúster. Para volver a agregar este sistema al clúster, debe realizar una instalación nueva de XenServer. Esta nueva instalación aparece en el clúster como un host nuevo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Qué hago si mi clúster sigue perdiendo quórum y sus anfitriones mantienen el cerco?

Si uno o más de los hosts de XenServer del clúster entran en un bucle cerrado debido a que pierden o ganan quórum de forma continua, puede arrancar el host con el argumento de la línea de comandos del `nocluster` kernel. Conéctese a la consola física o serie del host y edite los argumentos de arranque en grub.

Ejemplo :

```
/boot/grub/grub.cfg
menuentry 'XenServer' {

        search --label --set root root-oyftuj
        multiboot2 /boot/xen.gz dom0_mem=4096M,max:4096M watchdog ucode
            =scan dom0_max_vcpus=1-16 crashkernel=192M,below=4G console=
            vga vga=mode-0x0311
        module2 /boot/vmlinuz-4.4-xen root=LABEL=root-oyftuj ro nolvm
            hpet=disable xencons=hvc console=hvc0 console=tty0 quiet vga
            =785 splash plymouth.ignore-serial-consoles nocluster
        module2 /boot/initrd-4.4-xen.img
 }

menuentry 'XenServer (Serial)' {

        search --label --set root root-oyftuj
        multiboot2 /boot/xen.gz com1=115200,8n1 console=com1,vga
            dom0_mem=4096M,max:4096M watchdog ucode=scan dom0_max_vcpus
            =1-16 crashkernel=192M,below=4G
        module2 /boot/vmlinuz-4.4-xen root=LABEL=root-oyftuj ro nolvm
            hpet=disable console=tty0 xencons=hvc console=hvc0 nocluster
        module2 /boot/initrd-4.4-xen.img
 }

<!--NeedCopy-->
```

¿Qué ocurre cuando el coordinador de la piscina se reinicia en una piscina agrupada?

En la mayoría de los casos, el comportamiento cuando el coordinador del grupo se cierra o reinicia en un grupo agrupado es el mismo que cuando otro miembro del grupo cierra o reinicia.

La forma en que se cierra o reinicia el host puede afectar al quórum del grupo agrupado en clústeres. Para obtener más información sobre el quórum, consulte Quórum.

La única diferencia de comportamiento depende de si la HA está habilitada en su grupo:

- Si la alta disponibilidad está habilitada, se selecciona un nuevo coordinador y se mantiene el servicio general.
- Si la alta disponibilidad no está habilitada, no hay ningún coordinador para el grupo. Las máquinas virtuales en ejecución en los hosts restantes siguen ejecutándose. La mayoría de las

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

operaciones administrativas no están disponibles hasta que el coordinador se reinicie.

¿Por qué ha desaparecido mi piscina después de que un anfitrión de la piscina agrupada se vea obligado a cerrar?

Si cierra un host de forma normal (no forzosa), se elimina temporalmente de los cálculos de quórum hasta que se vuelva a activar. Sin embargo, si se apaga por la fuerza un host o se queda sin alimentación, ese host seguirá contabilizándose para los cálculos del quórum. Por ejemplo, si tiene un grupo de 3 anfitriones y cierra por la fuerza 2 de ellos, el anfitrión restante se cierra porque ya no tiene quórum.

Intenta cerrar siempre de forma limpia los anfitriones de una piscina agrupada. Para obtener más información, consulte Administrar su grupo agrupado.

¿Por qué se reiniciaron todos los hosts del grupo agrupado al mismo tiempo?

Se considera que todos los hosts de un clúster activo han perdido quórum cuando la cantidad de hosts contactables en el grupo es inferior a estos valores:

- Para una piscina con un número par de anfitriones: n/2
- Para una piscina con un número impar de anfitriones: (n+1) /2

La letra n indica el número total de hosts del grupo agrupado. Para obtener más información sobre el quórum, consulte Quórum.

En esta situación, todos los hosts se autocercan y verá que todos los hosts se reinician.

Para diagnosticar por qué el grupo perdió el quórum, la siguiente información puede ser útil:

- En XenCenter, consulte **la sección Notificaciones para ver la** hora en que se produjo el problema para ver si se produjo el autobloqueo.
- En los hosts del clúster, compruebe `/var/opt/xapi-clusterd/boot-times` si se ha producido un reinicio en un momento inesperado.
- En `Crit.log`, compruebe si se emite algún mensaje de autodelimitación.
- Revise el resultado del `dlm_tool status` comando para obtener información sobre el vallado.

  Ejemplo `dlm_tool status` de salida:

```
dlm_tool status

cluster nodeid 1 quorate 1 ring seq 8 8
daemon now 4281 fence_pid 0
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  node 1 M add 3063 rem 0 fail 0 fence 0 at 0 0
  node 2 M add 3066 rem 0 fail 0 fence 0 at 0 0
  <!--NeedCopy-->
```

Al recopilar registros para la depuración, recopile información de diagnóstico de todos los hosts del clúster. En el caso de que un único host se autoproteja, es más probable que los demás hosts del clúster dispongan de información útil.

Recopile informes completos sobre el estado de los servidores de los hosts de su grupo agrupado en clústeres. Para obtener más información, consulte Registros de host de XenServer.

¿Por qué no puedo recuperar mi grupo agrupado cuando tengo quórum?

Si tiene un grupo agrupado en clústeres con un número par de hosts, el número de hosts necesario para *lograr* el quórum es uno más que el número de hosts necesario para *conservar* el quórum. Para obtener más información sobre el quórum, consulte Quórum.

Si se encuentra en un grupo de números pares y ha recuperado la mitad de los hosts, debe recuperar un host más antes de poder recuperar el clúster.

¿Por qué aparece un `Invalid token` error al cambiar la configuración del clúster?

Al actualizar la configuración del clúster, es posible que reciba el siguiente mensaje de error sobre un token no válido (`"[[\"InternalError\",\"Invalid token\"]]"`).

Puede resolver este problema siguiendo los pasos siguientes:

1. (Opcional) Realice una copia de seguridad de la configuración actual del clúster recopilando un informe de estado del servidor que incluya los registros de xapi-clusterd y del sistema.
2. Use XenCenter para separar el GFS2 SR del grupo agrupado en clústeres.

   En la pestaña Almacenamiento**del grupo, haga clic con el botón derecho en la GFS2 SR y seleccione Separar**....
3. En cualquier host del clúster, ejecute este comando para destruir el clúster por la fuerza:

   ```
   xe cluster-pool-force-destroy cluster-uuid=<uuid>
   ```
4. Use XenCenter para volver a habilitar la agrupación en clústeres en su grupo.

   a) En la barra de herramientas, seleccione **Grupo > Propiedades**.
   b) En la pestaña **Clústeres**, selecciona **Habilitar clústeres** y elige la red que quieres usar para la agrupación en clústeres.
   c) Haga clic en **Aceptar** para aplicar el cambio

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Use XenCenter para volver a conectar el GFS2 SR al grupo.

   En la pestaña Almacenamiento de**la piscina, haga clic con el botón derecho en la GFS2 SR y seleccione Reparar.**

---

layout: doc
description: Use Active Directory to create additional users that can administer XenServer. Configure the user permissions with role-based access control.—

Administrar usuarios

La definición de usuarios, grupos, funciones y permisos le permite controlar quién tiene acceso a los hosts y grupos de XenServer y qué acciones pueden realizar.

Al instalar XenServer por primera vez, se agrega automáticamente una cuenta de usuario a XenServer. Esta cuenta es el superusuario local (LSU), o root, que XenServer autentica localmente.

La LSU, o raíz, es una cuenta de usuario especial destinada a la administración del sistema y tiene todos los permisos. En XenServer, la LSU es la cuenta predeterminada en la instalación. XenServer autentica la cuenta de LSU. La LSU no requiere ningún servicio de autenticación externo. Si se produce un error en un servicio de autenticación externo, la LSU aún puede iniciar sesión y administrar el sistema. La LSU siempre puede acceder al servidor físico de XenServer a través de SSH.

Puede crear más usuarios agregando las cuentas de Active Directory a través de la ficha Usuarios de XenCenter o la CLI de xe. Si su entorno no usa Active Directory, está limitado a la cuenta de LSU.

> **Nota:**
>
> Al crear usuarios, XenServer no asigna automáticamente funciones RBAC a las cuentas de usuario recién creadas. Por lo tanto, estas cuentas no tienen acceso al grupo de XenServer hasta que se les asigne una función.

Estos permisos se otorgan a través de roles, como se explica en la sección *Autenticación de usuarios con Active Directory (AD)*.

Autenticar usuarios con Active Directory (AD)

Si desea tener varias cuentas de usuario en un host o un grupo, debe usar las cuentas de usuario de Active Directory para la autenticación. Las cuentas de AD permiten a los usuarios de XenServer iniciar sesión en un grupo con sus credenciales de dominio de Windows.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Puede habilitar el enlace de canales LDAP y la firma LDAP en sus controladores de dominio de AD. Para obtener más información, consulte Asesoramiento de seguridad de Microsoft.

Puede configurar distintos niveles de acceso para usuarios específicos habilitando la autenticación de Active Directory, agregando cuentas de usuario y asignando funciones a esas cuentas.

Los usuarios de Active Directory pueden usar la CLI xe (pasando los argumentos `-u` y `-pw` apropiados) y también conectarse al host mediante XenCenter. La autenticación se realiza por grupo de recursos.

Los sujetos controlan el acceso a las cuentas de usuario. En XenServer, un sujeto se asigna a una entidad del servidor Active Directory (un usuario o un grupo). Al habilitar la autenticación externa, XenServer comprueba las credenciales utilizadas para crear una sesión con las credenciales raíz locales y, a continuación, con la lista de asuntos. Para permitir el acceso, cree una entrada de asunto para la persona o el grupo al que quiere conceder acceso. Puede usar XenCenter o la CLI xe para crear una entrada de asunto.

Si está familiarizado con XenCenter, tenga en cuenta que la CLI xe utiliza una terminología ligeramente diferente para referirse a Active Directory y a las funciones de las cuentas de usuario:

Término de XenCenter	Exe CLI Term
Usuarios, Agregar usuarios	Asignaturas, Agregar asignaturas

Aunque XenServer está basado en Linux, XenServer le permite usar cuentas de Active Directory para las cuentas de usuario de XenServer. Para hacerlo, pasa las credenciales de Active Directory al controlador de dominio de Active Directory.

Al agregar Active Directory a XenServer, los usuarios y grupos de Active Directory se convierten en sujetos de XenServer. Los sujetos se denominan usuarios en XenCenter. Los usuarios o grupos se autentican mediante Active Directory al iniciar sesión al registrar un asunto en XenServer. Los usuarios y los grupos no necesitan calificar su nombre de usuario mediante un nombre de dominio.

Para calificar un nombre de usuario, debe escribir el nombre de usuario en el formato Nombre de inicio de sesión de nivel inferior; por ejemplo, `mydomain\myuser`.

> **Nota:**
>
> De forma predeterminada, si no calificó el nombre de usuario, XenCenter intentará iniciar sesión en los servidores de autenticación de AD mediante el dominio al que está unido. La excepción a

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> esto es la cuenta de LSU, que XenCenter siempre autentica primero de forma local (es decir, en el XenServer).

El proceso de autenticación externa funciona de la siguiente manera:

1. Las credenciales que se proporcionan al conectarse a un host se pasan al controlador de dominio de Active Directory para su autenticación.
2. El controlador de dominio comprueba las credenciales. Si no son válidas, la autenticación falla de inmediato.
3. Si las credenciales son válidas, se consulta al controlador de Active Directory para obtener el identificador del sujeto y la pertenencia al grupo asociados a las credenciales.
4. Si el identificador del sujeto coincide con el almacenado en XenServer, la autenticación se realiza correctamente.

Cuando se une a un dominio, habilita la autenticación de Active Directory para el grupo. Sin embargo, cuando un grupo se une a un dominio, solo los usuarios de ese dominio (o un dominio con el que tiene relaciones de confianza) pueden conectarse al grupo.

> **Nota:**
>
> La actualización manual de la configuración DNS de un PIF de red configurado por DHCP no es compatible y puede provocar que la integración de AD y, por lo tanto, la autenticación de usuarios, fallen o dejen de funcionar.

Configurar la autenticación de Active Directory

XenServer admite el uso de servidores Active Directory con Windows 2008 o posterior.

Para autenticar Active Directory para los hosts de XenServer, debe usar el mismo servidor DNS tanto para el servidor Active Directory (configurado para permitir la interoperabilidad) como para el host de XenServer.
En algunas configuraciones, el servidor Active Directory puede proporcionar el propio DNS. Esto se puede lograr mediante DHCP para proporcionar la dirección IP y una lista de servidores DNS al host de XenServer. Como alternativa, puede establecer los valores en los objetos PIF o usar el instalador cuando se usa una configuración estática manual.

Recomendamos habilitar DHCP para asignar nombres de host. No asigne los nombres de host `localhost` ni `linux` a los hosts.

> **Advertencia:**
>
> Los nombres de host de XenServer deben ser únicos en toda la implementación de XenServer.

Tenga en cuenta lo siguiente:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- XenServer etiqueta su entrada de AD en la base de datos de AD con su nombre de host. Si dos hosts XenServer con el mismo nombre de host se unen al mismo dominio de AD, el segundo XenServer sobrescribe la entrada de AD del primer XenServer. La sobrescritura se produce independientemente de si los hosts pertenecen al mismo grupo o a grupos diferentes. Esto puede provocar que la autenticación de AD en el primer XenServer deje de funcionar.

  Puede usar el mismo nombre de host en dos hosts de XenServer, siempre que se unan a dominios de AD diferentes.

- Los hosts de XenServer pueden estar en diferentes zonas horarias, ya que se compara con la hora UTC. Para garantizar que la sincronización sea correcta, puede usar los mismos servidores NTP para el grupo de XenServer y el servidor Active Directory.

- No se admiten los grupos de autenticación mixta. No puede tener un grupo en el que algunos hosts del grupo estén configurados para usar Active Directory y otros no.

- La integración de XenServer Active Directory utiliza el protocolo Kerberos para comunicarse con los servidores Active Directory. Por lo tanto, XenServer no admite la comunicación con servidores Active Directory que no utilizan Kerberos.

- Para que la autenticación externa mediante Active Directory se realice correctamente, los relojes de los hosts de XenServer deben estar sincronizados con los relojes del servidor Active Directory. Cuando XenServer se une al dominio de Active Directory, se comprueba la sincronización y se produce un error en la autenticación si hay demasiada asimetría entre los servidores.

> **Advertencia:**
>
> Los nombres de host deben constar únicamente de un máximo de 63 caracteres alfanuméricos y no deben ser puramente numéricos.
>
> Una limitación en los clientes SSH recientes significa que SSH no funciona para nombres de usuario que contienen alguno de los siguientes caracteres: `{ } [] | &`. Asegúrese de que sus nombres de usuario y nombres de servidores de Active Directory no contengan ninguno de estos caracteres.

Cuando agrega un host a un grupo después de habilitar la autenticación de Active Directory, se le pide que configure Active Directory en el host que se une al grupo. Cuando se le soliciten las credenciales del host de unión, escriba las credenciales de Active Directory con privilegios suficientes para agregar hosts a ese dominio.

Integración con Active Directory

Asegúrese de que los siguientes puertos de firewall estén abiertos al tráfico saliente para que XenServer pueda acceder a los controladores de dominio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puerto	Protocolo	Uso
53	UDP/TCP	DNS
88	UDP/TCP	Kerberos 5
123	UDP	NTP
137	UDP	Servicio de nombres NetBIOS
139	TCP	Sesión NetBIOS (SMB)
389	UDP/TCP	LDAP
445	TCP	SMB a través de TCP
464	UDP/TCP	Cambios de contraseña de máquinas
636	UDP/TCP	LDAP por SSL
3268	TCP	Búsqueda en el catálogo global

Para obtener más información, consulte Puertos de comunicación utilizados por XenServer.

> **Notas:**
>
> - Para ver las reglas de firewall en un equipo Linux usando *iptables*, ejecute el siguiente comando: `iptables -nL`.

Winbind

XenServer usa Winbind para autenticar a los usuarios de Active Directory (AD) en el servidor de AD y para cifrar las comunicaciones con el servidor de AD.

Winbind no admite los siguientes casos:

- Espacio al principio o al final de un nombre de usuario o grupo de dominios de dominio.
- Nombres de usuario de dominio que contengan 64 caracteres o más.
- Nombres de usuario de dominio que incluyan cualquiera de los caracteres especiales +<>” =/%@:,;\ ‘
- Nombres de grupos de dominios que incluyan cualquiera de los caracteres especiales,;\ ‘

Configuración de Winbind Configure el comportamiento de Winbind con las siguientes opciones de configuración, que se pueden incluir en el archivo `/etc/xapi.conf`:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- `winbind_machine_pwd_timeout`: El valor de esta opción define la frecuencia, en segundos, con la que se rota la contraseña de la máquina para este host de XenServer. Defina un valor como entero.

  El valor predeterminado es 1209600 segundos (14 días). Se recomienda conservar el valor predeterminado o no reducirlo por debajo del valor predeterminado para garantizar el tiempo suficiente para sincronizar la nueva contraseña entre los controladores de dominio.

- `winbind_kerberos_encryption_type`: Los valores de esta opción son sólidos, heredados y todo eso. El valor predeterminado es todos.

  - El valor `all` permite los siguientes conjuntos de cifrado: `aes256-cts-hmac-sha1-96`, `aes128-cts-hmac-sha1-96` y `arcfour-hmac-md5`
  - El valor `strong` permite los siguientes conjuntos de cifrado: `aes256-cts-hmac-sha1-96` y `aes128-cts-hmac-sha1-96`
  - El valor `legacy` permite los siguientes conjuntos de cifrado: `arcfour-hmac-md5`

    La opción antigua no es segura y ñe recomendamos que solo la utilices para depurar problemas.

  Para mejorar la seguridad, le recomendamos que aplique el cifrado AES. Para ello:

  1. Asegúrese de que el controlador de dominio admita `aes256-cts-hmac-sha1-96` y `aes128-cts-hmacsha1-96`.
  2. Configure el controlador de dominio para habilitar **El otro dominio admite el cifrado AES Kerberos** en la confianza del dominio.

     Para obtener más información, consulte Método 3: configurar la confianza para que admita el cifrado AES128 y AES 256 en lugar del cifrado RC4 en la documentación de Microsoft.
  3. Actualice la `winbind_kerberos_encryption_type` opción para usar el valor `strong`.
  4. Reinicie la pila de herramientas.

     No reinicie la pila de herramientas mientras la alta disponibilidad esté habilitada. Si es posible, inhabilite temporalmente HA antes de reiniciar la pila de herramientas.

- `winbind_cache_time`: Winbind almacena en caché algunos datos de dominio de forma local. El valor de esta opción define el número de segundos entre cada actualización de la caché. El valor predeterminado es de 60 segundos.

Tras actualizar cualquiera de estas opciones de configuración, reinicie la pila de herramientas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Cómo administra XenServer la contraseña de la cuenta de máquina para la integración de AD?

Al igual que en las máquinas cliente Windows, Winbind actualiza automáticamente la contraseña de la cuenta de la máquina. Winbind actualiza automáticamente la contraseña de la cuenta de la máquina cada 14 días o según lo especifique la opción `winbind_machine_pwd_timeout`de configuración.

Habilitar la autenticación externa en un grupo

La autenticación externa mediante Active Directory se puede configurar mediante XenCenter o la CLI mediante el siguiente comando.

```
xe pool-enable-external-auth auth-type=AD \
  service-name=full-qualified-domain \
  config:user=username \
  config:pass=password
<!--NeedCopy-->
```

El usuario especificado debe tener privilegios `Add/remove computer objects or workstations`, que es el valor predeterminado para los administradores de dominio.

Si no utiliza DHCP en la red que utilizan Active Directory y los hosts de XenServer, utilice los siguientes enfoques para configurar el DNS:

1. Configure el orden de búsqueda de sufijos DNS de dominio para resolver entradas que no sean de FQDN:

   ```
   xe pif-param-set uuid=pif_uuid_in_the_dns_subnetwork \
      "other-config:domain=suffix1.com suffix2.com suffix3.com"
   <!--NeedCopy-->
   ```

2. Configure el servidor DNS para usarlo en los hosts de XenServer:

   ```
   xe pif-reconfigure-ip mode=static dns=dnshost ip=ip \
     gateway=gateway netmask=netmask uuid=uuid
   <!--NeedCopy-->
   ```

3. Configure manualmente la interfaz de administración para usar un PIF que esté en la misma red que su servidor DNS:

   ```
   xe host-management-reconfigure pif-uuid=pif_in_the_dns_subnetwork
   <!--NeedCopy-->
   ```

> **Nota:**
>
> La autenticación externa es una propiedad por host. Sin embargo, le recomendamos que habilite y inhabilite la autenticación externa por grupo. Una configuración por grupo permite a

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> XenServer tratar los errores que se producen al habilitar la autenticación en un host determinado. XenServer también revierte cualquier cambio que pueda ser necesario, lo que garantiza una configuración coherente en todo el grupo. Use el comando `host-param-list` para inspeccionar las propiedades de un host y para determinar el estado de la autenticación externa comprobando los valores de los campos relevantes.

Use XenCenter para inhabilitar la autenticación de Active Directory o el siguiente comando xe:

```
xe pool-disable-external-auth
<!--NeedCopy-->
```

Autenticación de usuarios

Para permitir que un usuario acceda al host de XenServer, debe agregar un asunto para ese usuario o grupo en el que se encuentre. (Las pertenencias a grupos transitivos también se verifican de la manera normal. Por ejemplo, agregar un asunto para el grupo `A`, donde el grupo `A` contiene el grupo `B` y `user 1` es miembro del grupo `B` permitiría el acceso a `user 1`). Si quiere administrar los permisos de usuario en Active Directory, puede crear un único grupo que, a continuación, agregue y elimine usuarios hacia/desde. Como alternativa, puede agregar y eliminar usuarios individuales de XenServer o una combinación de usuarios y grupos, según corresponda, según sus requisitos de autenticación. Puede administrar la lista de asuntos desde XenCenter o mediante la CLI como se describe en la siguiente sección.

Al autenticar a un usuario, las credenciales se comparan primero con la cuenta raíz local, lo que le permite recuperar un sistema cuyo servidor de AD ha fallado. Si las credenciales (nombre de usuario y contraseña) no coinciden, se realiza una solicitud de autenticación al servidor de AD. Si la autenticación tiene éxito, la información del usuario se recupera y valida en la lista de temas local. Se deniega el acceso si la autenticación falla. La validación con respecto a la lista de temas se realiza correctamente si el usuario o un grupo de la pertenencia al grupo transitivo del usuario está en la lista de asuntos.

> **Nota:**
>
> Cuando se usan grupos de Active Directory para conceder acceso a los usuarios del administrador de grupos que requieren acceso ssh de host, el tamaño del grupo de AD no debe superar los 500 usuarios.

Para agregar un asunto de AD a XenServer:

```
xe subject-add subject-name=entity_name
<!--NeedCopy-->
```

Entity_name es el nombre del usuario o grupo al que quiere conceder acceso. Puede incluir el dominio de la entidad (por ejemplo, 'xendt\ user1'en lugar de 'user1'), aunque el comportamiento es el mismo

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a menos que se requiera la desambiguación.

Busque el identificador de sujeto del usuario. El identificador es el usuario o el grupo que lo contiene. Al eliminar un grupo, se elimina el acceso a todos los usuarios de ese grupo, siempre que no se especifiquen también en la lista de asuntos. Use el comando `subject list` para buscar el identificador de sujeto del usuario. :

```
xe subject-list
<!--NeedCopy-->
```

Este comando devuelve una lista de todos los usuarios.

Para aplicar un filtro a la lista, por ejemplo, para buscar el identificador de asunto de un usuario `user1` en el comando `testad`:

```
xe subject-list other-config:subject-name='testad\user1'
<!--NeedCopy-->
```

Elimine al usuario mediante el comando `subject-remove` y pase el identificador de sujeto que aprendió en el paso anterior:

```
xe subject-remove subject-uuid=subject_uuid
<!--NeedCopy-->
```

Puede finalizar cualquier sesión actual que este usuario ya haya autenticado. Para obtener más información, consulte *Terminar todas las sesiones autenticadas con xe* y *Terminar sesiones de usuarios individuales con xe* en la siguiente sección. Si no finaliza las sesiones, los usuarios con permisos revocados pueden seguir accediendo al sistema hasta que cierren sesión.

Ejecute el siguiente comando para identificar la lista de usuarios y grupos con permiso para acceder al host o grupo de XenServer:

```
xe subject-list
<!--NeedCopy-->
```

Eliminar el acceso de un usuario

Cuando un usuario se autentica, puede acceder al host hasta que finalice su sesión o hasta que otro usuario finalice su sesión. Eliminar a un usuario de la lista de asuntos, o eliminarlo de un grupo en la lista de asuntos, no revoca automáticamente ninguna sesión ya autenticada que tenga el usuario. Los usuarios pueden seguir accediendo al grupo mediante XenCenter u otras sesiones de API que ya hayan creado. XenCenter y la CLI brindan facilidades para finalizar sesiones individuales o todas las sesiones activas de manera forzada. Consulte la documentación de XenCenter para obtener información sobre los procedimientos que utilizan XenCenter o la siguiente sección para conocer los procedimientos que utilizan la CLI.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Finalizar todas las sesiones autenticadas con xe

Ejecute el siguiente comando de la CLI para finalizar todas las sesiones autenticadas con xe:

```
xe session-subject-identifier-logout-all
<!--NeedCopy-->
```

Finalizar sesiones de usuarios individuales mediante xe

1. Determine el identificador de sujeto de cuya sesión quiere cerrar sesión. Use los comandos `session-subject-identifier-list` o `subject-list` xe para buscar el identificador de sujeto. El primer comando muestra a los usuarios que tienen sesiones. El segundo comando muestra todos los usuarios, pero se puede filtrar. Por ejemplo, mediante el uso de un comando como `xe subject-list other-config:subject-name=xendt\\user1`. Es posible que necesite una barra invertida doble (como se muestra en función de su caparazón).
2. Ejecute el comando `session-subject-logout`, pasando el identificador de asunto que ha determinado en el paso anterior como parámetro, por ejemplo:

   ```
   xe session-subject-identifier-logout subject-identifier=subject_id
   <!--NeedCopy-->
   ```

Dejar un dominio de AD

> **Advertencia:**
>
> Al salir del dominio, todos los usuarios que se hayan autenticado en el grupo o el host con credenciales de Active Directory se desconectan.

Use XenCenter para dejar un dominio de AD. Para obtener más información, consulte la documentación de XenCenter. Ejecute alternativamente el comando `pool-disable-external-auth`, especificando el UUID del grupo si es necesario.

> **Nota:**
>
> Dejar el dominio no elimina los objetos de host de la base de datos de AD. Consulte la documentación de Active Directory para obtener información sobre cómo detectar y eliminar las entradas de host inhabilitadas.

Control de acceso basado en roles

August 24, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La función de control de acceso basado en roles (RBAC) de XenServer le permite asignar usuarios, roles y permisos para controlar quién tiene acceso a su XenServer y qué acciones pueden realizar. El sistema RBAC de XenServer asigna un usuario (o un grupo de usuarios) a funciones definidas (un conjunto de permisos con nombre). Las funciones tienen permisos de XenServer asociados para realizar determinadas operaciones.

Los permisos no se asignan directamente a los usuarios. Los usuarios adquieren permisos a través de roles que se les asignan. Por lo tanto, la administración de los permisos de usuario individuales se convierte en una cuestión de asignar al usuario el rol apropiado, lo que simplifica las operaciones comunes. XenServer mantiene una lista de usuarios autorizados y sus funciones.

RBAC le permite restringir las operaciones que pueden realizar los diferentes grupos de usuarios, lo que reduce la probabilidad de un accidente por parte de un usuario inexperto.

El RBAC también proporciona una función de registro de auditoría para el cumplimiento y la auditoría.

El RBAC depende de Active Directory para los servicios de autenticación. En concreto, XenServer mantiene una lista de usuarios autorizados basada en las cuentas de usuario y grupo de Active Directory. Como resultado, debe unirse al grupo al dominio y agregar cuentas de Active Directory antes de poder asignar funciones.

El superusuario local (LSU), o raíz, es una cuenta de usuario especial que se utiliza para la administración del sistema y tiene todos los derechos o permisos. El superusuario local es la cuenta predeterminada en la instalación en XenServer. La LSU se autentica a través de XenServer y no a través de un servicio de autenticación externo. Si el servicio de autenticación externa falla, la LSU aún puede iniciar sesión y administrar el sistema. La LSU siempre puede acceder al host físico de XenServer a través de SSH.

Proceso RBAC

En la siguiente sección se describe el proceso estándar para implementar RBAC y asignar una función a un usuario o grupo:

1. Únete al dominio. Para obtener más información, consulte Habilitar la autenticación externa en un grupo.
2. Agregue un usuario o grupo de Active Directory al grupo. Esto se convierte en un tema. Para obtener más información, consulte Para agregar un asunto a RBAC.
3. Asigne (o cambie) la función de RBAC del sujeto. Para obtener más información, consulte Para asignar una función de RBAC a un sujeto.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

layout: doc
description: Learn about the different roles and permissions that can be assigned to your XenServer users.—

Funciones y permisos de RBAC

Roles

XenServer se suministra con las siguientes seis funciones preestablecidas:

- *Administrador* de grupos (administrador de grupos): igual que la raíz local. Puede realizar todas las operaciones.

  > **Nota:**
  >
  > El superusuario local (root) tiene la función de "Administrador del grupo". La función de administrador del grupo tiene los mismos permisos que la raíz local.
  >
  > Si le quitas la función de administrador del grupo a un usuario, considera la posibilidad de cambiar también la contraseña raíz y rotar el secreto del grupo. Para obtener más información, consulte Seguridad de la agrupación.

- *Operador* de Agrupación (Operador de Agrupación): Puede hacer todo aparte de agregar/eliminar usuarios y cambiar sus roles. Esta función se centra principalmente en la administración de hosts y grupos (es decir, crear almacenamiento, crear grupos, administrar los hosts, etc.).
- *Virtual Machine Power Administrator* (VM Power Admin): crea y administra máquinas virtuales. Esta función se centra en aprovisionar máquinas virtuales para que las use un operador de VM.
- *Administrador de máquinas virtuales (administrador* de VM): similar a un administrador de energía de VM, pero no puede migrar máquinas virtuales ni realizar instantáneas.
- *Operador de máquina virtual* (operador de VM), similar al administrador de VM, pero no puede crear/destruir máquinas virtuales, pero puede realizar operaciones de ciclo de vida de inicio/detención.
- *Solo lectura* (solo lectura): puede ver el grupo de recursos y los datos de rendimiento.

> **Nota:**
>
> - Para aplicar actualizaciones a los grupos de XenServer 8, debe iniciar sesión en XenCenter como administrador u operador de grupos, o con una cuenta raíz local.
> - Cuando se utilizan grupos de Active Directory para conceder acceso a los usuarios del administrador de grupos que requieren acceso SSH al host, el número de usuarios del grupo

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> de Active Directory no debe superar los 500.

Para obtener un resumen de los permisos disponibles para cada rol y para obtener información sobre las operaciones disponibles para cada permiso, consulte *Definiciones de roles y permisos de RBAC* en la siguiente sección.

Al crear un usuario en XenServer, primero debe asignar un rol al usuario recién creado para que pueda usar la cuenta. XenServer **no** asigna automáticamente un rol al usuario recién creado. Como resultado, estas cuentas no tienen acceso al grupo de XenServer hasta que se les asigne una función.

1. Modificar el tema a la asignación de roles. Esto requiere el permiso de asignar/modificar rol, que solo está disponible para un administrador del grupo.
2. Modifique la pertenencia al grupo que contiene el usuario en Active Directory.

Definiciones de roles y permisos de RBAC

En la siguiente tabla se resumen los permisos disponibles para cada función. Para obtener detalles sobre las operaciones disponibles para cada permiso, consulte *Definiciones de permisos*.

Permisos de roles	Administrador del grupo	Operador de grupo	Administrador de energía de VM	Administrador de VM	Operador de VM	Solo lectura
Asignar/modificar funciones	X					
Inicie sesión en consolas de servidor (físicas) (a través de SSH y XenCenter)	X					
Backup/restore de servidores	X					

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Permisos de roles	Administrador del grupo	Operador de grupo	Administrador de energía de VM	Administrador de VM	Operador de VM	Solo lectura
Importación/exportación de paquetes OVF/OVA e imágenes de disco	X					
Establecer núcleos por zócalo	X	X	X	X		
Convierta máquinas virtuales con XenServer Conversion Manager	X					
Bloqueo del puerto del conmutador	X	X				
Múltiples rutas	X	X				
Cerrar sesión en las conexiones de usuario activas	X	X				
Supervisar los recursos del host y del dom0 con NRPE	X					

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Permisos de roles	Administrador del grupo	Operador de grupo	Administrador de energía de VM	Administrador de VM	Operador de VM	Solo lectura
Supervisar los recursos de host y dom0 con SNMP	X					
Crear y descartar alertas	X	X				
Cancelar la tarea de cualquier usuario	X	X				
Administración de grupo	X	X				
Migración en vivo	X	X	X			
Migración en vivo de	X	X	X			
Operaciones avanzadas de VM	X	X	X			
Operaciones de creación/destrucción de VM	X	X	X	X		
Medios de CD de cambio de VM	X	X	X	X	X	
Cambio de estado de energía de VM	X	X	X	X	X	
Ver consolas de VM	X	X	X	X	X	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Permisos de roles	Administrador del grupo	Operador de grupo	Administrador de energía de VM	Administrador de VM	Operador de VM	Solo lectura
Operaciones de administración de vistas de XenCenter	X	X	X	X	X	
Cancelar tareas propias	X	X	X	X	X	X
Leer registros de auditoría	X	X	X	X	X	X
Conéctese al grupo y lea todos los metadatos del grupo	X	X	X	X	X	X
Configurar la GPU virtual	X	X				
Ver la configuración de GPU virtual	X	X	X	X	X	X
Acceder a la unidad de configuración (solo máquinas virtuales CoreOS)	X					

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Permisos de roles	Administrador del grupo	Operador de grupo	Administrador de energía de VM	Administrador de VM	Operador de VM	Solo lectura
Instantáneas programadas (agregar/quitar máquinas virtuales a programaciones de instantáneas existentes)	X	X	X			
Instantáneas programadas (agregar/-modificar/eliminar programaciones de instantáneas)	X	X				
Recopilar información de diagnóstico	X	X				
Configurar el seguimiento de bloques cambiados	X	X	X	X		
Listar bloques cambiados	X	X	X	X	X	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Permisos de roles	Administrador del grupo	Operador de grupo	Administrador de energía de VM	Administrador de VM	Operador de VM	Solo lectura
Configurar PVS-Accelerator	X	X				
Ver la configuración del acelerador PVS	X	X	X	X	X	X

Definiciones de permisos

Asignar/modificar funciones:

- Agregar/eliminar usuarios
- Agregar o quitar roles de los usuarios
- Habilitar y inhabilitar la integración de Active Directory (unirse al dominio)

Este permiso permite al usuario concederse a sí mismo cualquier permiso o realizar cualquier tarea.

Advertencia: Esta función permite al usuario inhabilitar la integración de Active Directory y todos los temas agregados desde Active Directory.

Inicie sesión en las consolas del servidor:

- Acceso a la consola del servidor mediante ssh
- Acceso a la consola del servidor mediante XenCenter

Advertencia: Con acceso a un shell raíz, la persona asignada puede reconfigurar arbitrariamente todo el sistema, incluido el RBAC.

Operaciones de creación/destrucción de VM de copia de seguridad/restauración de servidores:

- Realizar copias de seguridad y restaurar servidores
- Realizar copias de seguridad y restaurar metadatos de grupos

La capacidad de restaurar una copia de seguridad permite a la persona asignada revertir los cambios de configuración de RBAC.

Importar/exportar paquetes OVF/OVA e imágenes de disco:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Importar paquetes OVF y OVA
- Importar imágenes de disco
- Exportación de máquinas virtuales como paquetes OVF/OVA

Establecer núcleos por zócalo:

- Establecer la cantidad de núcleos por socket para las CPU virtuales de la VM

Este permiso permite al usuario especificar la topología de las CPU virtuales de la VM.

Convierta máquinas virtuales con XenServer Conversion Manager:

- Convertir máquinas virtuales VMware ESXi/vCenter en máquinas virtuales de XenServer

Este permiso permite al usuario convertir cargas de trabajo de VMware a XenServer copiando lotes de máquinas virtuales VMware ESXi/vCenter al entorno de XenServer.

Bloqueo del puerto del conmutador:

- Controlar el tráfico en una red

Este permiso permite al usuario bloquear todo el tráfico en una red de forma predeterminada o definir direcciones IP específicas desde las que una máquina virtual puede enviar tráfico.

Rutas múltiples:

- Habilitar multipathing
- Inhabilitar rutas múltiples

Cerrar sesión en las conexiones de usuario activas:

- Posibilidad de desconectar a los usuarios que han

Crear/descartar alertas:

- Configurar XenCenter para que genere alertas cuando el uso de recursos supere ciertos umbrales
- Eliminar alertas de la vista Alertas

Advertencia: un usuario con este permiso puede descartar las alertas de todo el grupo.

Nota: La capacidad de ver alertas forma parte del permiso Conectarse al grupo y leer todos los metadatos del grupo.

Cancela la tarea de cualquier usuario:

- Cancelar la tarea en ejecución de cualquier usuario

Este permiso permite al usuario solicitar a XenServer que cancele una tarea en curso iniciada por cualquier usuario.

Gestión de agrupaciones:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Establecer las propiedades del grupo (nombre, SR predeterminados)
- Crea un grupo agrupado
- Habilitar, inhabilitar y configurar la alta disponibilidad
- Establecer prioridades de reinicio de alta disponibilidad por VM
- Configurar DR y realizar operaciones de conmutación por error, conmutación por recuperación y conmutación por error de prueba de DR
- Habilitar, inhabilitar y configurar el equilibrio de carga de trabajo (WLB)
- Agregar y quitar el servidor del grupo
- Coordinador de transición de emergencia a agrupación
- Dirección del coordinador de agrupaciones de emergencia
- Miembros del grupo de recuperación de emergencia
- Designar un nuevo coordinador de agrupaciones
- Administrar los certificados de grupos y hosts
- Aplicación de parches
- Definir las propiedades del anfitrión
- Configurar el registro del host
- Habilitar y inhabilitar servidores
- Apagar, reiniciar y encender los servidores
- Reiniciar toolstack
- Informes de estado del sistema
- Solicitar licencia
- Migración en vivo de todas las demás máquinas virtuales de un host a otro host, debido al modo de mantenimiento o a la alta disponibilidad
- Configurar la interfaz de administración del host y las interfaces secundarias
- Desactivar la administración de hosts
- Eliminar volcados de memoria
- Agregar, modificar y eliminar redes
- Agregar, modificar y eliminar PBDS/PIFS/VLAN/Bonds/SRS
- Agregar, eliminar y recuperar secretos

Este permiso incluye todas las acciones necesarias para mantener un grupo.

Nota: Si la interfaz de administración no funciona, ningún inicio de sesión puede autenticarse, excepto los inicios de sesión raíz locales.

Migración en vivo:

- Migrar máquinas virtuales de un host a otro cuando las máquinas virtuales estén en almacenamiento compartido por ambos hosts

Migración de almacenamiento en vivo:

- Migrar de un host a otro host cuando las VM no estén en el almacenamiento compartido entre

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

los dos hosts
- Mover disco vDisk (VDI) de un SR a otro SR

Operaciones avanzadas de VM:

- Ajuste de la memoria de la VM (mediante el control dinámico de memoria)
- Cree una instantánea de VM con memoria, tome instantáneas de VM y deshaga las VM
- Migrar máquinas virtuales
- Iniciar máquinas virtuales, incluida la especificación del servidor físico
- Reanudar VM

Este permiso proporciona al cesionario privilegios suficientes para iniciar una máquina virtual en un host diferente si no está satisfecho con el host XenServer seleccionado.

Operaciones de creación/destrucción de VM:

- Instalar o eliminar
- Clonar/copiar máquinas virtuales
- Agregar, quitar y configurar dispositivos de disco vDisk/CD
- Agregar, eliminar y configurar dispositivos de red virtuales
- Importación/exportación de archivos XVA
- Cambio de configuración de VM
- Backup/restore de servidores

> **Nota:**
>
> La función de administrador de VM solo puede importar archivos XVA a un grupo con una SR compartida. La función de administrador de VM no tiene permisos suficientes para importar un archivo XVA en un host o en un grupo sin almacenamiento compartido.

CD de cambio de VM:

- Expulsar el CD actual
- Insertar CD nuevo

Importación/exportación de paquetes OVF/OVA; importación de imágenes de disco

Cambio de estado de energía de VM:

- Iniciar máquinas virtuales (colocación automática)
- Apagar máquinas virtuales
- Reiniciar máquinas virtuales
- Suspender máquinas virtuales
- Reanudar máquinas virtuales (colocación automática)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Este permiso no incluye start_on, resume_on y migrate, que forman parte del permiso de operaciones avanzadas de VM.

Ver consolas de VM:

- Vea e interactúe con consolas de VM

Este permiso no permite al usuario ver las consolas host.

Operaciones de administración de vistas de XenCenter:

- Crear y modificar carpetas globales de XenCenter
- Crear y modificar campos personalizados globales de XenCenter
- Crear y modificar búsquedas globales de XenCenter

Las carpetas, los campos personalizados y las búsquedas se comparten entre todos los usuarios que acceden al grupo

Cancelar tareas propias:

- Permite a un usuario cancelar sus propias tareas

Lea el registro de auditoría:

- Descargar el registro de auditoría de XenServer

Conéctese al grupo y lea todos los metadatos del grupo:

- Inicie sesión en la agrupación
- Ver metadatos del grupo
- Ver datos de rendimiento históricos
- Ver los usuarios que han iniciado sesión
- Ver usuarios y roles
- Ver mensajes
- Regístrese y reciba eventos

Configurar la GPU virtual:

- Especificar una directiva de ubicación para todo el grupo
- Asignar una GPU virtual a una VM
- Eliminar una GPU virtual de una VM
- Modificar los tipos de GPU virtuales permitidos
- Crear, destruir o asignar un grupo de GPU

Ver la configuración de GPU virtual:

- Ver GPU, directivas de ubicación de GPU y asignaciones de GPU virtuales

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Instantáneas programadas:

- Agregar máquinas virtuales a las programaciones de instantáneas existentes
- Eliminar las máquinas virtuales de las programaciones de instantáneas existentes
- Agregar programaciones de instantáneas
- Modificar programas de instantáneas
- Eliminar programaciones de instantáneas

Recopile información de diagnóstico de XenServer:

- Iniciar la recolección de GC y la compactación del montón
- Recopilar estadísticas de recolección de basura
- Recopilar estadísticas de bases
- Recopilar estadísticas de red

Configurar el seguimiento de bloques modificados:

- Habilitar el seguimiento de bloques modificados
- Desactivar el seguimiento de bloques modificados
- Destruya los datos asociados a una instantánea y conserve los metadatos
- Obtener la información de conexión NBD para una VDI

El seguimiento de bloques modificados solo se puede habilitar en instancias con licencia de XenServer Premium Edition.

Lista de bloques cambiados:

- Compare dos instantáneas de VDI y enumere los bloques que han cambiado entre ellas

Configurar PVS-Accelerator:

- Habilitar PVS-Accelerator
- Inhabilitar PVS-Accelerator
- Configuración de caché de actualización (PVS-Accelerator)
- Agregar o quitar configuración de caché (acelerador PVS)

Ver la configuración del acelerador PVS:

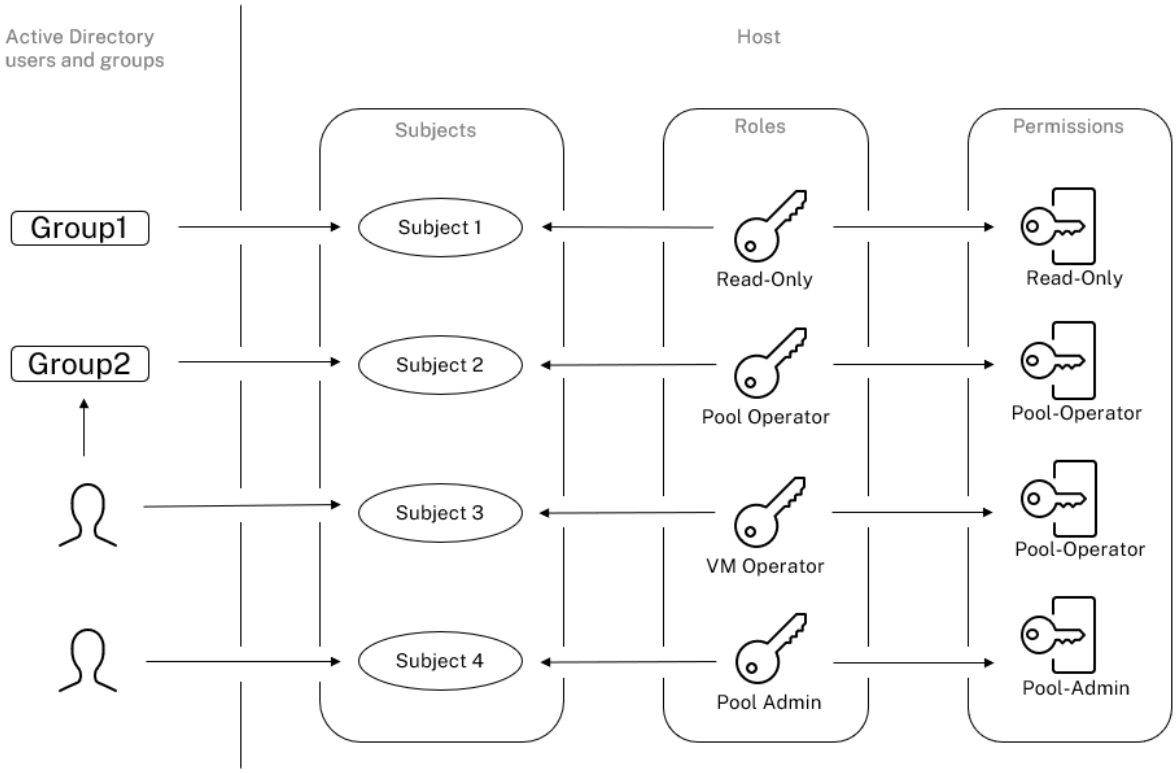
- Ver el estado de PVS-Accelerator

> **Nota:**
>
> A veces, un usuario de solo lectura no puede mover un recurso a una carpeta en XenCenter, incluso después de recibir una solicitud de elevación y proporcionar las credenciales de un usuario con más privilegios. En este caso, inicie sesión en XenCenter como el usuario más privilegiado y vuelva a intentar la acción.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Cómo calcula XenServer las funciones de la sesión?

1. El sujeto se autentica a través del servidor de Active Directory para comprobar a qué grupos contendientes puede pertenecer también el sujeto.
2. A continuación, XenServer verifica qué funciones se han asignado tanto al sujeto como a los grupos que lo contienen.
3. Como los sujetos pueden ser miembros de varios grupos de Active Directory, heredan todos los permisos de las funciones asociadas.



Usar RBAC con la CLI

August 24, 2023

comandos CLI de RBAC xe

Use los siguientes comandos para trabajar con roles y temas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para enumerar todos los roles definidos disponibles

Ejecute el comando: `xe role-list`

Este comando devuelve una lista de los roles definidos actualmente, por ejemplo:

```
     uuid( RO): 0165f154-ba3e-034e-6b27-5d271af109ba
     name ( RO): pool-admin
     description ( RO): The Pool Administrator role has full access to
        all
     features and settings, including accessing Dom0 and managing
        subjects,
     roles and external authentication

     uuid ( RO): b9ce9791-0604-50cd-0649-09b3284c7dfd
     name ( RO): pool-operator
     description ( RO): The Pool Operator role manages host-  and pool-
        wide resources,
     including setting up storage, creating resource pools and managing
        patches, and
     high availability (HA).

     uuid( RO): 7955168d-7bec-10ed-105f-c6a7e6e63249
     name ( RO): vm-power-admin
     description ( RO): The VM Power Administrator role has full access
        to VM and
     template management and can choose where to start VMs and use the
        dynamic memory
     control and VM snapshot features

     uuid ( RO): aaa00ab5-7340-bfbc-0d1b-7cf342639a6e
     name ( RO): vm-admin
     description ( RO):  The VM Administrator role can manage VMs and
        templates

     uuid ( RO): fb8d4ff9-310c-a959-0613-54101535d3d5
     name ( RO): vm-operator
     description ( RO):  The VM Operator role can use VMs and interact
        with VM consoles

     uuid ( RO): 7233b8e3-eacb-d7da-2c95-f2e581cdbf4e
     name ( RO): read-only
     description ( RO): The Read-Only role can log in with basic read-
        only access
<!--NeedCopy-->
```

> **Nota:**
>
> Esta lista de funciones es estática. No puede agregar, eliminar ni modificar roles.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para mostrar una lista de temas actuales

Ejecute este comando:

```
xe subject-list
<!--NeedCopy-->
```

Este comando devuelve una lista de los usuarios de XenServer, su uuid y las funciones a las que están asociados:

```
    uuid ( RO): bb6dd239-1fa9-a06b-a497-3be28b8dca44
    subject-identifier ( RO): S
       -1-5-21-1539997073-1618981536-2562117463-2244
    other-config (MRO): subject-name: example01\user_vm_admin; subject-
       upn: \
      user_vm_admin@XENDT.NET; subject-uid: 1823475908; subject-gid:
         1823474177; \
      subject-sid: S-1-5-21-1539997073-1618981536-2562117463-2244;
         subject-gecos: \
      user_vm_admin; subject-displayname: user_vm_admin; subject-is-
         group: false; \
      subject-account-disabled: false; subject-account-expired: false;
         \
      subject-account-locked: false;subject-password-expired: false
    roles (SRO): vm-admin

    uuid ( RO): 4fe89a50-6a1a-d9dd-afb9-b554cd00c01a
    subject-identifier ( RO): S
       -1-5-21-1539997073-1618981536-2562117463-2245
    other-config (MRO): subject-name: example02\user_vm_op; subject-upn
       : \
      user_vm_op@XENDT.NET; subject-uid: 1823475909; subject-gid:
         1823474177; \
      subject-sid: S-1-5-21-1539997073-1618981536-2562117463-2245; \
      subject-gecos: user_vm_op; subject-displayname: user_vm_op; \
      subject-is-group: false; subject-account-disabled: false; \
      subject-account-expired: false; subject-account-locked: \
      false; subject-password-expired: false
    roles (SRO): vm-operator

    uuid ( RO): 8a63fbf0-9ef4-4fef-b4a5-b42984c27267
    subject-identifier ( RO): S
       -1-5-21-1539997073-1618981536-2562117463-2242
    other-config (MRO): subject-name: example03\user_pool_op; \
      subject-upn: user_pool_op@XENDT.NET; subject-uid: 1823475906; \
      subject-gid: 1823474177; subject-s id:
      S-1-5-21-1539997073-1618981536-2562117463-2242; \
      subject-gecos: user_pool_op; subject-displayname: user_pool_op; \
      subject-is-group: false; subject-account-disabled: false; \
      subject-account-expired: false; subject-account-locked: \
      false; subject-password-expired: false
      roles (SRO): pool-operator
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para agregar un asunto a RBAC

Para permitir que los usuarios de AD existentes usen RBAC, cree una instancia de asunto en XenServer, ya sea directamente para el usuario de AD o para los grupos que la contienen:

Ejecute el siguiente comando para agregar una nueva instancia de asunto:

```
xe subject-add subject-name=AD user/group
<!--NeedCopy-->
```

Para asignar una función de RBAC a un sujeto

Después de agregar un asunto, puede asignarlo a una función de RBAC. Puede hacer referencia a la función por su UUID o nombre:

Ejecute el comando:

```
xe subject-role-add uuid=subject uuid role-uuid=role_uuid
<!--NeedCopy-->
```

O bien:

```
xe subject-role-add uuid=subject uuid role-name=role_name
<!--NeedCopy-->
```

Por ejemplo, el siguiente comando agrega un asunto con el UUID `b9b3d03b-3d10-79d3-8ed7-a782c5ea13b4` a la función de administrador del grupo:

```
xe subject-role-add uuid=b9b3d03b-3d10-79d3-8ed7-a782c5ea13b4 role-name
   =pool-admin
<!--NeedCopy-->
```

Para cambiar la función de RBAC de un sujeto

Para cambiar el rol de un usuario, es necesario quitarlo de su rol existente y agregarlo a un nuevo rol:

Ejecute los comandos siguientes:

```
xe subject-role-remove uuid=subject_uuid role-name=role_name_to_remove
xe subject-role-add uuid=subject_uuid role-name=role_name_to_add
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El usuario debe cerrar sesión y volver a iniciarla para asegurarse de que la nueva función surta efecto. Esto requiere el permiso «Cerrar sesión de conexiones de usuario activas» disponible para el administrador o el operador del grupo.

Si le quitas la función de administrador del grupo a un usuario, considera la posibilidad de cambiar también la contraseña raíz y rotar el secreto del grupo. Para obtener más información, consulte Seguridad de la agrupación.

> **Advertencia:**
>
> Cuando agrega o elimina un asunto de administrador de grupo, todos los hosts del grupo pueden tardar unos segundos en aceptar sesiones ssh asociadas con este tema.

Auditoría

El registro de auditoría de RBAC registra cualquier operación realizada por un usuario que ha iniciado sesión.

- El mensaje registra el ID de asunto y el nombre de usuario asociados a la sesión que invocó la operación.
- Si un sujeto invoca una operación que no está autorizada, se registra la operación.
- También se graba cualquier operación correcta. Si la operación falló, se registrará el código de error.

Comandos CLI de auditoría log xe

El siguiente comando descarga todos los registros disponibles del archivo de auditoría RBAC en el grupo en un archivo. Si el parámetro opcional "desde"está presente, solo descarga los registros de ese punto específico en el tiempo.

```
xe audit-log-get [since=timestamp] filename=output filename
<!--NeedCopy-->
```

Para obtener todos los registros de auditoría del grupo

Ejecute este comando:

```
xe audit-log-get filename=/tmp/auditlog-pool-actions.out
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para obtener registros de auditoría del grupo desde una marca de tiempo precisa en milisegundos

Ejecute este comando:

```
xe audit-log-get since=2009-09-24T17:56:20.530Z \
    filename=/tmp/auditlog-pool-actions.out
<!--NeedCopy-->
```

Para obtener registros de auditoría del grupo desde una marca de tiempo precisa por minuto

Ejecute este comando:

```
xe audit-log-get since=2009-09-24T17:56Z \
    filename=/tmp/auditlog-pool-actions.out
<!--NeedCopy-->
```

---

layout: doc
description: Understand the concepts involved in XenServer networking, including networks, VLANs, and NIC bonds.—

Redes

En esta sección se proporciona información general sobre las redes de XenServer, incluidas las redes, las VLAN y los enlaces NIC. También se explica cómo administrar la configuración de red y solucionar problemas.

> **Importante:**
>
> vSwitch es la pila de red predeterminada de XenServer. Siga las instrucciones en redes vSwitch para configurar la pila de redes de Linux.

Si ya está familiarizado con los conceptos de redes de XenServer, puede pasar directamente a Administrar redes para obtener información sobre las siguientes secciones:

- Cree redes para hosts XenServer independientes
- Cree redes para los hosts de XenServer que estén configurados en un grupo de recursos
- Cree VLAN para los hosts de XenServer, independientes o como parte de un grupo de recursos
- Cree vínculos para hosts XenServer independientes

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Cree enlaces para los hosts de XenServer que estén configurados en un grupo de recursos

> **Nota:**
>
> El término “interfaz de administración”se usa para indicar la NIC habilitada para IP que transporta el tráfico de administración. El término “interfaz secundaria”se utiliza para indicar una NIC habilitada para IP configurada para el tráfico de almacenamiento.

Soporte de redes

XenServer admite hasta 16 interfaces de red físicas (o hasta 4 interfaces de red enlazadas) por host y hasta 7 interfaces de red virtuales por máquina virtual.

> **Nota:**
>
> XenServer proporciona una configuración y administración automatizadas de las NIC mediante la interfaz de línea de comandos (CLI) xe. No modifique los archivos de configuración de redes del host directamente.

Redes vSwitch

Las redes vSwitch admiten el flujo abierto.

- Admite directivas de seguridad específicas para controlar el flujo de tráfico enviado hacia y desde una VM.
- Proporciona visibilidad detallada sobre el comportamiento y el rendimiento de todo el tráfico enviado en el entorno de red virtual.

Un vSwitch simplifica en gran medida la administración de TI en entornos de redes virtualizados. Toda la configuración y las estadísticas de VM permanecen vinculadas a la VM incluso cuando la VM migra de un host físico del grupo de recursos a otro.

Para determinar qué pila de redes está configurada, ejecute el siguiente comando:

```
xe host-list params=software-version
<!--NeedCopy-->
```

En el resultado del comando, busque `network_backend`. Cuando vSwitch se configura como la pila de red, la salida aparece de la siguiente manera:

```
network_backend: openvswitch
<!--NeedCopy-->
```

Cuando el puente de Linux se configura como la pila de red, la salida aparece de la siguiente manera:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
network_backend: bridge
<!--NeedCopy-->
```

Para volver a la pila de red de Linux, ejecute el siguiente comando:

```
xe-switch-network-backend bridge
<!--NeedCopy-->
```

Reinicie el host después de ejecutar este comando.

Descripción general de las redes de XenServer

En esta sección se describen los conceptos generales de las redes en el entorno XenServer.

XenServer crea una red para cada NIC física durante la instalación. Al añadir un host a un grupo, se fusionan las redes predeterminadas. Esto es para garantizar que todas las NIC físicas con el mismo nombre de dispositivo estén conectadas a la misma red.

Por lo general, agrega una red para crear una red interna, configurar una nueva VLAN con una NIC existente o crear un enlace NIC.

Puede configurar cuatro tipos diferentes de redes en XenServer:

- **Las redes externas** tienen una asociación con una interfaz de red física. Las redes externas proporcionan un puente entre una máquina virtual y la interfaz de red física conectada a la red. Las redes externas permiten que una máquina virtual se conecte a los recursos disponibles a través de la NIC física del host.
- **Las redes enlazadas** crean un vínculo entre dos o más NIC para crear un canal único y de alto rendimiento entre la máquina virtual y la red.
- **Las redes privadas de un solo servidor** no están asociadas a una interfaz de red física. Las redes privadas de un solo servidor se pueden usar para proporcionar conectividad entre las máquinas virtuales en un host determinado, sin conexión con el mundo exterior.

> **Nota:**
>
> Algunas opciones de red tienen comportamientos diferentes cuando se utilizan con hosts XenServer independientes en comparación con los grupos de recursos. Esta sección contiene secciones sobre información general que se aplica tanto a los hosts como a los grupos independientes, seguidas de información y procedimientos específicos para cada uno.

Objetos de red

En esta sección se utilizan tres tipos de objetos de software del lado del servidor para representar entidades de red. Estos objetos son:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Un *PIF*, que representa una NIC física en un host. Los objetos PIF tienen un nombre y una descripción, un UUID, los parámetros de la NIC que representan y la red y el host a los que están conectados.
- Una *VIF*, que representa una NIC virtual en una máquina virtual. Los objetos VIF tienen un nombre y una descripción, un UUID y la red y la VM a las que están conectados.
- Una *red*, que es un conmutador Ethernet virtual en un host. Los objetos de red tienen un nombre y una descripción, un UUID y la colección de VIF y PIF conectados a ellos.

XenCenter y la CLI xe le permiten configurar las opciones de red. Puede controlar la NIC utilizada para las operaciones de administración y crear funciones de red avanzadas, como VLAN y vínculos NIC.

Redes

Cada host de XenServer tiene una o más redes, que son conmutadores Ethernet virtuales. Las redes que no están asociadas a un PIF se consideran *internas*. Las redes internas se pueden usar para proporcionar conectividad solo entre máquinas virtuales en un host de XenServer determinado, sin conexión con el mundo exterior. Las redes asociadas a un PIF se consideran *externas*. Las redes externas proporcionan un puente entre las VIF y la PIF conectadas a la red, lo que permite la conectividad a los recursos disponibles a través de la NIC de la PIF.

VLAN

Las VLAN, tal como se definen en el estándar IEEE 802.1Q, permiten que una sola red física admita varias redes lógicas. Los hosts XenServer admiten las VLAN de varias maneras.

> **Nota:**
>
> - Recomendamos no usar una SR de GFS2 con una VLAN debido a un problema conocido por el que no se pueden agregar ni quitar hosts en una agrupación en clústeres si la red del clúster está en una VLAN que no es de administración.
> - Todas las configuraciones de VLAN compatibles se aplican por igual a grupos y hosts independientes, y a las configuraciones enlazadas y no enlazadas.

Usar VLAN con máquinas virtuales Los puertos de conmutación configurados como puertos troncales de VLAN 802.1Q se pueden usar con las funciones de VLAN de XenServer para conectar interfaces de red virtuales (VIF) invitadas a VLAN específicas. En este caso, el host de XenServer realiza las funciones de etiquetado y desetiquetado de la VLAN para el huésped, que desconoce ninguna configuración de VLAN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Las VLAN de XenServer se representan mediante objetos PIF adicionales que representan las interfaces de VLAN correspondientes a una etiqueta de VLAN especificada. Puede conectar las redes de XenServer al PIF que representa la NIC física para ver todo el tráfico de la NIC. También puede conectar las redes a un PIF que represente una VLAN para ver solo el tráfico con la etiqueta VLAN especificada. También puede conectar una red de modo que solo vea el tráfico de VLAN nativa, adjuntándolo a la VLAN 0.

Para ver los procedimientos sobre cómo crear VLAN para los hosts de XenServer, ya sean independientes o como parte de un grupo de recursos, consulte Creación de VLAN.

Si quiere que el invitado realice las funciones de etiquetado y desetiquetado de VLAN, el invitado debe conocer las VLAN. Al configurar la red para las máquinas virtuales, configure los puertos del conmutador como puertos troncales de VLAN, pero no cree VLAN para el host de XenServer. En su lugar, use VIF en una red normal que no sea VLAN.

Uso de VLAN con interfaces de administración La interfaz de administración se puede configurar en una VLAN mediante un puerto de switch configurado como puerto troncal o puerto de modo de acceso. Use la CLI de XenCenter o xe para configurar una VLAN y convertirla en la interfaz de administración. Para obtener más información, consulte Interfaz de administración.

Uso de VLAN con NIC de almacenamiento dedicadas Las NIC de almacenamiento dedicadas se pueden configurar para que usen puertos de modo de acceso o VLAN nativos como se describe en la sección anterior para las interfaces de administración. Las NIC de almacenamiento dedicadas también se conocen como NIC habilitadas para IP o interfaces secundarias. Puede configurar las NIC de almacenamiento dedicadas para que usen puertos troncales y VLAN de XenServer, como se describe en la sección anterior para máquinas virtuales. Para obtener más información, consulte Configuración de una NIC de almacenamiento dedicada.

Combinación de interfaces de administración y VLAN invitadas en una NIC de host único Se puede configurar un solo puerto de conmutador con VLAN troncales y nativas, lo que permite utilizar una NIC de host para una interfaz de administración (en la VLAN nativa) y para conectar VIF invitados a identificadores de VLAN específicos.

Marcos Jumbo

Las tramas gigantes se pueden usar para optimizar el rendimiento del tráfico en redes de almacenamiento y redes de VM. Las tramas gigantes son tramas Ethernet que contienen más de 1500 bytes de carga útil. Los marcos Jumbo se utilizan normalmente para lograr un mejor rendimiento, reducir la carga en la memoria del bus del sistema y reducir la sobrecarga de la CPU.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> XenServer admite marcos gigantes solo cuando se usa vSwitch como pila de red en todos los hosts del grupo.

Requisitos para el uso de tramas gigantes Tenga en cuenta lo siguiente cuando utilice tramas gigantes:

- Las tramas gigantes se configuran a nivel de grupo
- vSwitch debe configurarse como back-end de red en todos los hosts del grupo
- Todos los dispositivos de la subred deben configurarse para usar tramas gigantes.
- No se admite la habilitación de tramas gigantes en la red de administración

Para usar tramas gigantes, establezca la Unidad de transmisión máxima (MTU) en un valor entre 1500 y 9216. Puede usar XenCenter o la CLI xe para establecer la MTU.

Vínculos NIC

Los bonos NIC, también conocidos como formación de equipos de NIC, mejoran la resiliencia y el ancho de banda del host XenServer al permitir a los administradores configurar dos o más NIC juntas. Los enlaces NIC funcionan lógicamente como una tarjeta de red y todas las NIC enlazadas comparten una dirección MAC.

Si falla una NIC del enlace, el tráfico de red del host se redirige automáticamente a través de la segunda NIC. XenServer admite hasta ocho redes enlazadas.

XenServer admite los modos de unión activo-activo, activo-pasivo y LACP. La cantidad de NIC admitidas y el modo de enlace admitido varían según la pila de red:

- La vinculación LACP solo está disponible para el vSwitch, mientras que el enlace activo-activo y el activo-pasivo están disponibles tanto para el vSwitch como para el puente Linux.
- Cuando vSwitch es la pila de red, puede unir dos, tres o cuatro NIC.
- Cuando el puente de Linux es la pila de red, solo puede unir dos NIC.

Todos los modos de enlace admiten la conmutación por error. Sin embargo, no todos los modos permiten que todos los enlaces estén activos para todos los tipos de tráfico. XenServer admite la unión de los siguientes tipos de NIC:

- **NIC (no de administración)**. Puede vincular las NIC que XenServer utiliza únicamente para el tráfico de máquinas virtuales. La vinculación de estas NIC no solo proporciona resiliencia, sino que también equilibra el tráfico de varias máquinas virtuales entre las NIC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Interfaces de administración**. Puede vincular una interfaz de administración a otra NIC para que la segunda NIC proporcione conmutación por error para el tráfico de administración. Si bien la configuración de un enlace de agregación de enlaces LACP proporciona un equilibrio de carga para el tráfico de administración, el enlace NIC activo-activo no lo hace. Puede crear una VLAN en las NIC enlazadas y la interfaz de administración del host se puede asignar a esa VLAN.
- **Interfaces secundarias**. Puede unir NIC que haya configurado como interfaces secundarias (por ejemplo, para almacenamiento). Sin embargo, para la mayoría del almacenamiento de iniciadores de software iSCSI, recomendamos configurar las rutas múltiples en lugar de la unión de NIC, como se describe en Diseño de configuraciones de red de XenServer.

  A lo largo de esta sección, el término tráfico de almacenamiento basado en IP se utiliza para describir el tráfico iSCSI y NFS de forma colectiva.

Puede crear un enlace si una VIF ya está utilizando una de las interfaces que se unirán: el tráfico de VM migra automáticamente a la nueva interfaz enlazada.

En XenServer, un PIF adicional representa un bono NIC. Los enlaces NIC de XenServer incluyen por completo los dispositivos físicos subyacentes (PIF).

> **Notas:**
>
> - No se admite la creación de un enlace que contenga solo una NIC.
> - Las NIC unidas pueden ser modelos diferentes entre sí.
> - Los vínculos NIC no se admiten en NIC que transportan tráfico FCoE.

Prácticas recomendadas

Siga estas prácticas recomendadas al configurar sus bonos de NIC:

- Conecte los enlaces del enlace a diferentes conmutadores de red físicos, no solo a los puertos del mismo conmutador.
- Asegúrese de que los conmutadores independientes obtengan energía de unidades de distribución de energía (PDU) diferentes e independientes.
- Si es posible, en su centro de datos, coloque las PDU en diferentes fases de la alimentación o incluso en las fuentes proporcionadas por diferentes empresas de servicios públicos.
- Considere la posibilidad de utilizar unidades de alimentación ininterrumpida para garantizar que los conmutadores y los hosts de la red puedan seguir funcionando o realizar un apagado ordenado en caso de un corte de energía.

Estas medidas aumentan la resiliencia frente a las fallas de software, hardware o alimentación que pueden afectar a los conmutadores de red.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puntos clave sobre el direccionamiento IP

Las NIC enlazadas tienen una dirección IP o ninguna dirección IP, de la siguiente manera:

- **Redes de administración y almacenamiento**.
  - Si vincula una interfaz de administración o una interfaz secundaria, se asigna una sola dirección IP al vínculo. Es decir, cada NIC no tiene su propia dirección IP. XenServer trata las dos NIC como una conexión lógica.
  - Cuando los vínculos se utilizan para el tráfico que no es de VM, por ejemplo, para conectarse al almacenamiento de red compartido o a XenCenter para la administración, configure una dirección IP para el enlace. Sin embargo, si ya asignó una dirección IP a una de las NIC (es decir, creó una interfaz de administración o una interfaz secundaria), esa dirección IP se asigna a todo el enlace automáticamente.
  - Si vincula una interfaz de administración o una interfaz secundaria a una NIC sin una dirección IP, el enlace asume la dirección IP de la interfaz respectiva.
  - Si une una interfaz de administración de VLAN etiquetada y una interfaz secundaria, la VLAN de administración se crea en esa NIC enlazada.
- **Redes de máquinas virtuales**. Cuando se utilizan NIC enlazadas para el tráfico de VM, no es necesario configurar una dirección IP para el enlace. Esto se debe a que el enlace opera en la capa 2 del modelo OSI, la capa de enlace de datos, y no se utiliza ninguna dirección IP en esta capa. Las direcciones IP de las máquinas virtuales se asocian a las VIF.

Tipos de unión

XenServer ofrece tres tipos diferentes de enlaces, todos los cuales se pueden configurar mediante la CLI o XenCenter:

- Modo activo-activo, con tráfico de VM equilibrado entre las NIC conectadas. Consulte Enlace activo-activo.
- Modo activo-pasivo, donde solo una NIC transporta tráfico de forma activa. Consulte Enlace activo-pasivo.
- Agregación de enlaces LACP, en la que las NIC activas y en espera se negocian entre el conmutador y el host. Consulte Enlace del protocolo de control de agregación de enlaces LACP.

> **Nota:**
>
> La unión se configura con un retardo de subida de 31.000 ms y un retardo de bajada de 200 ms. La demora de subida aparentemente larga es deliberada debido al tiempo que tardan algunos conmutadores en habilitar el puerto. Sin demora, cuando un enlace regresa después de fallar, el

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> vínculo puede reequilibrar el tráfico hacia él antes de que el switch esté listo para pasar el tráfico. Para mover ambas conexiones a un conmutador diferente, mueva uno y espere 31 segundos a que se vuelva a utilizar antes de mover el otro. Para obtener información sobre cómo cambiar la demora, consulte Cambiar la demora de los vínculos.

Situación de los vínculos

XenServer proporciona el estado de los bonos en los registros de eventos de cada host. Si uno o más enlaces de un enlace fallan o se restauran, se anotan en el registro de eventos. Del mismo modo, puede consultar el estado de los vínculos de un vínculo mediante el parámetro `links-up` como se muestra en el siguiente ejemplo:

```
xe bond-param-get uuid=bond_uuid param-name=links-up
<!--NeedCopy-->
```

XenServer comprueba el estado de los enlaces en los bonos aproximadamente cada cinco segundos. Por lo tanto, si fallan más enlaces en el vínculo en la ventana de cinco segundos, el fallo no se registra hasta la siguiente verificación de estado.

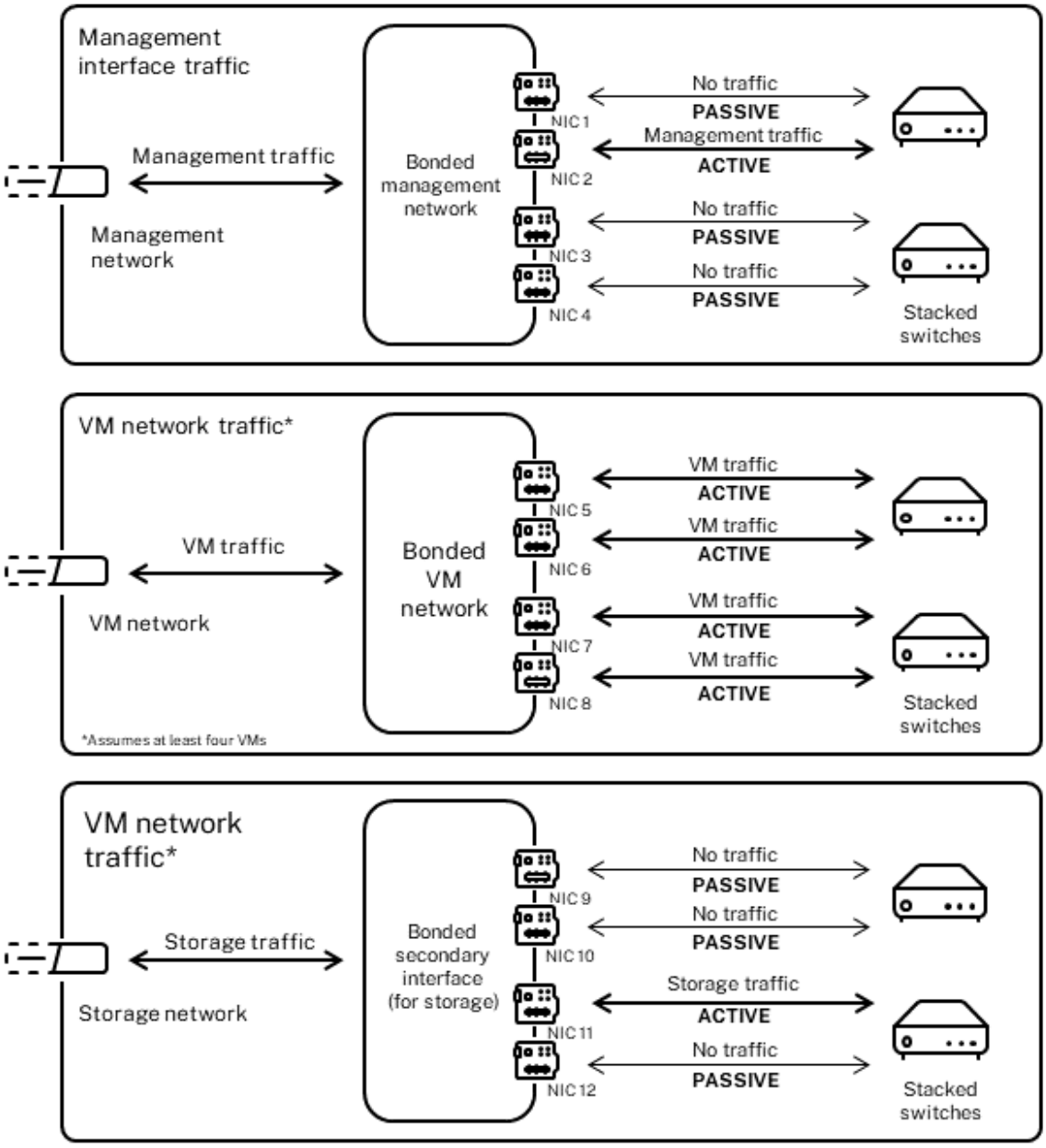
Los registros de eventos de vinculación aparecen en la ficha Registros de XenCenter. Para los usuarios que no ejecutan XenCenter, los registros de eventos también aparecen en `/var/log/xensource.log` en cada host.

Enlace activo-activo

Activo-activo es una configuración activa/activa para el tráfico de invitados: ambas NIC pueden redirigir el tráfico de VM simultáneamente. Cuando los vínculos se utilizan para el tráfico de administración, solo una NIC en el enlace puede redirigir el tráfico: la otra NIC permanece sin usar y ofrece la conmutación por error. El modo activo-activo es el modo de enlace predeterminado cuando el puente de Linux o la pila de red vSwitch están habilitados.

Cuando se utiliza el enlace activo-activo con el puente de Linux, solo se pueden unir dos NIC. Al utilizar vSwitch como pila de red, puede unir dos, tres o cuatro NIC en modo activo-activo. Sin embargo, en el modo activo-activo, unir tres o cuatro NIC solo es beneficioso para el tráfico de VM, como se muestra en la siguiente ilustración.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Active-active bonds (vSwitch network stack)

XenServer solo puede enviar tráfico a través de dos o más NIC cuando hay más de una dirección MAC asociada al enlace. XenServer puede usar las direcciones MAC virtuales del VIF para enviar tráfico a través de varios enlaces. En concreto:

- **Tráfico de VM**. Siempre que habilite la vinculación en las NIC que transportan solo tráfico de VM (invitado), todos los enlaces están activos y la unión de NIC puede equilibrar el tráfico de VM distribuido en las NIC. El tráfico de una VIF individual nunca se divide entre NIC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Tráfico de administración o almacenamiento**. Solo uno de los enlaces (NIC) del enlace está activo y las demás NIC permanecen sin usar a menos que el tráfico se conmute por error. La configuración de una interfaz de administración o una interfaz secundaria en una red conectada proporciona resiliencia.
- **Tráfico mixto**. Si la NIC enlazada lleva una mezcla de tráfico de almacenamiento basado en IP y tráfico de invitados, solo se equilibra la carga del tráfico de dominio de invitado y de control. El dominio de control es esencialmente una máquina virtual, por lo que utiliza una NIC como los demás huéspedes. XenServer equilibra el tráfico del dominio de control de la misma manera que equilibra el tráfico de máquinas virtuales.

Balance de tráfico XenServer equilibra el tráfico entre las NIC mediante la dirección MAC de origen del paquete. Como para el tráfico de administración, solo hay una dirección MAC de origen, el modo activo-activo solo puede usar una NIC y el tráfico no está equilibrado. El equilibrio del tráfico se basa en dos factores:

- La máquina virtual y su VIF asociada envían o reciben el tráfico
- La cantidad de datos (en kilobytes) que se envían.

XenServer evalúa la cantidad de datos (en kilobytes) que envía y recibe cada NIC. Si la cantidad de datos enviados a través de una NIC supera la cantidad de datos enviados a través de la otra NIC, XenServer reequilibra qué VIF utilizan qué NIC. Se transfiere toda la carga del VIF. La carga de una VIF nunca se divide entre dos NIC.

Si bien la vinculación NIC activa-activa puede proporcionar equilibrio de carga para el tráfico de varias VM, no puede proporcionar a una sola VM el rendimiento de dos NIC. Cualquier VIF dado solo usa uno de los enlaces de un vínculo a la vez. Como XenServer reequilibra el tráfico periódicamente, las VIF no se asignan permanentemente a una NIC específica del bono.

El modo activo-activo a veces se describe como enlace de equilibrio de carga de origen (SLB), ya que XenServer usa SLB para compartir la carga entre las interfaces de red enlazadas. SLB se deriva del modo de equilibrio de carga adaptable (ALB) de código abierto y reutiliza la funcionalidad de ALB para reequilibrar la carga en las NIC de forma dinámica.

Cuando se reequilibra, se realiza un seguimiento del número de bytes que pasan por cada secundario (interfaz) durante un período determinado. Si un paquete que se va a enviar contiene una nueva dirección MAC de origen, se asigna a la interfaz secundaria con la menor utilización. El tráfico se reequilibra a intervalos regulares.

Cada dirección MAC tiene una carga correspondiente y XenServer puede desplazar cargas enteras entre NIC en función de la cantidad de datos que envíe y reciba una máquina virtual. Para el tráfico activo-activo, todo el tráfico de una máquina virtual se puede enviar en una sola NIC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

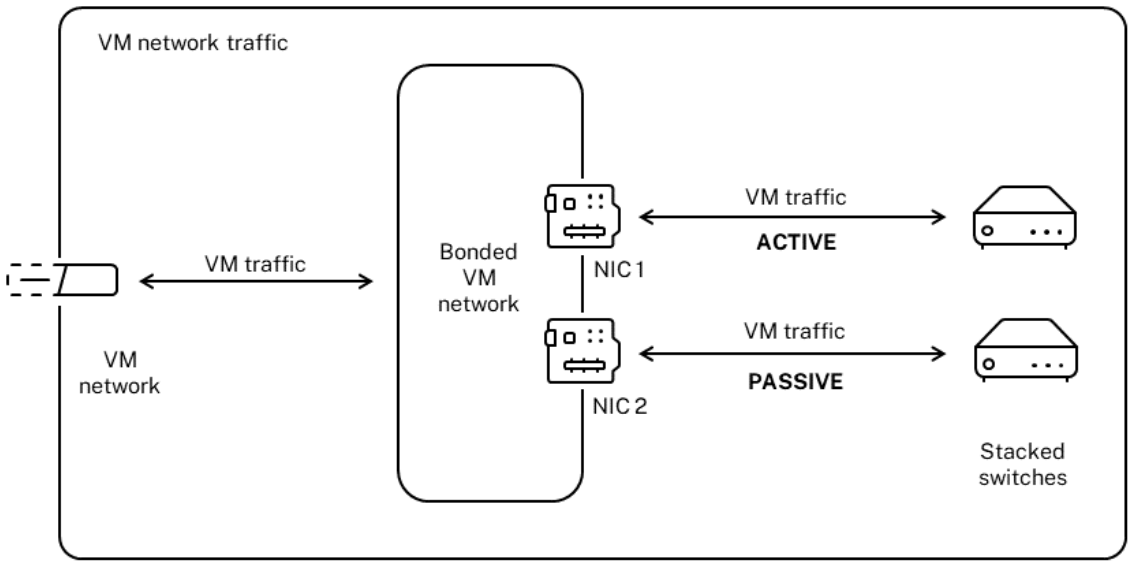
> **Nota:**
>
> El enlace activo-activo no requiere soporte de conmutador para EtherChannel o 802.3ad (LACP).

Enlace activo-pasivo

Un enlace activo-pasivo redirige el tráfico solo a través de una de las NIC. Si la NIC activa pierde la conectividad de red, el tráfico conmuta por error a la otra NIC del enlace. Los enlaces activo-pasivo redirigen el tráfico a través de la NIC activa. El tráfico cambia a la NIC pasiva si falla la NIC activa.

El enlace activo-pasivo está disponible en el puente de Linux y en la pila de red vSwitch. Cuando se usa con el puente de Linux, puede unir dos NIC juntas. Cuando se usa con vSwitch, solo puede unir dos, tres o cuatro NIC juntas. Sin embargo, independientemente del tipo de tráfico, cuando vincula NIC en modo activo-pasivo, solo un enlace está activo y no hay equilibrio de carga entre los enlaces.

La siguiente ilustración muestra dos NIC conectadas configuradas en modo activo-pasivo.



Active-passive bond

El modo activo-activo es la configuración de enlace predeterminada en XenServer. Si configura enlaces mediante la CLI, debe especificar un parámetro para el modo activo-pasivo. De lo contrario, se crea un enlace activo-activo. No necesita configurar el modo activo-pasivo porque una red transporta tráfico de administración o tráfico de almacenamiento.

Activo-pasivo puede ser una buena opción para la resiliencia, ya que ofrece varios beneficios. Con los vínculos activo-pasivo, el tráfico no se mueve entre las NIC. Del mismo modo, la vinculación activa-pasiva le permite configurar dos conmutadores para redundancia, pero no requiere apilamiento. Si

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

el conmutador de administración muere, los conmutadores apilados pueden ser un punto único de falla.

El modo activo-pasivo no requiere soporte de conmutador para EtherChannel o 802.3ad (LACP).

Considere la posibilidad de configurar el modo activo-pasivo en situaciones en las que no necesite equilibrio de carga o cuando solo pretenda enviar tráfico en una NIC.

> **Importante:**
>
> Después de crear VIF o de que su agruación esté en producción, tenga cuidado al cambiar los vínculos o crear vínculos.

Enlace del protocolo de control de agregación de enlaces LACP

El protocolo de control de agregación de enlaces LACP es un tipo de enlace que agrupa un grupo de puertos y lo trata como un único canal lógico. La vinculación LACP proporciona conmutación por error y puede aumentar la cantidad total de ancho de banda disponible.

A diferencia de otros modos de vinculación, la vinculación LACP requiere configurar ambos lados de los enlaces: Crear un enlace en el host y crear un grupo de agregación de enlaces (LAG) para cada enlace en el switch. Consulte Configuración del switch para los vínculos LACP. Debe configurar el vSwitch como la pila de red para usar la vinculación LACP. Además, los conmutadores deben admitir el estándar IEEE 802.3ad.

Una comparación de la unión SLB activa-activa y la unión LACP:

Enlace SLB activo-activo Ventajas:

- Se puede usar con cualquier interruptor de la lista de compatibilidad de hardware.
- No requiere interruptores que admitan apilamiento.
- Admite cuatro NIC.

Consideraciones:

- El equilibrio de carga óptimo requiere al menos una NIC por VIF.
- El tráfico de almacenamiento o administración no se puede dividir en varias NIC.
- El equilibrio de carga solo se produce si hay varias direcciones MAC presentes.

Adhesión LACP Ventajas:

- Todos los enlaces pueden estar activos independientemente del tipo de tráfico.
- El equilibrio del tráfico no depende de las direcciones MAC de origen, por lo que se pueden equilibrar todos los tipos de tráfico.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Consideraciones:

- Los conmutadores deben admitir el estándar IEEE 802.3ad.
- Requiere configuración en el lado del conmutador.
- Solo se admite para vSwitch.
- Requiere un interruptor único o un interruptor apilado.

Balance de tráfico XenServer admite dos tipos de hash de unión LACP. El término hash describe cómo las NIC y el conmutador distribuyen el tráfico: (1) el equilibrio de carga en función de la IP y el puerto de las direcciones de origen y destino y (2) el equilibrio de carga en función de la dirección MAC de origen.

Según el tipo de hash y el patrón de tráfico, la vinculación LACP puede distribuir el tráfico de manera más uniforme que la unión NIC activa-activa.

> **Nota:**
>
> Configure los ajustes para el tráfico saliente y entrante por separado en el host y el conmutador: la configuración no tiene que coincidir en ambos lados.

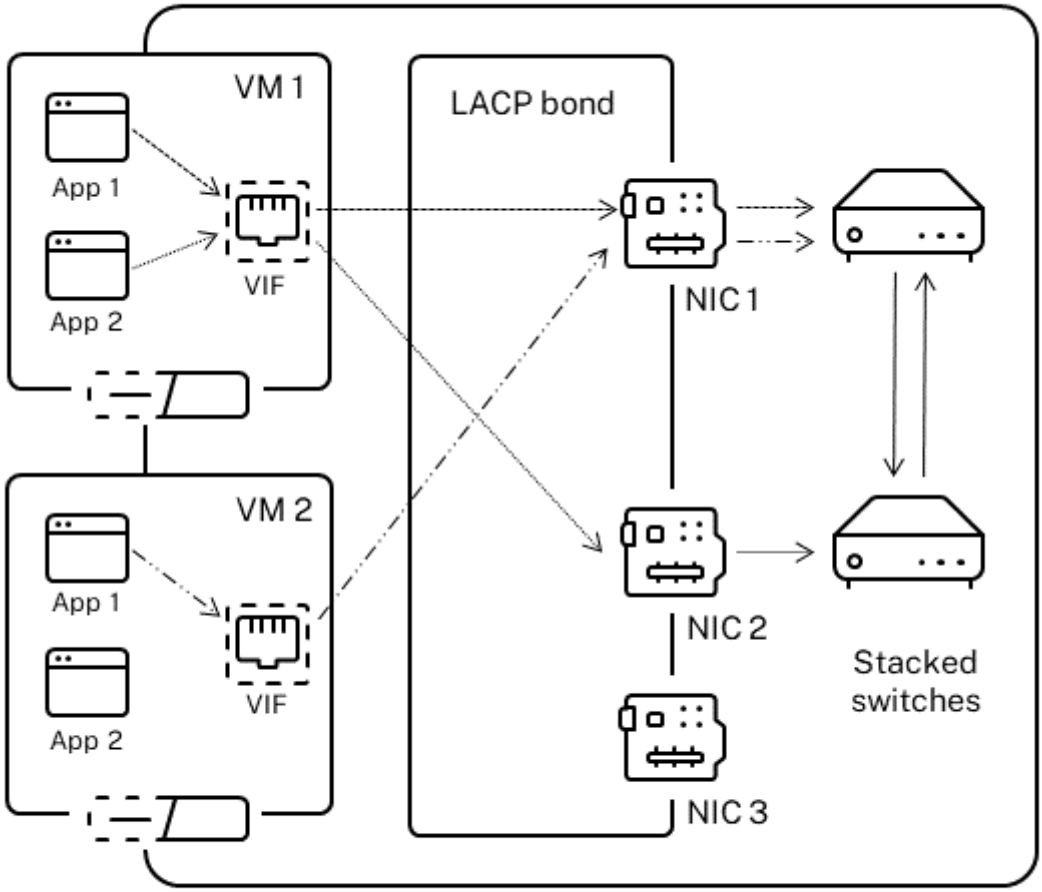
Equilibrio de carga basado en IP y puerto de direcciones de origen y destino.

Este tipo de hash es el algoritmo de hash de enlace LACP predeterminado. Si hay una variación en los números de puerto o IP de origen o destino, el tráfico de un invitado se puede distribuir en dos enlaces.

Si una máquina virtual ejecuta varias aplicaciones que utilizan diferentes direcciones IP o números de puerto, este tipo de hash distribuye el tráfico a través de varios enlaces. La distribución del tráfico ofrece al huésped la posibilidad de utilizar el rendimiento agregado. Este tipo de hash permite que un invitado utilice todo el rendimiento de varias NIC.

Como se muestra en la siguiente ilustración, este tipo de hash puede distribuir el tráfico de dos aplicaciones diferentes en una máquina virtual a dos NIC diferentes.

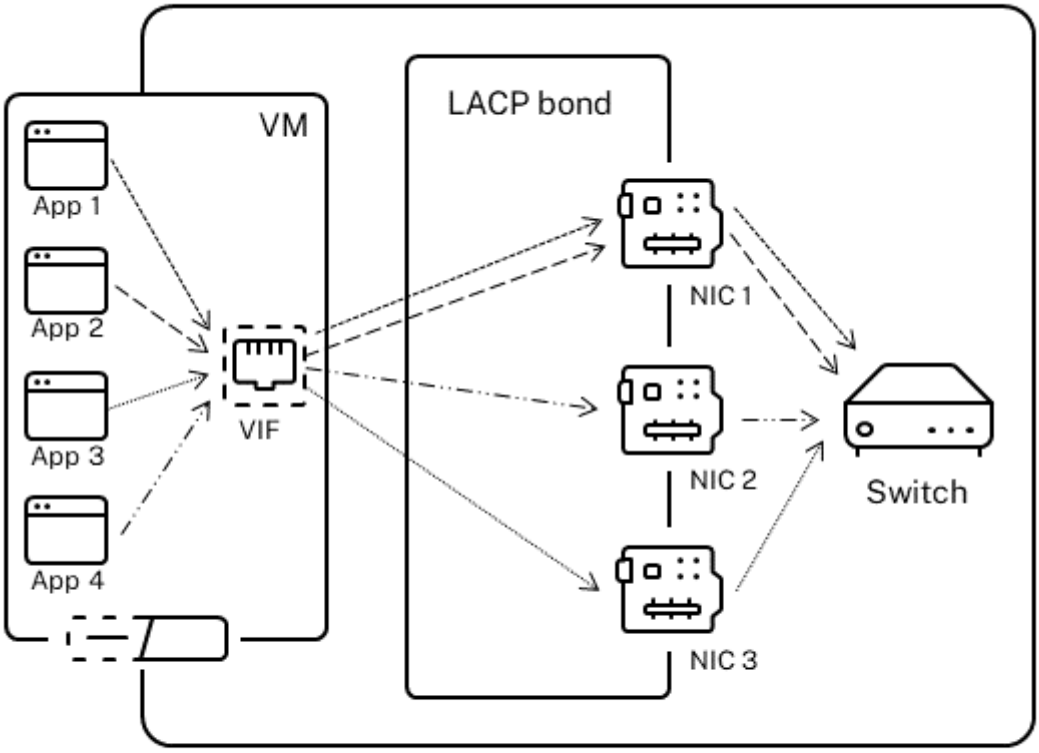
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Load balancing based on IP and port of source and destination addresses

La configuración de la vinculación LACP en función de la IP y el puerto de la dirección de origen y destino es beneficiosa cuando se quiere equilibrar el tráfico de dos aplicaciones diferentes en la misma VM. Por ejemplo, cuando solo se configura una máquina virtual para usar un enlace de tres NIC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



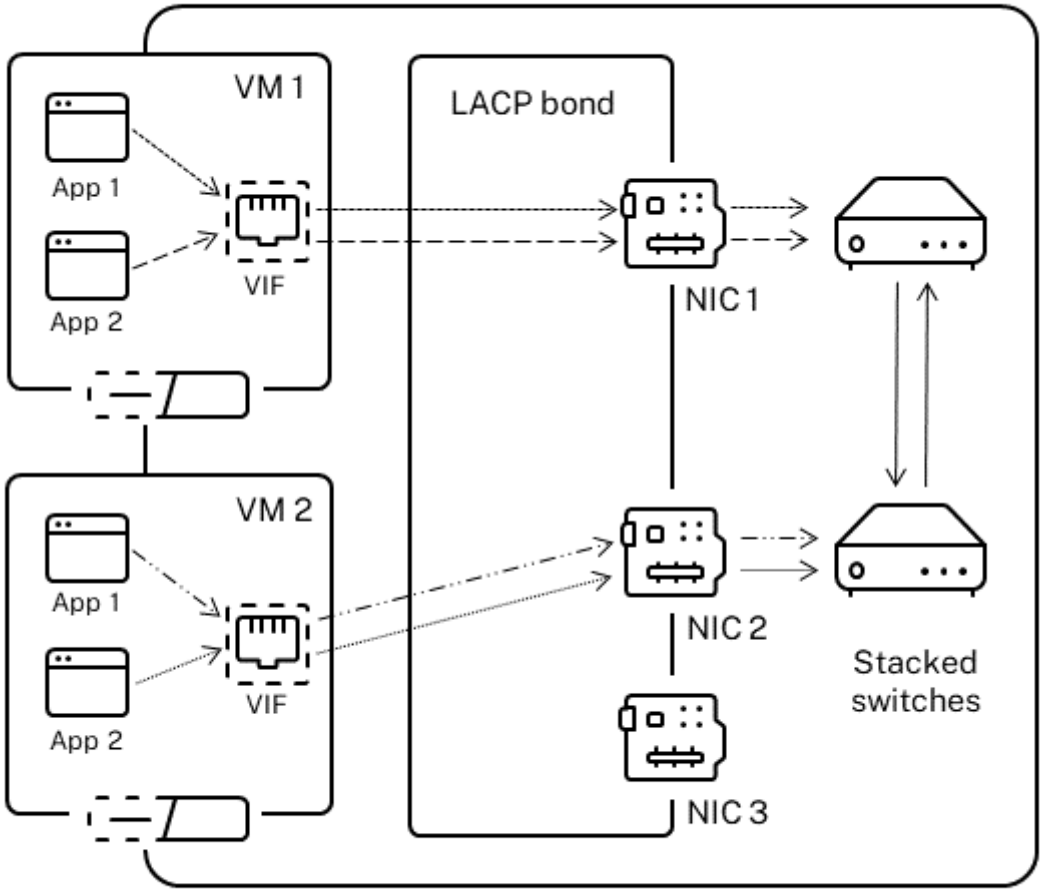
Load balancing based on IP and port of source and destination addresses

El algoritmo de equilibrio para este tipo de hash utiliza cinco factores para distribuir el tráfico en las NIC: la dirección IP de origen, el número de puerto de origen, la dirección IP de destino, el número de puerto de destino y la dirección MAC de origen.

Equilibrio de carga según la dirección MAC de origen.

Este tipo de equilibrio de carga funciona bien cuando hay varias máquinas virtuales en el mismo host. El tráfico se equilibra en función de la dirección MAC virtual de la máquina virtual desde la que se originó el tráfico. XenServer envía el tráfico saliente mediante el mismo algoritmo que en la vinculación activo-activo. El tráfico procedente del mismo huésped no se divide en varias NIC. Como resultado, este tipo de hash no es adecuado si hay menos VIF que NIC: el equilibrio de carga no es óptimo porque el tráfico no se puede dividir entre NIC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Load balancing based on source MAC address

Configuración del conmutador

Según sus requisitos de redundancia, puede conectar las NIC en el enlace a los mismos conmutadores apilados o a conmutadores apilados separados. Si conecta una de las NIC a un segundo conmutador redundante y falla una NIC o un conmutador, el tráfico se conmuta por error a la otra NIC. La adición de un segundo conmutador evita un único punto de falla en su configuración de las siguientes maneras:

- Cuando conecta uno de los enlaces en una interfaz de administración conectada a un segundo conmutador, si el conmutador falla, la red de administración permanece en línea y los hosts pueden seguir comunicándose entre sí.
- Si conecta un enlace (para cualquier tipo de tráfico) a un segundo conmutador y se produce un error en la NIC o el conmutador, las máquinas virtuales permanecen en la red mientras su tráfico conmuta por error a la otra NIC o conmutador.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Utilice conmutadores apilados cuando quiera conectar NIC conectadas a varios conmutadores y haya configurado el modo de enlace LACP. El término "conmutadores apilados"se utiliza para describir la configuración de varios conmutadores físicos para que funcionen como un único conmutador lógico. Debe unir los conmutadores físicamente y a través del software de administración de conmutadores para que los conmutadores funcionen como una única unidad de conmutación lógica, según las directrices del fabricante del conmutador. Por lo general, el apilamiento de conmutadores solo está disponible a través de extensiones propietarias y los proveedores de conmutadores pueden comercializar esta funcionalidad en términos diferentes

> **Nota:**
>
> Si tiene problemas con los vínculos activos-activos, puede ser necesario el uso de interruptores apilados. Los enlaces activo-pasivo no requieren interruptores apilados.

Configuración de switch para vínculos LACP Debido a que los detalles específicos de la configuración del switch varían según el fabricante, hay algunos puntos clave que se deben recordar al configurar los switches para su uso con enlaces LACP:

- El conmutador debe admitir LACP y el estándar IEEE 802.3ad.
- Al crear el grupo LAG en el conmutador, debe crear un grupo LAG para cada enlace LACP en el host. Por ejemplo, si tiene un grupo de cinco hosts y creó un enlace LACP en las NIC 4 y 5 de cada host, debe crear cinco grupos de LAG en el conmutador. Un grupo para cada conjunto de puertos correspondientes a las NIC del host.

  Es posible que también deba agregar su ID de VLAN a su grupo LAG.
- Los enlaces LACP de XenServer requieren establecer el parámetro de modo estático en el grupo LAG en inhabilitado.

Como se mencionó anteriormente en *Configuración de conmutadores*, se requieren conmutadores de apilamiento para conectar enlaces LACP a varios conmutadores.

Configuración de red inicial después de la instalación

La configuración de red del host de XenServer se especifica durante la instalación inicial del host. Las opciones como la configuración de la dirección IP (DHCP/estática), la NIC utilizada como interfaz de administración y el nombre del host se configuran en función de los valores proporcionados durante la instalación.

Cuando un host tiene varias NIC, la configuración presente después de la instalación depende de la NIC que se seleccione para las operaciones de administración durante la instalación:

- Los PIF se crean para cada NIC en el host

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- El PIF de la NIC seleccionada para su uso como interfaz de administración se configura con las opciones de direccionamiento IP especificadas durante la instalación.
- Se crea una red para cada PIF (“red 0”, “red 1”, etc.)
- Cada red está conectada a un PIF
- Las opciones de direccionamiento IP se dejan sin configurar para todos los PIF que no sean el PIF utilizado como interfaz de administración.

Cuando un host tiene una sola NIC, se presenta la siguiente configuración después de la instalación:

- Se crea un único PIF correspondiente a la NIC única del host
- El PIF se configura con las opciones de direccionamiento IP especificadas durante la instalación y para permitir la administración del host
- El PIF está configurado para su uso en operaciones de administración de host
- Se crea una sola red, red 0
- La red 0 está conectada al PIF para permitir la conectividad externa a las VM

Cuando se realiza una instalación de XenServer en una red VLAN etiquetada, se presenta la siguiente configuración después de la instalación:

- Los PIF se crean para cada NIC en el host
- El PIF de la VLAN etiquetada en la NIC seleccionada para su uso como interfaz de administración se configura con la configuración de dirección IP especificada durante la instalación.
- Se crea una red para cada PIF (por ejemplo: red 1, red 2, etc.). Se crea una red VLAN adicional (por ejemplo, para la red de todo el grupo asociada con eth0 en VLAN<TAG>)
- Cada red está conectada a un PIF. El PIF de VLAN está configurado para su uso en operaciones de administración de hosts

En ambos casos, la configuración de red resultante permite la conexión al host de XenServer mediante XenCenter, la CLI xe y cualquier otro software de administración que se ejecute en máquinas independientes a través de la dirección IP de la interfaz de administración. La configuración también proporciona redes externas para las máquinas virtuales creadas en el host.

El PIF utilizado para las operaciones de administración es el único PIF que se ha configurado con una dirección IP durante la instalación de XenServer. La red externa para las VM se logra mediante la conexión de PIF a VIF mediante el objeto de red que actúa como un conmutador Ethernet virtual.

Los pasos necesarios para las funciones de red, como VLAN, vínculos NIC y la dedicación de una NIC al tráfico de almacenamiento de información, se describen en las secciones siguientes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cambiar la configuración de redes

Puede cambiar la configuración de red modificando el objeto de red. Para hacerlo, ejecute un comando que afecte al objeto de red o al VIF.

Modificación del objeto de red

Puede cambiar aspectos de una red, como el tamaño de trama (MTU), la etiqueta de nombre, la descripción del nombre, el propósito y otros valores. Ejecute el comando `network-param-set` xe y sus parámetros asociados para cambiar los valores.

Al ejecutar el comando xe `network-param-set`, el único parámetro obligatorio es `uuid`.

Los parámetros opcionales incluyen:

- `default_locking_mode`. Consulte Simplificación de la configuración del modo de bloqueo de VIF en la nube.
- `name-label`
- `name-description`
- `MTU`
- `purpose`. Consulte Adición de un propósito a una red.
- `other-config`

Si no se da un valor para un parámetro, el parámetro se establece en un valor nulo. Para establecer un par (clave, valor) en un parámetro de mapa, use la sintaxis `map-param:key=value`.

Cambiar la demora de los vínculos

La vinculación se configura con una demora de activación de 31 000 ms de forma predeterminada para evitar que el tráfico se reequilibre en una NIC después de que falla. Aunque aparentemente es largo, el retardo de subida es importante para todos los modos de unión y no solo para activo-activo.

Sin embargo, si comprende la configuración adecuada para seleccionar para su entorno, puede cambiar la demora de los vínculos mediante el procedimiento que se indica a continuación.

Configure la demora en milisegundos:

```
1 xe pif-param-set uuid=<uuid of bond interface PIF> other-config:bond-
     updelay=<delay in ms>
2 <!--NeedCopy-->
```

Para que el cambio surta efecto, debe desconectar y volver a conectar la interfaz física:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe pif-unplug uuid=<uuid of bond interface PIF>
<!--NeedCopy-->
```

```
xe pif-plug uuid=<uuid of bond interface PIF>
<!--NeedCopy-->
```

Administrar redes

February 23, 2024

Los procedimientos de configuración de red de esta sección varían en función de si se configura un host independiente o un host que forma parte de un grupo de recursos.

Cree redes en un host independiente

Como las redes externas se crean para cada PIF durante la instalación del host, la creación de redes adicionales normalmente solo se requiere para:

- Use una red privada
- Admite operaciones avanzadas como VLAN o vinculación NIC

Para obtener información sobre cómo agregar o eliminar redes mediante XenCenter, consulte Agregar una nueva red en la documentación de XenCenter.

Abra la consola de texto del host de XenServer.

Cree la red mediante el comando network-create, que devuelve el UUID de la red recién creada:

```
xe network-create name-label=mynetwork
<!--NeedCopy-->
```

En este punto, la red no está conectada a un PIF y, por lo tanto, es interna.

Crear redes en grupos de recursos

Todos los hosts de XenServer de un grupo de recursos deben tener la misma cantidad de NIC físicas. Este requisito no se aplica estrictamente cuando un host se une a un grupo. Una de las NIC siempre se designa como *interfaz de administración*y se utiliza para el tráfico de administración de XenServer.

Como todos los hosts de un grupo comparten un conjunto común de redes. Es importante tener la misma configuración de red física para los hosts de XenServer en un grupo. Los PIF de los hosts individuales se conectan a redes de todo el grupo según el nombre del dispositivo. Por ejemplo, todos

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

los hosts XenServer de un grupo con una NIC eth0 tienen el PIF correspondiente conectado a la red de todo el grupo. `Network 0` Lo mismo ocurre con los hosts con NIC eth1 y `Network 1`otras NIC presentes en al menos un host de XenServer del grupo.

Si un host de XenServer tiene un número de NIC diferente al de los demás hosts del grupo, pueden surgir complicaciones. Las complicaciones pueden surgir porque no todas las redes de grupos son válidas para todos los hosts de grupos. Por ejemplo, si los hosts *host1* y *host2* están en el mismo grupo y *host1* tiene cuatro NIC y *host2* solo tiene dos, solo las redes conectadas a los PIF correspondientes a eth0 y eth1 son válidas en *host2*. Las máquinas virtuales en *host1* con VIF conectadas a redes correspondientes a eth2 y eth3 no pueden migrar al host *host2*.

Creación de VLAN

Para los hosts de un grupo de recursos, puede usar el comando `pool-vlan-create`. Este comando crea la VLAN y crea y conecta automáticamente los PIF requeridos en los hosts del grupo. Para obtener más información, consulte `pool-vlan-create`.

Abra la consola host de XenServer.

Cree una red para usarla con la VLAN. Se devuelve el UUID de la nueva red:

```
xe network-create name-label=network5
<!--NeedCopy-->
```

Utilice el comando `pif-list` para buscar el UUID del PIF correspondiente a la NIC física que admite la etiqueta VLAN deseada. Se devuelven los UUID y los nombres de dispositivos de todos los PIF, incluidas las VLAN existentes:

```
xe pif-list
<!--NeedCopy-->
```

Cree un objeto de VLAN que especifique la etiqueta de VLAN y PIF físicas deseadas en todas las máquinas virtuales que se conectarán a la nueva VLAN. Se crea un nuevo PIF y se conecta a la red especificada. Se devuelve el UUID del nuevo objeto PIF.

```
xe vlan-create network-uuid=network_uuid pif-uuid=pif_uuid vlan=5
<!--NeedCopy-->
```

Conecte VIF de VM a la nueva red. Para obtener más información, consulte Crear redes en un host independiente.

Crear vínculos NIC en un host independiente

Recomendamos usar XenCenter para crear vínculos NIC. Para obtener más información, consulte Configuración de NIC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

En esta sección, se describe cómo usar la CLI xe para vincular las interfaces NIC en los hosts de XenServer que no están en un grupo. Para obtener información sobre el uso de la CLI xe para crear enlaces NIC en los hosts de XenServer que forman un grupo de recursos, consulte *Crear enlaces NIC en grupos de recursos*.

Crear un vínculo NIC

Cuando une una NIC, la unión absorbe la PIF/NIC en uso como interfaz de administración. La interfaz de gestión se traslada automáticamente al PIF de vínculos.

1. Utilice el comando `network-create` para crear una red para usarla con la NIC enlazada. Se devuelve el UUID de la nueva red:

```
xe network-create name-label=bond0
<!--NeedCopy-->
```

2. Utilice el comando `pif-list` para determinar los UUID de los PIF que se utilizarán en el enlace:

```
xe pif-list
<!--NeedCopy-->
```

3. Lleve a cabo una de las siguientes acciones:

   - Para configurar el enlace en modo activo-activo (predeterminado), utilice el comando `bond-create` para crear el enlace. Con comas para separar los parámetros, especifique el UUID de red recién creado y los UUID de los PIF que se van a unir:

```
xe bond-create network-uuid=network_uuid /
     pif-uuids=pif_uuid_1,pif_uuid_2,pif_uuid_3,pif_uuid_4
<!--NeedCopy-->
```

     Escriba dos UUID cuando vincule dos NIC y cuatro UUID cuando vincule cuatro NIC. El UUID del enlace se devuelve después de ejecutar el comando.

   - Para configurar el enlace en modo activo-pasivo o enlace LACP, utilice la misma sintaxis, agregue el parámetro `mode` opcional y especifique `lacp` o `active-backup`:

```
xe bond-create network-uuid=network_uuid pif-uuids=pif_uuid_1
    , /
      pif_uuid_2,pif_uuid_3,pif_uuid_4 /
      mode=balance-slb | active-backup | lacp
<!--NeedCopy-->
```

Controlar la dirección MAC del vínculo

Cuando se une la interfaz de administración, se subsume el PIF/NIC en uso como interfaz de administración. Si el host usa DHCP, la dirección MAC del enlace es la misma que la PIF/NIC en uso. La

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

dirección IP de la interfaz de administración puede permanecer sin cambios.

Puede cambiar la dirección MAC del vínculo para que sea diferente de la dirección MAC de la NIC de la interfaz de administración (actual). Sin embargo, a medida que se habilita el enlace y cambia la dirección MAC/IP en uso, se eliminan las sesiones de red existentes en el host.

Puede controlar la dirección MAC de un vínculo de dos maneras:

- Se puede especificar un parámetro `mac` opcional en el comando `bond-create`. Puede utilizar este parámetro para establecer la dirección MAC de enlace en cualquier dirección arbitraria.
- Si no se especifica el `mac` parámetro, XenServer utiliza la dirección MAC de la interfaz de administración si es una de las interfaces del enlace. Si la interfaz de administración no forma parte del vínculo, pero sí lo es otra interfaz de administración, el vínculo utiliza la dirección MAC (y también la dirección IP) de esa interfaz de administración. Si ninguna de las NIC del vínculo es una interfaz de administración, el vínculo utiliza el MAC de la primera NIC nombrada.

Revertir vínculos NIC

Al revertir el host de XenServer a una configuración no enlazada, `bond-destroy` el comando configura automáticamente la NIC principal como interfaz para la interfaz de administración. Por lo tanto, todas las VIF se trasladan a la interfaz de administración. Si la interfaz de administración de un host está en una interfaz enlazada de VLAN etiquetada, al `bond-destroy`ejecutarla, la VLAN de administración se mueve a la NIC principal.

El término NIC principal se refiere al PIF del que se copió la configuración MAC e IP al crear el vínculo. Al unir dos NIC, la NIC principal es:

1. La NIC de la interfaz de administración (si la interfaz de administración es una de las NIC conectadas).
2. Cualquier otra NIC con una dirección IP (si la interfaz de administración no formaba parte del vínculo).
3. La primera NIC denominada. Puede averiguar cuál es ejecutando lo siguiente:

```
xe bond-list params=all
<!--NeedCopy-->
```

Crear vínculos NIC en grupos de recursos

Siempre que sea posible, cree vínculos de NIC como parte de la creación inicial del grupo de recursos, antes de unir más hosts al grupo o de crear máquinas virtuales. Esto permite que la configuración de enlace se replique automáticamente en los hosts a medida que se unen al grupo y reduce la cantidad de pasos requeridos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Agregar un vínculo NIC a un grupo existente requiere una de las siguientes opciones:

- Uso de la CLI para configurar los vínculos en el coordinador del grupo y, a continuación, en cada miembro del grupo.
- Usar la CLI para configurar enlaces en el coordinador del grupo y, a continuación, reiniciar cada miembro del grupo para que herede su configuración del coordinador del grupo.
- Uso de XenCenter para configurar los enlaces en el coordinador del grupo. XenCenter sincroniza automáticamente la configuración de red de los hosts miembros con el coordinador del grupo, por lo que no es necesario reiniciar los hosts miembros.

Para simplificar y evitar errores de configuración, recomendamos usar XenCenter para crear enlaces NIC. Para obtener más información, consulte Configuración de NIC.

En esta sección, se describe el uso de la CLI xe para crear interfaces NIC enlazadas en los hosts de XenServer que forman un grupo de recursos. Para obtener información sobre el uso de la CLI xe para crear vínculos NIC en un host independiente, consulte *Creación de enlaces NIC en un host independiente*.

> **Advertencia:**
>
> No intente crear vínculos de red cuando la alta disponibilidad esté habilitada. El proceso de creación de vínculos perturba los latidos del corazón de alta disponibilidad en curso y hace que los anfitriones se autocerquen (se apaguen). Los hosts pueden no reiniciarse correctamente y pueden necesitar el comando `host-emergency-ha-disable` para recuperarse.

Selecciona el anfitrión que quieres que sea el coordinador de la agrupación. El coordinador del grupo pertenece a un grupo sin nombre de forma predeterminada. Para crear una agrupación de recursos con la CLI, cambie el nombre del grupo sin nombre existente:

```
1 xe pool-param-set name-label="New Pool" uuid=pool_uuid
2 <!--NeedCopy-->
```

Cree el vínculo NIC como se describe en Crear un vínculo NIC.

Abra una consola en un host al que quiera unir al grupo y ejecute el comando:

```
1 xe pool-join master-address=host1 master-username=root master-password=
     password
2 <!--NeedCopy-->
```

La información de red y vínculos se replica automáticamente en el nuevo host. La interfaz de administración se mueve automáticamente de la NIC del host en la que se configuró originalmente al PIF enlazado. Es decir, la interfaz de administración ahora se absorbe en el vínculo para que todo el vínculo funcione como interfaz de administración.

Utilice el comando `host-list` para buscar el UUID del host que se está configurando:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe host-list
<!--NeedCopy-->
```

> **Advertencia:**
>
> No intente crear vínculos de red mientras la alta disponibilidad esté habilitada. El proceso de creación de vínculos perturba los latidos del corazón de alta disponibilidad en curso y hace que los anfitriones se autocerquen (se apaguen). Los hosts pueden no reiniciarse correctamente y es posible que deba ejecutar el comando `host-emergency-ha-disable` para recuperarse.

Configurar una NIC de almacenamiento dedicada

Puede usar XenCenter o la CLI xe para asignar una dirección IP a una NIC y dedicarla a una función específica, como el tráfico de almacenamiento. Cuando configura una NIC con una dirección IP, lo hace mediante la creación de una interfaz secundaria. (La NIC habilitada para IP que XenServer utiliza para la administración se conoce como interfaz de administración).

Cuando quiera dedicar una interfaz secundaria para un propósito específico, asegúrese de que se haya implementado la configuración de red adecuada. Esto es para garantizar que la NIC se utilice únicamente para el tráfico deseado. Para dedicar una NIC al tráfico de almacenamiento, configure la NIC, el destino de almacenamiento, el conmutador y la VLAN de modo que solo se pueda acceder al destino a través de la NIC asignada. Si su configuración física e IP no limita el tráfico enviado a través de la NIC de almacenamiento, puede enviar tráfico, como el tráfico de administración, a través de la interfaz secundaria.

Cuando crea una nueva interfaz secundaria para el tráfico de almacenamiento, debe asignarle una dirección IP que sea:

- En la misma subred que el controlador de almacenamiento, si procede, y
- No en la misma subred que cualquier otra interfaz secundaria o la interfaz de administración.

Al configurar interfaces secundarias, cada interfaz secundaria debe estar en una subred independiente. Por ejemplo, si quiere configurar dos interfaces secundarias más para el almacenamiento, necesitará direcciones IP en tres subredes diferentes: una subred para la interfaz de administración, una subred para la interfaz secundaria 1 y una subred para la interfaz secundaria 2.

Si está utilizando la vinculación para la resiliencia de su tráfico de almacenamiento, puede considerar el uso de LACP en lugar de la vinculación de puente de Linux. Para usar la vinculación LACP, debe configurar el vSwitch como su pila de redes. Para obtener más información, consulte Redes de vSwitch.

> **Nota:**
>
> Al seleccionar una NIC para configurarla como interfaz secundaria para usarla con SR iSCSI o NFS,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> asegúrese de que la NIC dedicada utilice una subred IP independiente que no se pueda redirigir desde la interfaz de administración. Si no se aplica, es posible que el tráfico de almacenamiento se dirija a través de la interfaz de administración principal después de reiniciar el host, debido al orden en que se inicializan las interfaces de red.

Asegúrese de que el PIF esté en una subred independiente o que la redirección esté configurada para adaptarse a su topología de red para forzar el tráfico deseado a través del PIF seleccionado.

Configure una configuración de IP para el PIF, agregando los valores apropiados para el parámetro mode. Si usa direcciones IP estáticas, agregue los parámetros IP, máscara de red, puerta de enlace y DNS:

```
xe pif-reconfigure-ip mode=DHCP | Static uuid=pif-uuid
<!--NeedCopy-->
```

Establezca el parámetro disallow-unplug de PIF en true:

```
xe pif-param-set disallow-unplug=true uuid=pif-uuid
<!--NeedCopy-->
```

```
xe pif-param-set other-config:management_purpose="Storage" uuid=pif-
    uuid
<!--NeedCopy-->
```

Si quiere utilizar una interfaz secundaria para el almacenamiento que también se puede redirigir desde la interfaz de administración (teniendo en cuenta que esta configuración no es la mejor práctica), tiene dos opciones:

- Después de reiniciar el host, asegúrese de que la interfaz secundaria esté configurada correctamente. Use los comandos `xe pbd-unplug` y `xe pbd-plug` para reinicializar las conexiones de almacenamiento en el host. Este comando reinicia la conexión de almacenamiento y la redirige a través de la interfaz correcta.
- Como alternativa, puede utilizar `xe pif-forget` para eliminar la interfaz de la base de datos de XenServer y configurarla manualmente en el dominio de control. `xe pif-forget` es una opción avanzada y requiere que esté familiarizado con la configuración manual de las redes Linux.

Usar NIC habilitadas para SR-IOV

La virtualización de E/S de raíz única (SR-IOV) es una tecnología de virtualización que permite que un solo dispositivo PCI aparezca como varios dispositivos PCI en el sistema físico. El dispositivo físico real se conoce como función física (PF), mientras que los demás se conocen como funciones virtuales (VF). El hipervisor puede asignar una o más VF a una máquina virtual (VM): el huésped puede usar el dispositivo como si se hubiera asignado directamente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La asignación de una o más VF NIC a una máquina virtual permite que su tráfico de red omita el conmutador virtual. Cuando se configura, cada VM se comporta como si estuviera mediante la NIC directamente, lo que reduce la sobrecarga de procesamiento y mejora el performance.

Beneficios del SR-IOV

Un VF SR-IOV tiene un rendimiento mejor que el VIF. Puede garantizar la segregación basada en hardware entre el tráfico de diferentes máquinas virtuales a través de la misma NIC (sin pasar por la pila de red de XenServer).

Con esta función, puede:

- Habilite SR-IOV en las NIC que admiten SR-IOV.
- Inhabilite SR-IOV en las NIC que admiten SR-IOV.
- Administre las VF de SR-IOV como un grupo de recursos de VF.
- Asigne VF de SR-IOV a una VM.
- Configure las VF SR-IOV (por ejemplo, dirección MAC, VLAN, velocidad).
- Realice pruebas para confirmar si SR-IOV se admite como parte del kit de certificación automatizada.

Configuración del sistema

Configure la plataforma de hardware correctamente para admitir SR-IOV. Se requieren las siguientes tecnologías:

- Virtualización de MMU de E/S (AMD-vi e Intel VT-d)
- Interpretación alternativa de ID de redirección (ARI)
- Servicios de traducción de direcciones (ATS)
- Servicios de control de acceso (ACS)

Consulte la documentación que viene con el sistema para obtener información sobre cómo configurar el firmware del sistema para habilitar las tecnologías mencionadas.

Habilitar una red SR-IOV en una NIC

En XenCenter, use el asistente **Nueva red** en la ficha **Redes** para crear y habilitar una red SR-IOV en una NIC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Asignar una red SR-IOV a la interfaz virtual (nivel de VM)

En XenCenter, en el nivel de VM, use el asistente **Agregar interfaz virtual** en la ficha **Redes** para agregar una red habilitada para SR-IOV como interfaz virtual para esa VM. Para obtener más información, consulte Agregar una red nueva.

NIC e invitados compatibles

Para obtener una lista de las plataformas de hardware y NIC compatibles, consulte Lista de compatibilidad de hardware. Consulte la documentación proporcionada por el proveedor para un huésped en particular para determinar si es compatible con SR-IOV.

Limitaciones

- Para ciertas NIC que utilizan controladores heredados (por ejemplo, la familia Intel I350), el host debe reiniciarse para habilitar o inhabilitar SR-IOV en estos dispositivos.
- No se admite una red SR-IOV a nivel de grupo que tenga diferentes tipos de NIC.
- Es posible que una VF SR-IOV y una VIF normal de la misma NIC no puedan comunicarse entre sí debido a las limitaciones de hardware de la NIC. Para permitir que estas máquinas virtuales se comuniquen, asegúrese de que la comunicación utilice el patrón VF a VF o VIF a VIF y no VF a VIF.
- La configuración de calidad de servicio para algunas VF SR-IOV no se aplica porque no admiten la limitación de velocidad de la red.
- La migración en vivo, la suspensión y el punto de control no se admiten en las máquinas virtuales que utilizan una VF SR-IOV.
- Las VF SR-IOV no admiten la conexión en caliente.
- Las máquinas virtuales SR-IOV no admiten el arranque en red.
- Para algunas NIC con controladores NIC heredados, es posible que sea necesario reiniciar incluso después del reinicio del host, lo que indica que la NIC no puede habilitar SR-IOV.
- Si su VM tiene una VF SR-IOV, las funciones que requieren migración en vivo no son posibles. Esto se debe a que la VM está directamente vinculada a la VF NIC habilitada para SR-IOV física.
- La SR-IOV se puede usar en un entorno que hace uso de la alta disponibilidad. Sin embargo, la SR-IOV no se considera en la planificación de la capacidad. Las máquinas virtuales que tienen asignadas VF de SR-IOV se reinician según el mejor esfuerzo cuando hay un host en el grupo que tiene los recursos adecuados. Estos recursos incluyen SR-IOV habilitado en la red correcta y una VF gratuita.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Las VF SR-IOV no son compatibles con el PVS-Accelerator.

Configurar VF SR-IOV para controladores heredados

Por lo general, la cantidad máxima de VF que admite una NIC se puede determinar automáticamente. Para las NIC que utilizan controladores heredados (por ejemplo, la familia Intel I350), el límite se define en el archivo de configuración del módulo del controlador. Es posible que el límite deba ajustarse manualmente. Para ajustarlo al máximo, abra el archivo con un editor y cambie la línea que comienza:

```
## VFs-maxvfs-by-user:
<!--NeedCopy-->
```

Por ejemplo, para establecer el máximo de VF en 4 para que la edición `/etc/modprobe.d/igb.conf` del controlador `igb` lea:

```
## VFs-param: max_vfs
## VFs-maxvfs-by-default: 7
## VFs-maxvfs-by-user: 4
options igb max_vfs=0
<!--NeedCopy-->
```

> **Notas:**
>
> - El valor debe ser menor o igual que el valor de la línea `VFs-maxvfs-by-default`.
> - No cambie ninguna otra línea en estos archivos.
> - Realice los cambios antes de habilitar SR-IOV.

CLI

Consulte Comandos de SR-IOV para obtener instrucciones de la CLI sobre cómo crear, eliminar y mostrar redes SR-IOV y asignar una VF de SR-IOV a una VM.

Controlar la velocidad de los datos salientes (QoS)

Para limitar la cantidad de datos *salientes* que una VM puede enviar por segundo, establezca un valor opcional de calidad de servicio (QoS) en las interfaces virtuales (VIF) de VM. La configuración le permite especificar una velocidad de transmisión máxima para los paquetes salientes en *kilobytes* por segundo.

El valor de Calidad de servicio limita la velocidad de transmisión *desde* la VM. La configuración de Calidad de servicio no limita la cantidad de datos que la VM puede recibir. Si se quiere un límite de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

este tipo, recomendamos limitar la velocidad de los paquetes entrantes más arriba en la red (por ejemplo, en el nivel del conmutador).

Según la pila de red configurada en el grupo, puede establecer el valor de Calidad de servicio en las interfaces virtuales (VIF) de VM en uno de dos lugares. Puede establecer este valor mediante la CLI xe o en XenCenter.

- **XenCenter** Puede establecer el valor límite de velocidad de transmisión de calidad de servicio en el cuadro de diálogo de propiedades de la interfaz virtual.
- **comandos xe** Puede establecer la velocidad de transmisión de la calidad de servicio mediante la CLI mediante los comandos de la sección siguiente.

Ejemplo de comando CLI para QoS

Para limitar un VIF a una velocidad de transmisión máxima de 100 kilobytes por segundo mediante la CLI, utilice el comando `vif-param-set`:

```
xe vif-param-set uuid=vif_uuid qos_algorithm_type=ratelimit
xe vif-param-set uuid=vif_uuid qos_algorithm_params:kbps=100
<!--NeedCopy-->
```

> **Nota:**
>
> El parámetro `kbps` indica *kilobytes* por segundo (Kbps), no kilobits por segundo (kbps).

Cambiar las opciones de configuración de redes

En esta sección se explica cómo cambiar la configuración de red del host de XenServer. Incluye:

- Cambiar el nombre de host (es decir, el nombre del Sistema de nombres de dominio (DNS))
- Agregar o eliminar servidores DNS
- Cambiar las direcciones IP
- Cambiar la NIC que se utiliza como interfaz de administración
- Agregar una nueva NIC física al servidor
- Adición de un propósito a una red
- Activación del filtrado ARP (bloqueo del puerto del conmutador)

Nombre de host

El nombre de host del sistema, también conocido como nombre de dominio o DNS, se define en la base de datos de todo el grupo y se cambia mediante el comando `xe host-set-hostname-live`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de la CLI de la siguiente manera:

```
xe host-set-hostname-live host-uuid=host_uuid host-name=host-name
<!--NeedCopy-->
```

El nombre de host del dominio de control subyacente cambia dinámicamente para reflejar el nuevo nombre de host.

Servidores DNS

Para agregar o eliminar servidores DNS en la configuración de direcciones IP del host de XenServer, utilice el comando `pif-reconfigure-ip`. Por ejemplo, para un PIF con una IP estática:

```
xe pif-reconfigure-ip uuid=pif_uuid mode=static DNS=new_dns_ip IP=IP
    netmask=netmask
<!--NeedCopy-->
```

Cambiar la configuración de la dirección IP para un host independiente

Puede usar la CLI xe para cambiar la configuración de la interfaz de red. No cambie directamente los scripts de configuración de red subyacentes.

Para cambiar la configuración de la dirección IP de un PIF, use el comando `pif-reconfigure-ip` de la CLI. Consulte `pif-reconfigure-ip` para obtener más información sobre los parámetros del comando `pif-reconfigure-ip`. Consulte la siguiente sección para obtener información sobre cómo cambiar las direcciones IP del host en los grupos de recursos.

Cambiar la configuración de direcciones IP en los grupos de recursos

Los hosts XenServer de los grupos de recursos tienen una única dirección IP de administración que se utiliza para la administración y la comunicación hacia y desde otros hosts del grupo. Los pasos necesarios para cambiar la dirección IP de la interfaz de administración de un host son diferentes para el coordinador de grupos y otros hosts.

> **Nota:**
>
> Debe tener cuidado al cambiar la dirección IP de un host y otros parámetros de red. Según la topología de red y el cambio que se realice, se pueden perder las conexiones al almacenamiento de red. Cuando esto ocurre, el almacenamiento debe volver a conectarse mediante la función **Reparar almacenamiento** en XenCenter o mediante el comando `pbd-plug` de la CLI. Por este motivo, le recomendamos que migre las máquinas virtuales fuera del host antes de cambiar su configuración IP.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Utilice el comandopif-reconfigure-ip CLI para establecer la dirección IP como quiera. Consulte pif-reconfigure-ip para obtener más información sobre los parámetros del comando pif-reconfigure-ip. :

```
xe pif-reconfigure-ip uuid=pif_uuid mode=DHCP
<!--NeedCopy-->
```

Use el comando host-list CLI para confirmar que el host miembro se ha vuelto a conectar correctamente al coordinador del grupo comprobando que todos los demás hosts de XenServer del grupo estén visibles:

```
xe host-list
<!--NeedCopy-->
```

Cambiar la dirección IP del host XenServer coordinador del grupo requiere pasos adicionales. Esto se debe a que cada miembro del grupo utiliza la dirección IP publicada del coordinador del grupo para la comunicación. Los miembros del grupo no saben cómo ponerse en contacto con el coordinador del grupo cuando cambia su dirección IP.

Siempre que sea posible, utilice una dirección IP dedicada que no vaya a cambiar durante la vida útil del grupo para los coordinadores del grupo.

Utilice el comando de la interfaz de línea de comandos pif-reconfigure-ip para configurar la dirección IP como quiera:

```
xe pif-reconfigure-ip uuid=pif_uuid mode=DHCP
<!--NeedCopy-->
```

Cuando la dirección IP del coordinador del grupo cambia, todos los hosts miembros entran en modo de emergencia cuando no se ponen en contacto con el coordinador del grupo.

En el coordinador del grupo, utilice el comando pool-recover-slaves para forzar al coordinador del grupo a ponerse en contacto con cada miembro del grupo e informarles de la nueva dirección IP del coordinador del grupo:

```
xe pool-recover-slaves
<!--NeedCopy-->
```

Interfaz de administración

Al instalar XenServer en un host, una de sus NIC se designa como *interfaz de administración: la NIC que se usa para el tráfico de administración*de XenServer. La interfaz de administración se utiliza para las conexiones de XenCenter al host (por ejemplo, Citrix Virtual Apps and Desktops) y para la comunicación de host a host.

Utilice el comando pif-list para determinar qué PIF corresponde a la NIC que se utilizará como interfaz de administración. Se devuelve el UUID de cada PIF.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe pif-list
<!--NeedCopy-->
```

Utilice el comando `pif-param-list` para verificar la configuración de direccionamiento IP para el PIF utilizado para la interfaz de administración. Si es necesario, utilice el comando `pif-reconfigure-ip` para configurar el direccionamiento IP para el PIF que se va a utilizar.

```
xe pif-param-list uuid=pif_uuid
<!--NeedCopy-->
```

Use el comando `host-management-reconfigure` de la CLI para cambiar el PIF utilizado para la interfaz de administración. Si este host forma parte de un grupo de recursos, *este comando debe emitirse en la consola del host miembro*:

```
xe host-management-reconfigure pif-uuid=pif_uuid
<!--NeedCopy-->
```

Utilice el comando `network-list` para determinar qué PIF corresponde a la NIC que se utilizará como interfaz de administración para todos los hosts del grupo. Se devuelve el UUID de la red de todo el grupo.

```
xe network-list
<!--NeedCopy-->
```

Utilice el comando `network-param-list` para obtener los UUID PIF de todos los hosts del grupo. Utilice el comando `pif-param-list` para verificar la configuración de direccionamiento IP para el PIF de la interfaz de administración. Si es necesario, utilice el comando `pif-reconfigure-ip` para configurar el direccionamiento IP para el PIF que se va a utilizar.

```
xe pif-param-list uuid=pif_uuid
<!--NeedCopy-->
```

Use el comando `pool-management-reconfigure` de la CLI para cambiar el PIF utilizado para la interfaz de administración que se muestra en la lista Redes.

```
xe pool-management-reconfigure network-uuid=network_uuid
<!--NeedCopy-->
```

Restringir el uso del puerto 80

Puede usar HTTPS a través del puerto 443 o HTTP a través del puerto 80 para comunicarse con XenServer. Por motivos de seguridad, puede cerrar el puerto TCP 80 de la interfaz de administración. De forma predeterminada, el puerto 80 sigue abierto. Si lo cierra, cualquier cliente externo que utilice la interfaz de administración debe usar HTTPS a través del puerto 443 para conectarse a XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sin embargo, antes de cerrar el puerto 80, compruebe si todos sus clientes de API (en particular Citrix Virtual Apps and Desktops) pueden usar HTTPS a través del puerto 443.

Para cerrar el puerto 80, consulte el comando `https-only` xe CLI.

Desactivar el acceso de

Para inhabilitar por completo el acceso remoto a la consola de administración, utilice el comando de la interfaz de línea de comandos `host-management-disable`.

> **Advertencia:**
>
> Cuando la interfaz de administración está inhabilitada, debe iniciar sesión en la consola del host físico para realizar las tareas de administración. Las interfaces externas, como XenCenter, no funcionan cuando la interfaz de administración está inhabilitada.

Agregar una nueva NIC física

1. Instale una nueva NIC física en el host de XenServer de la manera habitual.
2. Reinicie el host de XenServer.
3. Enumere todas las NIC físicas de ese host de XenServer mediante el siguiente comando:

   ```
   xe pif-list host-uuid=<host_uuid>
   ```

4. Si no ve la NIC adicional, busque nuevas interfaces físicas mediante el siguiente comando:

   ```
   xe pif-scan host-uuid=<host_uuid>
   ```

   Este comando crea un nuevo objeto PIF para la nueva NIC.

5. Vuelva a enumerar las NIC físicas del host de XenServer para comprobar que la nueva NIC esté visible:

   ```
   xe pif-list host-uuid=<host_uuid>
   ```

6. El nuevo PIF aparece inicialmente como desconectado (`currently-attached ( RO): false`). Para que aparezca, usa el siguiente comando:

   ```
   xe pif-plug uuid=<uuid_of_pif>
   ```

Como alternativa, puede usar XenCenter para volver a buscar nuevas NIC. Para obtener más información, consulte Configuración de NIC en la documentación de XenCenter.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Eliminar una NIC física

Antes de quitar la NIC, asegúrese de conocer el UUID del PIF correspondiente. Elimine la NIC física del host de XenServer de la forma habitual. Tras reiniciar el host, ejecute el comando de CLI xe `pif-forget uuid=<UUID>` para destruir el objeto PIF.

Agregar un propósito a una red

El propósito de la red se puede utilizar para agregar funcionalidades adicionales a una red. Por ejemplo, la capacidad de usar la red para realizar conexiones NBD.

Para agregar un propósito de red, utilice el`xe network-param-add` comando:

```
1 xe network-param-add param-name=purpose param-key=purpose uuid=network-
     uuid
2 <!--NeedCopy-->
```

Para eliminar un propósito de red, utilice el`xe network-param-remove` comando:

```
1 xe network-param-remove param-name=purpose param-key=purpose uuid=
     network-uuid
2 <!--NeedCopy-->
```

Actualmente, los valores disponibles para el propósito de la red son `nbd` y `insecure_nbd`. Para obtener más información, consulte la Guía de seguimiento de bloques modificados de XenServer.

Usar el bloqueo del puerto del conmutador

La función de bloqueo de puertos del conmutador de XenServer le permite controlar el tráfico enviado desde máquinas virtuales desconocidas, que no son de confianza o potencialmente hostiles, al limitar su capacidad de fingir que tienen una dirección MAC o IP que no se les ha asignado. Puede usar los comandos de bloqueo de puertos para bloquear todo el tráfico en una red de forma predeterminada o definir direcciones IP específicas desde las que una VM individual puede enviar tráfico.

El bloqueo de puertos de conmutador es una función diseñada para los proveedores de servicios de nube pública en entornos preocupados por las amenazas internas. Esta funcionalidad ayuda a los proveedores de servicios en la nube pública que tienen una arquitectura de red en la que cada VM tiene una dirección IP pública conectada a Internet. Como los arrendatarios de la nube no son de confianza, puede usar medidas de seguridad, como la protección contra la suplantación, para garantizar que los arrendatarios no puedan atacar otras máquinas virtuales en la nube.

El uso del bloqueo de puertos de switch le permite simplificar la configuración de la red al permitir que todos sus arrendatarios o invitados usen la misma red de capa 2.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Una de las funciones más importantes de los comandos de bloqueo de puertos es que pueden restringir el tráfico que envía un invitado que no es de confianza. Esto restringe la capacidad del huésped de fingir que tiene una dirección MAC o IP que en realidad no posee. Específicamente, puede usar estos comandos para evitar que un invitado:

- Reclamar una dirección IP o MAC distinta de las que el administrador de XenServer ha especificado que puede usar
- Interceptar, falsificar o interrumpir el tráfico de otras VM

Requisitos

- La función de bloqueo de puertos del conmutador de XenServer es compatible con las pilas de redes Linux Bridge y vSwitch.
- Cuando habilita el control de acceso basado en roles (RBAC) en su entorno, el usuario que configura el bloqueo del puerto del conmutador debe iniciar sesión con una cuenta que tenga al menos un rol de operador de grupo o administrador de grupo. Cuando RBAC no está habilitado en su entorno, el usuario debe iniciar sesión con la cuenta raíz del coordinador del grupo.
- Cuando ejecuta los comandos de bloqueo del puerto del conmutador, las redes pueden estar en línea o fuera de línea.
- En los huéspedes de Windows, el icono de red desconectada solo aparece cuando XenServer VM Tools está instalado en el huésped.

Notas Sin ninguna configuración de bloqueo del puerto del conmutador, las VIF se establecen en "network_default"y las redes en "unlocked". "

No se admite la configuración del bloqueo del puerto del conmutador cuando se utilizan controladores de terceros en el entorno.

El bloqueo de puertos de switch no impide que los arrendatarios de la nube:

- Realizar un ataque a nivel de IP contra otro arrendatario/usuario. Sin embargo, el bloqueo del puerto del conmutador les impide realizar el ataque a nivel de IP si intentan utilizar los siguientes medios para hacerlo y el bloqueo del puerto del conmutador está configurado: a) hacerse pasar por otro arrendatario en la nube o usuario o b) iniciar una intercepción del tráfico destinado a otro usuario.
- Recursos de red agotadores.
- Recibir tráfico destinado a otras máquinas virtuales a través de comportamientos normales de inundación del conmutador (para direcciones MAC de difusión o direcciones MAC de destino desconocidas).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Del mismo modo, el bloqueo del puerto del conmutador no restringe a dónde puede enviar tráfico una máquina virtual.

Notas de implementación Puede implementar la funcionalidad de bloqueo del puerto del conmutador mediante la línea de comandos o la API de XenServer. Sin embargo, en entornos grandes, donde la automatización es una preocupación principal, el método de implementación más típico puede ser el uso de la API.

Ejemplos En esta sección se proporcionan ejemplos de cómo el bloqueo de puertos de switch puede prevenir ciertos tipos de ataques. En estos ejemplos, VM-c es una máquina virtual que un arrendatario hostil (Arrendatario C) arrienda y utiliza para los ataques. La máquina virtual a y la máquina virtual b son máquinas virtuales arrendadas por arrendatarios no atacantes.

Ejemplo 1: Cómo el bloqueo del puerto del conmutador puede evitar la suplantación de identidad de ARP:

La suplantación de ARP se utiliza para indicar los intentos de un atacante de asociar su dirección MAC con la dirección IP de otro nodo. La suplantación de ARP puede provocar que el tráfico del nodo se envíe al atacante. Para lograr este objetivo, el atacante envía mensajes ARP falsos (falsificados) a una LAN Ethernet.

Caso:

La máquina virtual A (VM-a) quiere enviar tráfico IP desde la máquina virtual a la máquina virtual B (VM-b) dirigiéndolo a la dirección IP de la máquina virtual B. El propietario de la máquina virtual C quiere usar la suplantación de ARP para simular que su VM, VM-c, es en realidad VM-b.

1. La VM-c envía un flujo especulativo de respuestas ARP a la VM-a. Las respuestas ARP afirman que la dirección MAC en la respuesta (c_MAC) está asociada a la dirección IP, b_IP

   Resultado: Como el administrador habilitó el bloqueo del puerto del conmutador, todos estos paquetes se descartan porque al habilitar el bloqueo del puerto del conmutador se evita la suplantación de identidad.

2. La VM-b envía una respuesta ARP a la VM-a, afirmando que la dirección MAC en la respuesta (b_MAC) está asociada a la dirección IP, b_IP.

   Resultado: VM-a recibe la respuesta ARP de la VM-b.

Ejemplo 2: Prevención de la suplantación de identidad de IP:

La suplantación de direcciones IP es un proceso que oculta la identidad de los paquetes mediante la creación de paquetes de Protocolo de Internet (IP) con una dirección IP de origen falsificada.

Caso:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El arrendatario C intenta realizar un ataque de denegación de servicio utilizando su host, Host-C, en un sistema remoto para disimular su identidad.

Intento 1:

El arrendatario C establece la dirección IP y la dirección MAC del Host-C en las direcciones IP y MAC de la máquina virtual (a_IP y a_MAC). El arrendatario C indica al Host-C que envíe tráfico IP a un sistema remoto.

Resultado: los paquetes Host-C se descartan. Esto se debe a que el administrador habilitó el bloqueo del puerto del conmutador. Los paquetes Host-C se descartan porque al habilitar el bloqueo del puerto del conmutador se evita la suplantación de identidad.

Intento 2:

El arrendatario C establece la dirección IP del Host-C en la dirección IP de la máquina virtual a (a_IP) y conserva su C_mac original.

El arrendatario C indica al Host-C que envíe tráfico IP a un sistema remoto.

Resultado: los paquetes Host-C se descartan. Esto se debe a que el administrador habilitó el bloqueo del puerto del conmutador, lo que evita la suplantación de identidad.

Ejemplo 3: Alojamiento web:

Caso:

Alice es administradora de infraestructuras.

Uno de sus arrendatarios, el arrendatario B, aloja varios sitios web desde su VM, VM-b. Cada sitio web necesita una dirección IP distinta alojada en la misma interfaz de red virtual (VIF).

Alice reconfigura la VIF de Host-B para que se bloquee en una sola MAC pero en muchas direcciones IP.

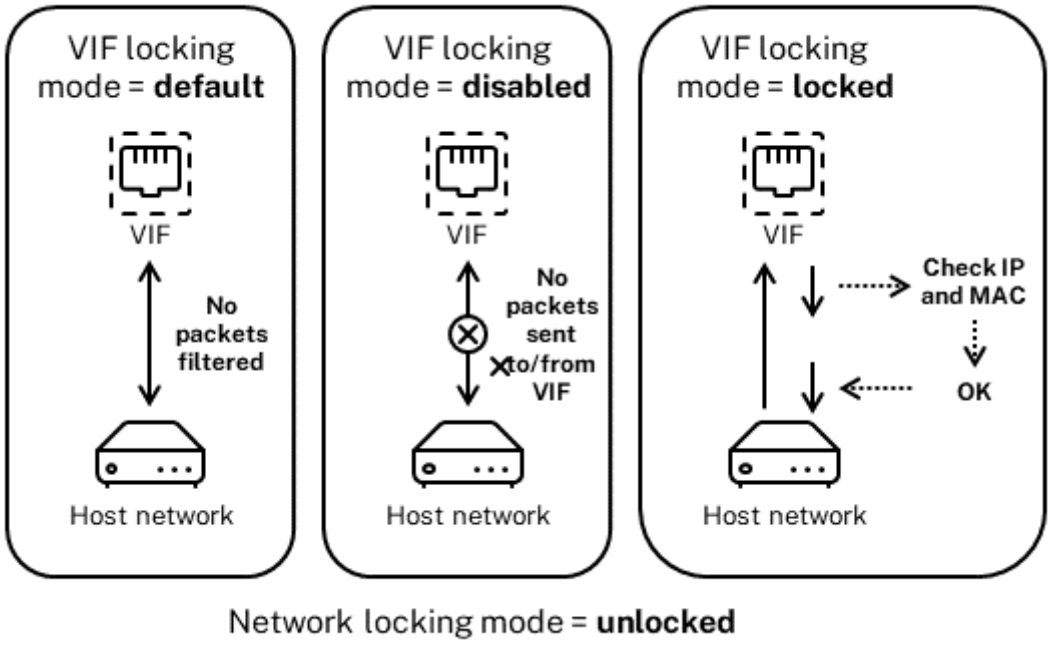
Cómo funciona el bloqueo de puertos de conmutación La función de bloqueo del puerto del conmutador le permite controlar el filtrado de paquetes en uno o más de dos niveles:

- **Nivel VIF**. Los ajustes que configure en el VIF determinan cómo se filtran los paquetes. Puede configurar el VIF para evitar que la máquina virtual envíe tráfico, restringir el VIF para que solo pueda enviar tráfico mediante su dirección IP asignada o permitir que la máquina virtual envíe tráfico a cualquier dirección IP de la red conectada al VIF.
- **Nivel de red**. La red XenServer determina cómo se filtran los paquetes. Cuando se establece el modo de bloqueo de un VIF en `network_default`, hace referencia a la configuración de bloqueo a nivel de red para determinar qué tráfico permitir.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Independientemente de la pila de red que utilice, la función funciona de la misma manera. Sin embargo, como se describe con más detalle en las secciones siguientes, el puente de Linux no admite completamente el bloqueo de puertos de conmutador en IPv6.

Estados del modo de bloqueo de VIF La función de bloqueo de puertos del conmutador de XenServer proporciona un modo de bloqueo que permite configurar las VIF en cuatro estados diferentes. Estos estados solo se aplican cuando el VIF está conectado a una máquina virtual en ejecución.



- **network_default**. Cuando el estado del VIF se establece en `network_default`, XenServer usa el parámetro de la red para determinar si **`default`**`-locking-mode` debe filtrar los paquetes que viajan a través del VIF y cómo hacerlo. El comportamiento varía en función de si la red asociada tiene el parámetro de modo de bloqueo predeterminado de la red establecido en inhabilitado o desbloqueado:

  -**`default`**`-locking-mode=disabled`, XenServer aplica una regla de filtrado para que el VIF elimine todo el tráfico.

  -**`default`**`-locking-mode`=desbloqueado, XenServer elimina todas las reglas de filtrado asociadas al VIF. De forma predeterminada, el parámetro de modo de bloqueo predeterminado se establece en `unlocked`.

  Para obtener información sobre el parámetro **`default`**`-locking-mode`, consulte Comandos de red.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El modo de bloqueo predeterminado de la red no afecta a las VIF conectadas cuyo estado de bloqueo es distinto de `network_default`.

> **Nota:**
>
> No se puede cambiar **`default`**`-locking-mode` de una red que tiene VIFs activos conectados a ella.

- **Bloqueado**. XenServer aplica reglas de filtrado para que solo el tráfico enviado hacia/desde las direcciones MAC e IP especificadas pueda enviarse a través del VIF. En este modo, si no se especifican direcciones IP, la VM no puede enviar tráfico a través de esa VIF, en esa red.

  Para especificar las direcciones IP desde las que el VIF acepta tráfico, utilice las direcciones IP IPv4 o IPv6 mediante los parámetros `ipv4_allowed` o `ipv6_allowed`. Sin embargo, si tiene configurado el puente de Linux, no escriba direcciones IPv6.

  XenServer le permite escribir direcciones IPv6 cuando el puente de Linux está activo. Sin embargo, XenServer no puede filtrar en función de las direcciones IPv6 escritas. La razón es que el puente de Linux no tiene módulos para filtrar paquetes de Neighbor Discovery Protocol (NDP). Por lo tanto, no se puede implementar una protección completa y los invitados podrían hacerse pasar por otro huésped falsificando paquetes NDP. Como resultado, si especifica una sola dirección IPv6, XenServer permite que todo el tráfico IPv6 pase a través del VIF. Si no especifica ninguna dirección IPv6, XenServer no permitirá que ningún tráfico IPv6 pase al VIF.
- **Desbloqueado**. Todo el tráfico de red puede pasar por el VIF. Es decir, no se aplican filtros a ningún tráfico que vaya hacia o desde el VIF.
- **Inhabilitado**. No se permite el paso del tráfico a través del VIF. (Es decir, XenServer aplica una regla de filtrado para que el VIF elimine todo el tráfico).

Configurar el bloqueo del puerto del conmutador En esta sección se describen tres procedimientos diferentes:

- Restringir las VIF para que usen una dirección IP específica
- Agregue una dirección IP a una lista restringida existente. Por ejemplo, para agregar una dirección IP a una VIF cuando la máquina virtual se está ejecutando y está conectada a la red (por ejemplo, si está desconectando una red temporalmente).
- Eliminar una dirección IP de una lista restringida existente

Si el modo de bloqueo de un VIF está establecido en `locked`, solo puede usar las direcciones especificadas en los parámetros `ipv4-allowed` o `ipv6-allowed`.

Dado que, en algunos casos relativamente raros, las VIF pueden tener más de una dirección IP, es posible especificar varias direcciones IP para una VIF.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puede realizar estos procedimientos antes o después de que se conecte la VIF (o se inicie la VM).

Cambie el modo de bloqueo predeterminado a bloqueado, si aún no lo está utilizando, ejecutando el siguiente comando:

```
xe vif-param-set uuid=vif-uuid locking-mode=locked
<!--NeedCopy-->
```

`vif-uuid` representa el UUID del VIF que quiere permitir el envío de tráfico. Para obtener el UUID, ejecute el comando `vif-list` xe en el host. `vm-uuid` Indica la máquina virtual para la que aparece la información. La ID del dispositivo indica el número de dispositivo de la VIF.

Ejecute el comando `vif-param-set` para especificar las direcciones IP desde las que la máquina virtual puede enviar tráfico. Realice una o varias de las siguientes acciones:

- Especifique uno o más destinos de direcciones IP IPv4. Por ejemplo:

```
xe vif-param-set uuid=vif-uuid ipv4-allowed=comma separated list
   of ipv4-addresses
<!--NeedCopy-->
```

- Especifique uno o más destinos de direcciones IP IPv6. Por ejemplo:

```
xe vif-param-set uuid=vif-uuid ipv6-allowed=comma separated list
   of ipv6-addresses
<!--NeedCopy-->
```

Puede especificar varias direcciones IP separándolas con una coma, como se muestra en el ejemplo anterior.

Después de realizar el procedimiento para restringir una VIF para que use una dirección IP específica, puede agregar una o más direcciones IP que la VIF puede usar.

Ejecute el comando `vif-param-add` para agregar las direcciones IP a la lista existente. Realice una o varias de las siguientes acciones:

- Especifique la dirección IP IPv4. Por ejemplo:

```
xe vif-param-add uuid=vif-uuid ipv4-allowed=comma separated list
   of ipv4-addresses
<!--NeedCopy-->
```

- Especifique la dirección IP IPv6. Por ejemplo:

```
xe vif-param-add uuid=vif-uuid ipv6-allowed=comma separated list
   of ipv6-addresses
<!--NeedCopy-->
```

Si restringe una VIF para que use dos o más direcciones IP, puede eliminar una de esas direcciones IP de la lista.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ejecute el comando `vif-param-remove` para eliminar las direcciones IP de la lista existente. Realice una o varias de las siguientes acciones:

- Especifique la dirección IP IPv4 que quiere eliminar. Por ejemplo:

```
xe vif-param-remove uuid=vif-uuid ipv4-allowed=comma separated
   list of ipv4-addresses
<!--NeedCopy-->
```

- Especifique la dirección IP IPv6 que quiere eliminar. Por ejemplo:

```
xe vif-param-remove uuid=vif-uuid ipv6-allowed=comma separated
   list of ipv6-addresses
<!--NeedCopy-->
```

Impedir que una máquina virtual envíe o reciba tráfico de una red específica El siguiente procedimiento evita que una máquina virtual se comunique a través de una VIF específica. Cuando un VIF se conecta a una red XenServer específica, puede usar este procedimiento para evitar que una máquina virtual envíe o reciba tráfico de una red específica. Esto proporciona un nivel de control más granular que la desactivación de una red completa.

Si utiliza el comando de la CLI, no necesita desconectar la VIF para establecer el modo de bloqueo de la VIF. El comando cambia las reglas de filtrado mientras se ejecuta el VIF. En este caso, la conexión de red aún parece estar presente, sin embargo, el VIF descarta todos los paquetes que la máquina virtual intenta enviar.

> **Consejo:**
>
> Para encontrar el UUID de un VIF, ejecute el comando `vif-list` xe en el host. La ID del dispositivo indica el número de dispositivo de la VIF.

Para evitar que un VIF reciba tráfico, inhabilite el VIF conectado a la red desde la que quiere impedir que la máquina virtual reciba tráfico:

```
xe vif-param-set uuid=vif-uuid locking-mode=disabled
<!--NeedCopy-->
```

También puede inhabilitar la VIF en XenCenter seleccionando la interfaz de red virtual en la ficha Redes de la máquina virtual y haciendo clic en Desactivar.

Eliminar la restricción de un VIF a una dirección IP Para volver al estado del modo de bloqueo predeterminado (original), utilice el procedimiento siguiente. De forma predeterminada, cuando se crea un VIF, XenServer lo configura para que no se limite al uso de una dirección IP específica.

Para revertir un VIF a un estado desbloqueado, cambie el modo de bloqueo predeterminado de VIF a desbloqueado. Si aún no está utilizando ese modo, ejecute el siguiente comando:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe vif-param-set uuid=vif_uuid locking-mode=unlocked
<!--NeedCopy-->
```

Simplifique la configuración del modo de bloqueo de VIF en la nube En lugar de ejecutar los comandos del modo de bloqueo de VIF para cada VIF, puede asegurarse de que todos los VIF estén inhabilitados de forma predeterminada. Para hacerlo, debe cambiar el filtrado de paquetes a nivel de red. Al cambiar el filtrado de paquetes, la red XenServer determina cómo se filtran los paquetes, como se describe en la sección anterior *Cómo funciona el bloqueo del puerto del conmutador*.

Específicamente, el parámetro **default**-locking-mode de una red determina cómo se comportan los nuevos VIF con configuración predeterminada. Siempre que el locking-mode de un VIF se establece en **default**, el VIF hace referencia al modo de bloqueo de red (**default**-locking-mode) para determinar si se filtran los paquetes que viajan a través del VIF y cómo hacerlo:

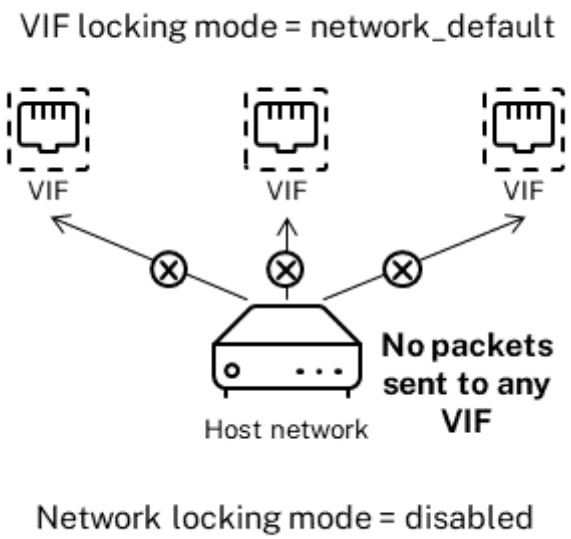
- **Desbloqueado**. Cuando el **default**-locking-mode parámetro de red está establecido en unlocked, XenServer permite que la máquina virtual envíe tráfico a cualquier dirección IP de la red a la que se conecte el VIF.
- **Inhabilitado**. Cuando el **default**-locking-mode parámetro se establece en disabled, XenServer aplica una regla de filtrado para que el VIF elimine todo el tráfico.

De forma predeterminada, **default**-locking-mode para todas las redes creadas en XenCenter y que utilizan la línea de comandos están configuradas en unlocked.

Al establecer el modo de bloqueo de la VIF en su valor predeterminado (network_default), puede crear una configuración básica predeterminada (a nivel de red) para todas las VIF recién creadas que se conectan a una red específica.

Esta ilustración muestra cómo, cuando el locking-mode de una VIF se establece en su configuración predeterminada (network_default), la VIF utiliza la red **default**-locking-mode para determinar su comportamiento.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Por ejemplo, de forma predeterminada, los VIF se crean con su `locking-mode` establecido en `network_default`. Si establece el **`default`**`-locking-mode=` de una red`disabled`, se inhabilitarán todas las VIF nuevas para las que no haya configurado el modo de bloqueo. Las VIF permanecen inhabilitadas hasta que (a) cambie el parámetro `locking-mode` de la VIF individual o (b) establezca explícitamente el `locking-mode` de las VIF en 'unlocked. Esto es útil cuando confías lo suficiente en una VM específica como para no querer filtrar su tráfico en absoluto.

Para cambiar la configuración del modo de bloqueo predeterminado de una red:

Después de crear la red, cambie el modo de bloqueo predeterminado ejecutando el siguiente comando:

```
xe network-param-set uuid=network-uuid default-locking-mode=[unlocked|
   disabled]
<!--NeedCopy-->
```

> **Nota:**
>
> Para obtener el UUID de una red, ejecute el comando xe `network-list`. Este comando muestra los UUID de todas las redes del host en el que ejecutó el comando.

Para comprobar la configuración del modo de bloqueo predeterminado de una red:

Ejecute uno de los siguientes comandos:

```
xe network-param-get uuid=network-uuid param-name=default-locking-mode
<!--NeedCopy-->
```

O BIEN:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe network-list uuid=network-uuid params=default-locking-mode
<!--NeedCopy-->
```

Usar la configuración de red para el filtrado de tráfico VIF El siguiente procedimiento indica a un VIF de una máquina virtual que utilice la **default**-locking-mode configuración de red de XenServer de la propia red para determinar cómo filtrar el tráfico.

1. Cambie el estado de bloqueo de VIF a network_default, si aún no está utilizando ese modo, ejecutando el siguiente comando:

   ```
   xe vif-param-set uuid=vif_uuid locking-mode=network_default
   <!--NeedCopy-->
   ```

2. Cambie el modo de bloqueo predeterminado a unlocked, si aún no lo está utilizando, ejecutando el siguiente comando:

   ```
   xe network-param-set uuid=network-uuid default-locking-mode=
      unlocked
   <!--NeedCopy-->
   ```

Solucionar problemas de redes

February 23, 2024

Si tiene problemas con la configuración de redes, primero asegúrese de que no ha cambiado directamente ninguno de los archivos ifcfg-* de dominio de control. El agente host de dominio de control administra los archivos ifcfg directamente y se sobrescriben los cambios.

Diagnóstico de corrupción en la red

Algunos modelos de tarjetas de red requieren actualizaciones de firmware del proveedor para funcionar de manera fiable bajo carga o cuando se activan ciertas optimizaciones. Si ve tráfico dañado en las máquinas virtuales, intente obtener el firmware más reciente del proveedor y, a continuación, utilícelo para actualizar el hardware.

Si el problema persiste, puede usar la CLI para inhabilitar las optimizaciones de descarga de recepción o transmisión en la interfaz física.

> **Advertencia:**
>
> La desactivación de las optimizaciones de descarga de recepción o transmisión puede provocar

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> una pérdida de rendimiento y un mayor uso de la CPU.

Primero, determine el UUID de la interfaz física. Puede filtrar en el campo `device` de la siguiente manera:

```
xe pif-list device=eth0
<!--NeedCopy-->
```

A continuación, defina el siguiente parámetro en el PIF para inhabilitar la descarga de TX:

```
xe pif-param-set uuid=pif_uuid other-config:ethtool-tx=off
<!--NeedCopy-->
```

Por último, vuelva a conectar el PIF o reinicie el host para que el cambio surta efecto.

Restablecimiento de la red

Una configuración de red incorrecta puede provocar la pérdida de la conectividad de red. Cuando no hay conectividad de red, es posible que no se pueda acceder al host de XenServer a través de XenCenter o SSH remoto. El restablecimiento de red de emergencia proporciona un mecanismo sencillo para recuperar y restablecer la red de un host.

La función de restablecimiento de red de emergencia está disponible en la CLI mediante el comando `xe-reset-networking` y en la sección **Interfaz de red y administración** de `xsconsole`.

Las configuraciones incorrectas que provocan una pérdida de conectividad de red incluyen cambiar el nombre de las interfaces de red, crear enlaces o VLAN, o errores al cambiar la interfaz de administración. Por ejemplo, escribir una dirección IP incorrecta. Es posible que también quiera ejecutar esta utilidad en los siguientes casos:

- Cuando una actualización gradual del grupo, actualización manual, instalación de parches rápidos o instalación de controladores provoca una falta de conectividad de red, o
- Si un coordinador de grupos o un host de un grupo de recursos no puede ponerse en contacto con otros hosts.

Utilice la utilidad `xe-reset-networking` solo en caso de emergencia, ya que elimina la configuración de todos los PIF, enlaces, VLAN y túneles asociados al host. Se conservan las redes de invitados y las VIF. Como parte de esta utilidad, las VM se cierran con fuerza. Antes de ejecutar este comando, apague las VM de forma limpia siempre que sea posible. Antes de aplicar un restablecimiento, puede cambiar la interfaz de administración y especificar qué configuración de IP, DHCP o estática se puede usar.

Si el coordinador del grupo requiere un restablecimiento de la red, primero restablezca la red en el coordinador del grupo antes de aplicar un restablecimiento de la red a los miembros del grupo. Aplique

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

el restablecimiento de red en todos los hosts restantes del grupo para garantizar que la configuración de red del grupo sea homogénea. La homogeneidad de la red es un factor importante para la migración en vivo.

> **Nota:**
>
> Si la dirección IP del coordinador del grupo (la interfaz de administración) cambia como resultado de un restablecimiento de la red o `xe host-management-reconfigure`, aplique el comando network reset a otros hosts del grupo. Esto es para garantizar que los miembros del grupo puedan volver a conectarse con el coordinador del grupo en su nueva dirección IP. En esta situación, se debe especificar la dirección IP del coordinador del grupo.
>
> El restablecimiento de red NO se admite cuando la alta disponibilidad está habilitada. Para restablecer la configuración de red en este caso, primero debe inhabilitar manualmente la alta disponibilidad y, a continuación, ejecutar el comando network reset.

Verificación del restablecimiento de la red

Después de especificar el modo de configuración que se utilizará después del restablecimiento de la red `xsconsole` y la configuración de visualización de la CLI que se aplicará después del reinicio del host. Es una última oportunidad de modificar antes de aplicar el comando de reinicio de red de emergencia. Después del reinicio, la nueva configuración de red se puede verificar en XenCenter y `xsconsole`. En XenCenter, con el host seleccionado, seleccione la ficha **Redes** para ver la nueva configuración de red. La sección Interfaz de red y administración de **xsconsole** muestra esta información.

> **Nota:**
>
> Ejecute el restablecimiento de la red de emergencia en otros miembros del grupo para replicar enlaces, VLAN o túneles desde la nueva configuración del coordinador del grupo.

Uso de la CLI para restablecer la red

En la tabla siguiente se muestran los parámetros opcionales disponibles que se pueden usar al ejecutar el comando `xe-reset-networking`.

> **Advertencia:**
>
> Los usuarios son responsables de garantizar la validez de los parámetros del comando `xe-reset-networking` y de comprobar los parámetros cuidadosamente. Si especifica parámetros no válidos, es posible que se pierdan la conectividad y la configuración de la red. En esta situación, le recomendamos que vuelva a ejecutar el comando `xe-reset-networking` sin utilizar ningún parámetro.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> El restablecimiento de la configuración de redes de un grupo completo **debe** comenzar en el coordinador del grupo, seguido del restablecimiento de la red en todos los hosts restantes del grupo.

Parámetro	Requerido/opcional	Descripción
`-m`, `--master`	Opcional	Dirección IP de la interfaz de administración del coordinador del grupo. El valor predeterminado es la última dirección IP del coordinador de grupo conocido.
`--device`	Opcional	Nombre del dispositivo de la interfaz de administración. De forma predeterminada, el nombre del dispositivo especificado durante la instalación.
`--mode=static`	Opcional	Habilita los cuatro parámetros de red siguientes para la configuración de IP estática para la interfaz de administración. Si no se especifica, las redes se configuran mediante DHCP.
`--ip`	Obligatorio, si `mode=static`	Dirección IP de la interfaz de administración del host. Solo válido si`mode=static`.
`--netmask`	Obligatorio, si `mode=static`	Máscara de red para la interfaz de administración. Solo válido si`mode=static`.
`--gateway`	Opcional	Puerta de enlace para la interfaz de administración. Solo válido si`mode=static`.
`--dns`	Opcional	Servidor DNS para la interfaz de administración. Solo válido si`mode=static`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Parámetro	Requerido/opcional	Descripción
`--vlan`	Opcional	Etiqueta VLAN para la interfaz de administración. Se establece de forma predeterminada en la etiqueta VLAN especificada durante la instalación.

Ejemplos de línea de comandos para coordinadores de grupos Ejemplos de comandos que se pueden aplicar en un coordinador de grupos:

Para restablecer las redes para la configuración de DHCP:

```
xe-reset-networking
<!--NeedCopy-->
```

Para restablecer las redes para la configuración de IP estática:

```
xe-reset-networking --mode= static --ip=ip-address \
    --netmask=netmask --gateway=gateway \
    --dns=dns
<!--NeedCopy-->
```

Para restablecer las redes para la configuración de DHCP si otra interfaz se convirtió en la interfaz de administración después de la configuración inicial:

```
xe-reset-networking --device=device-name
<!--NeedCopy-->
```

Para restablecer las redes para la configuración de IP estática si otra interfaz se convirtió en la interfaz de administración después de la configuración inicial:

```
xe-reset-networking --device=device-name --mode=static \
    --ip=ip-address --netmask=netmask \
    --gateway=gateway --dns=dns
<!--NeedCopy-->
```

Para restablecer las redes para la interfaz de administración en la VLAN:

```
xe-reset-networking --vlan=VLAN TAG
<!--NeedCopy-->
```

> **Nota:**
>
> El comando `reset-network` también se puede usar junto con los valores de configuración de IP.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ejemplos de línea de comandos de miembros del grupo Todos los ejemplos anteriores también se aplican a los miembros del grupo. Además, se puede especificar la dirección IP del coordinador del grupo (lo cual es necesario si ha cambiado).

Para restablecer las redes para la configuración de DHCP:

```
xe-reset-networking
<!--NeedCopy-->
```

Para restablecer las redes para DHCP si se cambió la dirección IP del coordinador del grupo:

```
xe-reset-networking --master=pool-coordinator-ip-address
<!--NeedCopy-->
```

Para restablecer las redes para la configuración de IP estática, suponiendo que la dirección IP del coordinador del grupo no haya cambiado:

```
xe-reset-networking --mode=static --ip=ip-address --netmask=netmask \
    --gateway=gateway --dns=dns
<!--NeedCopy-->
```

Para restablecer las redes para la configuración de DHCP si la interfaz de administración y la dirección IP del coordinador del grupo se cambiaron después de la configuración inicial:

```
xe-reset-networking --device=device-name --master=pool-coordinator-ip-
   address
<!--NeedCopy-->
```

---

layout: doc
description: Understand the concepts involved in XenServer storage.—

Almacenamiento

En esta sección se describe cómo el hardware de almacenamiento físico se asigna a las máquinas virtuales (VM) y los objetos de software que utiliza la API de administración para realizar tareas relacionadas con el almacenamiento. Las secciones detalladas de cada uno de los tipos de almacenamiento admitidos incluyen la siguiente información:

- Procedimientos para crear almacenamiento para máquinas virtuales mediante la CLI, con opciones de configuración de dispositivos específicos del tipo
- Generación de instantáneas para realizar copias de seguridad
- Prácticas recomendadas para administrar el almacenamiento

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Repositorios de almacenamiento (SR)

Un repositorio de almacenamiento (SR) es un destino de almacenamiento específico, en el que se almacenan las imágenes de disco virtual (VDI) de la máquina virtual (VM). Una VDI es una abstracción de almacenamiento que representa una unidad de disco duro virtual (HDD).

Los SR son flexibles, con soporte integrado para las siguientes unidades:

Conectados localmente:

- SATA
- SCSI
- SAS
- NVMe

El hardware de almacenamiento físico local puede ser una unidad de disco duro (HDD) o una unidad de estado sólido (SSD).

Conectado remotamente:

- iSCSI
- NFS
- SAS
- Pymes (solo versión 3)
- Canal de fibra

> **Nota:**
>
> No se admiten NVMe a través de canal de fibra ni NVMe a través de TCP.

Las abstracciones de SR y VDI permiten que las funciones de almacenamiento avanzadas se expongan en los destinos de almacenamiento que las admiten. Por ejemplo, funciones avanzadas como *aprovisionamiento ligero*, instantáneas de VDI y clonación rápida. Para los subsistemas de almacenamiento que no admiten operaciones avanzadas directamente, se proporciona una pila de software que implementa estas funciones. Esta pila de software se basa en la especificación de disco duro virtual (VHD) de Microsoft.

Un repositorio de almacenamiento es una estructura de datos en disco persistente. Para los tipos de SR que utilizan un dispositivo de bloques subyacente, el proceso de creación de un SR implica borrar todos los datos existentes en el destino de almacenamiento especificado. Otros tipos de almacenamiento, como NFS, crean un contenedor en la matriz de almacenamiento en paralelo a los SR existentes.

Cada host de XenServer puede usar varios SR y diferentes tipos de SR simultáneamente. Estos SR pueden compartirse entre hosts o dedicarse a hosts particulares. El almacenamiento compartido se

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

agrupa entre varios hosts dentro de un grupo de recursos definido. Un SR compartido debe ser accesible en red para cada host del grupo. Todos los hosts de un único grupo de recursos deben tener al menos un SR compartido en común. El almacenamiento compartido no se puede compartir entre varios grupos.

Los comandos SR proporcionan operaciones para crear, destruir, cambiar el tamaño, clonar, conectar y descubrir los VDI individuales que contienen. Las operaciones de CLI para administrar repositorios de almacenamiento se describen en los comandos de SR.

> **Advertencia:**
>
> XenServer no admite instantáneas en el nivel de SAN externo de un LUN para ningún tipo de SR.

Imagen de disco vDisk (VDI)

Una imagen de disco virtual (VDI) es una abstracción de almacenamiento que representa una unidad de disco duro (HDD) virtual. Los VDI son la unidad fundamental del almacenamiento virtualizado en XenServer. Los VDI son objetos persistentes en disco que existen independientemente de los hosts de XenServer. Las operaciones de la CLI para administrar VDI se describen en los comandos de VDI. La representación en disco de los datos varía según el tipo de SR. Una interfaz de complemento de almacenamiento independiente para cada SR, denominada API de SM, administra los datos.

Dispositivos de bloques físicos (PBD)

Los dispositivos de bloques físicos representan la interfaz entre un servidor físico y un SR conectado. Los PBD son objetos de conector que permiten que un SR determinado se asigne a un host. Los PBD almacenan los campos de configuración del dispositivo que se utilizan para conectarse e interactuar con un destino de almacenamiento determinado. Por ejemplo, la configuración del dispositivo NFS incluye la dirección IP del servidor NFS y la ruta asociada que monta el host XenServer. Los objetos PBD administran la conexión en tiempo de ejecución de un SR determinado a un host XenServer determinado. Las operaciones de CLI relacionadas con los PBD se describen en los comandos PBD.

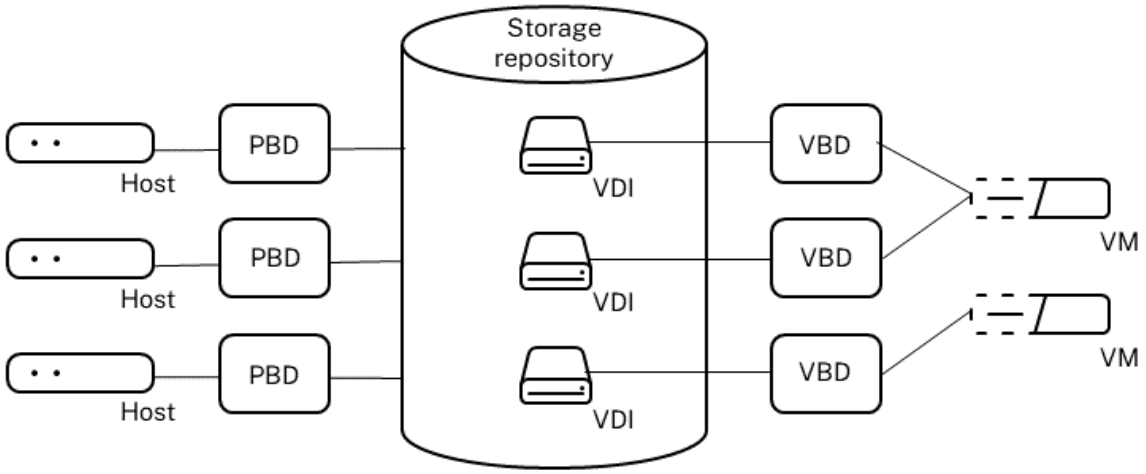
Dispositivos de bloques virtuales (VBD)

Los dispositivos de bloques virtuales son objetos de conector (similares al PBD descrito anteriormente) que permiten asignaciones entre VDI y VM. Además de proporcionar un mecanismo para conectar una VDI a una máquina virtual, las VBD permiten ajustar los parámetros relacionados con la prioridad de E/S del disco y las estadísticas de una VDI determinada, y si esa VDI se puede iniciar. Las operaciones de CLI relacionadas con los VBD se describen en los comandos de VBD.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Resumen de objetos de almacenamiento

La siguiente imagen es un resumen de cómo se relacionan los objetos de almacenamiento presentados hasta el momento:



Formatos de datos de discos virtuales

En general, existen los siguientes tipos de asignación de almacenamiento físico a una VDI:

1. *VHD basado en volúmenes lógicos en un LUN:* el almacenamiento predeterminado basado en bloques de XenServer inserta un administrador de volúmenes lógicos en un disco. Este disco es un dispositivo conectado localmente (LVM) o un LUN conectado a SAN a través de Fibre Channel, iSCSI o SAS. Los VDI se representan como volúmenes dentro del administrador de volúmenes y se almacenan en formato VHD para permitir el aprovisionamiento controlado de nodos de referencia en instantáneas y clones.
2. *QCOW2 basado en archivos en un LUN:* las imágenes de VM se almacenan como archivos de formato QCOW2 de aprovisionamiento fino en un sistema de archivos de disco compartido GFS2 en un LUN conectado a través de un iniciador de software iSCSI o un HBA de hardware.
3. *VHD basado en archivos en un sistema de archivos:* las imágenes de VM se almacenan como archivos en formato VHD de aprovisionamiento fino en un sistema de archivos local no compartido (EXT3/EXT4 tipo SR), un destino NFS compartido (NFS tipo SR) o un destino SMB remoto (SR de tipo SMB).
4. *QCOW2 basado en archivos en un sistema de archivos:* las imágenes de máquina virtual se almacenan como archivos de formato QCOW2 de aprovisionamiento delgado en un sistema de archivos XFS local no compartido.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Tipos de VDI

Para los SR de GFS2 y XFS, se crean VDI de QCOW2.

Para otros tipos de SR, se crean VDI en formato VHD. Puede optar por usar raw en el momento de crear la VDI. Esta opción solo se puede especificar mediante la CLI xe.

> **Nota:**
>
> Si crea una VDI sin procesar en una SR basada en LVM o SR de HBA/LUN por VDI, podría permitir que la máquina virtual propietaria acceda a los datos que formaban parte de una VDI eliminada anteriormente (de cualquier formato) que pertenece a cualquier máquina virtual. Le recomendamos que tenga en cuenta sus requisitos de seguridad antes de usar esta opción.
>
> Los VDI sin procesar en NFS, EXT o SMB SR no permiten el acceso a los datos de los VDI eliminados anteriormente que pertenecen a ninguna VM.

Para comprobar si se creó una VDI con `type=raw`, consulte su asignación de `sm-config`. Los comandos `sr-param-list` y `vdi-param-list` xe se pueden usar respectivamente para este propósito.

Cree un disco virtual sin formato mediante la CLI xe

1. Ejecute el siguiente comando para crear un VDI dado el UUID del SR en el que quiere colocar el disco virtual:

```
xe vdi-create sr-uuid=sr-uuid type=user virtual-size=virtual-size
    \
        name-label=VDI name sm-config:type=raw
<!--NeedCopy-->
```

2. Conecte el nuevo disco virtual a una VM. Use las herramientas de disco dentro de la VM para crear particiones y formatear, o use el disco nuevo. Puede usar el comando `vbd-create` para crear un VBD a fin de asignar el disco virtual a la VM.

Convertir entre formatos VDI

No es posible realizar una conversión directa entre los formatos raw y VHD. En su lugar, puede crear un VDI (ya sea sin procesar, como se describió anteriormente, o VHD) y, a continuación, copiar datos en él desde un volumen existente. Use la CLI xe para asegurarse de que la nueva VDI tenga un tamaño virtual al menos tan grande como la VDI desde la que está copiando. Puede hacerlo comprobando su campo `virtual-size`; por ejemplo, mediante el comando `vdi-param-list`. A continuación, puede conectar esta nueva VDI a una VM y usar su herramienta preferida dentro de la VM para hacer una copia en bloque directa de los datos. Por ejemplo, las herramientas de administración de discos

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

estándar en Windows o el comando dd en Linux. Si el nuevo volumen es un volumen VHD, utilice una herramienta que evite escribir sectores vacíos en el disco. Esta acción puede garantizar que el espacio se utilice de manera óptima en el repositorio de almacenamiento subyacente. Un enfoque de copia basado en archivos puede ser más adecuado.

VDI basados en VHD y basados en QCOW2

Las imágenes VHD y QCOW2 se pueden *encadenar*, lo que permite que dos VDI compartan datos comunes. En los casos en que se clona una VM respaldada por VHD o QCOW2, las VM resultantes comparten los datos comunes en disco en el momento de la clonación. Cada VM procede a realizar sus propios cambios en una versión aislada de copia en escritura de la VDI. Esta función permite que dichas VM se clonen rápidamente a partir de plantillas, lo que facilita el aprovisionamiento y la implementación muy rápidos de nuevas VM.

A medida que las VM y sus VDI asociados se clonan con el tiempo, esto crea árboles de VDI encadenados. Cuando se elimina uno de los VDI de una cadena, XenServer racionaliza los demás VDI de la cadena para eliminar los VDI innecesarios. Este *proceso de fusión se ejecuta de* forma asíncrona. La cantidad de espacio en disco recuperado y el tiempo que se tarda en realizar el proceso dependen del tamaño de la VDI y de la cantidad de datos compartidos.

Los formatos VHD y QCOW2 admiten el *aprovisionamiento ligero*. El archivo de imagen se extiende automáticamente en fragmentos granulares finos a medida que la VM escribe datos en el disco. Para el VHD basado en archivos y QCOW2 basado en GFS2, este enfoque tiene la ventaja considerable de que los archivos de imagen de VM ocupan solo el espacio necesario en el almacenamiento físico. Con VHD basado en LVM, el contenedor de volumen lógico subyacente debe ajustarse al tamaño virtual de la VDI. Sin embargo, el espacio no utilizado en el disco de instancia de copia en escritura subyacente se recupera cuando se produce una instantánea o un clon. La diferencia entre los dos comportamientos se puede describir de la siguiente manera:

- Para las *imágenes VHD basadas en LVM*, los diferentes nodos de disco dentro de la cadena consumen solo la cantidad de datos que se ha escrito en el disco. Sin embargo, los nodos hoja (clones de VDI) permanecen completamente inflados hasta el tamaño virtual del disco. Los nodos hoja de instantáneas (instantáneas de VDI) permanecen desinflados cuando no están en uso y se pueden adjuntar como de solo lectura para preservar la asignación desinflada. Los nodos de instantáneas que están conectados de lectura y escritura se inflan por completo al conectarlos y se desinflan al desconectarse.
- Para los *VHD basados en archivos y las**imágenes QCOW2 basadas en GFS2*, todos los nodos consumen solo la cantidad de datos que se ha escrito. Los archivos de nodo hoja crecen para acomodar los datos a medida que se escriben activamente. Si se asigna una VDI de 100 GB para una máquina virtual y se instala un sistema operativo, el archivo VDI solo tiene el tamaño físico de los datos del sistema operativo en el disco, además de una sobrecarga de metadatos menor.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Al clonar máquinas virtuales basadas en un único VHD o plantilla QCOW2, cada máquina virtual secundaria forma una cadena en la que se escriben nuevos cambios en la nueva máquina virtual. Los bloques antiguos se leen directamente de la plantilla principal. Si la nueva VM se convirtió en una plantilla adicional y se clonaron más VM, la cadena resultante reduce el rendimiento. XenServer admite una longitud de cadena máxima de 30. No se acerque a este límite sin una buena razón. En caso de duda, "copie"la máquina virtual mediante XenCenter o utilice el comando `vm-copy`, que restablece la longitud de la cadena a 0.

Notas específicas de VHD sobre la fusión Solo hay un proceso de coalescencia activo para una SR. Este hilo de proceso se ejecuta en el coordinador del grupo SR.

Si tiene máquinas virtuales críticas ejecutándose en el coordinador del grupo, puede tomar las siguientes medidas para mitigar la lentitud ocasional de las E/S:

- Migrar la máquina virtual a un host que no sea el coordinador del grupo de SR
- Establezca la prioridad de E/S del disco en un nivel superior y ajuste el programador. Para obtener más información, consulte Priorización de solicitudes de E/S de discos virtuales.

---

layout: doc
description: Create storage repositories for use in your XenServer environment.—

Crear un repositorio de almacenamiento

Puede utilizar el asistente para **nuevos repositorios de almacenamiento** de XenCenter para crear repositorios de almacenamiento (SR). El asistente lo guía a través de los pasos de configuración. También puede usar la CLI y el comando `sr-create`. El comando `sr-create` crea un RA en el sustrato de almacenamiento (que puede destruir cualquier dato existente). También crea el objeto de API de SR y un registro PBD correspondiente, lo que permite a las máquinas virtuales utilizar el almacenamiento. Al crear correctamente el SR, el PBD se conecta automáticamente. Si se establece el `shared=true` indicador SR, se crea y conecta un registro PBD para cada XenServer del grupo de recursos.

Si está creando un SR para almacenamiento basado en IP (iSCSI o NFS), puede configurar una de las siguientes opciones como red de almacenamiento: La NIC que administra el tráfico de administración o una NIC nueva para el tráfico de almacenamiento. Para asignar una dirección IP a una NIC, consulte Configurar una NIC de almacenamiento dedicada.

Todos los tipos de XenServer SR admiten el cambio de tamaño de la VDI, la clonación rápida y la creación de instantáneas. Los SR basados en el tipo de SR de LVM (local, iSCSI o HBA) proporcionan

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

aprovisionamiento ligero para los nodos primarios ocultos y de instantáneas. Los otros tipos de SR (EXT3/EXT4, NFS, GFS2) admiten el aprovisionamiento controlado completo, incluso para los discos virtuales que están activos.

> **Advertencias:**
>
> - Cuando los VDI de VHD no están conectados a una máquina virtual, por ejemplo, para una instantánea de VDI, se almacenan como aprovisionados con poca cantidad de forma predeterminada. Si intenta volver a conectar la VDI, asegúrese de que haya suficiente espacio en disco disponible para que la VDI se aprovisione de manera abundante. Los clones de VDI se aprovisionan en gran medida.
> - XenServer no admite instantáneas en el nivel de SAN externo de un LUN para ningún tipo de SR.
> - No intente crear un SR en el que el ID de LUN del LUN de destino sea superior a 255. Asegúrese de que su objetivo exponga el LUN con un ID de LUN inferior o igual a 255 antes de usar este LUN para crear un SR.
> - Si usa aprovisionamiento controlado en una SR basada en archivos, asegúrese de supervisar el espacio libre en su SR. Si el uso de SR aumenta hasta el 100%, fallan las escrituras posteriores de las VM. Estas escrituras fallidas pueden provocar que la VM se congele o se bloquee.

Los tamaños máximos de VDI admitidos son:

Formato de repositorio de almacenamiento	Tamaño máximo de VDI
EXT3/EXT4	2 TiB
GFS2 (con iSCSI o HBA)	16 TiB
XFS	16 TiB
LVM	2 TiB
LVMoFCOE (en desuso)	2 TiB
LVMoHBA	2 TiB
LVMoiSCSI	2 TiB
NFS	2 TiB
SMB	2 TiB

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

LVM local

El tipo LVM local presenta los discos dentro de un grupo de volúmenes conectado localmente.

De forma predeterminada, XenServer usa el disco local del host físico en el que está instalado. El Administrador de volúmenes lógicos de Linux (LVM) se usa para administrar el almacenamiento de VM. Un VDI se implementa en formato VHD en un volumen lógico LVM del tamaño especificado.

> **Nota:**
>
> El tamaño de bloque de un LVM LUN debe ser de 512 bytes. Para usar el almacenamiento con bloques físicos de 4 KB, el almacenamiento también debe admitir la emulación de bloques de asignación de 512 bytes (el tamaño del bloque lógico debe ser de 512 bytes).

Consideraciones de rendimiento de LVM

La funcionalidad de copia instantánea y clonación rápida para los SR basados en LVM conlleva una sobrecarga de rendimiento inherente. Cuando se requiere un rendimiento óptimo, XenServer admite la creación de VDI en formato *RAW* además del formato VHD predeterminado. La funcionalidad de instantáneas de XenServer no se admite en los VDI sin procesar.

> **Advertencia:**
>
> No intente hacer una instantánea de una máquina virtual que tenga discos `type=raw` conectados. Esta acción puede provocar la creación de una instantánea parcial. En esta situación, puede identificar los VDI de instantáneas huérfanos comprobando el campo `snapshot-of` y, a continuación, eliminándolos.

Creación de una SR de LVM local

Una SR de LVM se crea de forma predeterminada en la instalación del host.

Los parámetros de configuración del dispositivo para los SR de LVM son:

Nombre del parámetro	Descripción	¿Obligatorio?
`device`	Nombre del dispositivo en el host local que se utilizará para el SR. También puede proporcionar una lista de nombres separados por comas.	Sí

Para crear una SR LVM local en `/dev/sdb`, utilice el siguiente comando.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    xe sr-create host-uuid=valid_uuid content-type=user \
    name-label="Example Local LVM SR" shared=false \
    device-config:device=/dev/sdb type=lvm
<!--NeedCopy-->
```

EXT3/EXT4 local

El uso de EXT3/EXT4 permite el aprovisionamiento controlado en almacenamiento local. Sin embargo, el tipo de repositorio de almacenamiento predeterminado es LVM, ya que proporciona un rendimiento de escritura consistente y evita la sobreasignación de almacenamiento. Si usa EXT3/EXT4, es posible que vea un rendimiento reducido en los siguientes casos:

- Al llevar a cabo operaciones del ciclo de vida de VM, como crear y suspender/reanudar VM
- Al crear archivos grandes desde la VM

Los SR EXT3/EXT4 del disco local deben configurarse mediante la CLI de XenServer.

El hecho de que un EXT SR local utilice EXT3 o EXT4 depende de la versión de XenServer que lo haya creado:

- Si creó el EXT SR local en una versión anterior de Citrix Hypervisor o XenServer y, a continuación, lo actualizó a XenServer 8, utilizará EXT3.
- Si creó el EXT SR local en XenServer 8, utilizará EXT4.

> **Nota:**
>
> El tamaño de bloque de un disco EXT3/EXT4 debe ser de 512 bytes. Para usar el almacenamiento con bloques físicos de 4 KB, el almacenamiento también debe admitir la emulación de bloques de asignación de 512 bytes (el tamaño del bloque lógico debe ser de 512 bytes).

Creación de una SR EXT4 local (`ext`)

Parámetros de configuración del dispositivo para SRs ext:

Nombre del parámetro	Descripción	¿Obligatorio?
`device`	Nombre del dispositivo en el host local que se utilizará para el SR. También puede proporcionar una lista de nombres separados por comas.	Sí

Para crear una SR EXT4 local en `/dev/sdb`, utilice el siguiente comando:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    xe sr-create host-uuid=valid_uuid content-type=user \
       name-label="Example Local EXT4 SR" shared=false \
       device-config:device=/dev/sdb type=ext
<!--NeedCopy-->
```

XFS local

El uso de XFS permite un aprovisionamiento ligero en el almacenamiento local. El tipo XFS local permite crear dispositivos de almacenamiento local con bloques físicos de 4 KB sin necesidad de un tamaño de bloque lógico de 512 bytes.

Creación de un SR de XFS local

Parámetros de configuración del dispositivo para los SR de XFS:

Nombre del parámetro	Descripción	¿Obligatorio?
`device`	Nombre del dispositivo en el host local que se utilizará para el SR. También puede proporcionar una lista de nombres separados por comas.	Sí

Para crear un SR de XFS local en `/dev/sdb`, use el siguiente comando:

```
    xe sr-create host-uuid=valid_uuid content-type=user \
       name-label="Example Local XFS SR" shared=false \
       device-config:device=/dev/sdb type=xfs
<!--NeedCopy-->
```

udev

El tipo udev representa los dispositivos conectados mediante el administrador de dispositivos udev como VDI.

XenServer tiene dos SR de tipo udev que representan almacenamiento extraíble. Una es para el disco CD o DVD de la unidad física de CD o DVD-ROM del host XenServer. La otra es para un dispositivo USB conectado a un puerto USB del host XenServer. Los VDI que representan los medios van y vienen a medida que se insertan y extraen discos o memorias USB.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ISO

El tipo ISO maneja las imágenes de CD almacenadas como archivos en formato ISO. Este tipo de SR es útil para crear bibliotecas ISO compartidas.

Están disponibles los siguientes tipos de ISO SR:

- `nfs_iso`: El tipo NFS ISO SR gestiona las imágenes de CD almacenadas como archivos en formato ISO disponibles como un recurso compartido NFS.
- `cifs`: El tipo SR de Windows File Sharing (SMB/CIFS) gestiona las imágenes de CD almacenadas como archivos en formato ISO disponibles como recursos compartidos de Windows (SMB/CIFS).

Si no especifica el tipo de almacenamiento que se va a usar para el SR, XenServer usa el parámetro de configuración del `location`dispositivo para decidir el tipo.

Parámetros de configuración del dispositivo para los SR ISO:

Nombre del parámetro	Descripción	¿Obligatorio?
`location`	Camino al monte.	Sí
`type`	Tipo de almacenamiento que se utilizará para el SR: `cifs`o `nfs_iso`.	No
`nfsversion`	Para el tipo de almacenamiento NFS, la versión del protocolo NFS que se va a utilizar: 3, 4, 4.0 o 4.1.	No
`vers`	Para el tipo de almacenamiento CIFS/SMB, la versión de SMB que se utilizará: 1.0 o 3.0. El valor predeterminado es 3.0.	No
`username`	Para el tipo de almacenamiento CIFS/SMB, si se requiere un nombre de usuario para el servidor de archivos de Windows.	No
`cifspassword_secret`	(Recomendado) Para el tipo de almacenamiento CIFS/SMB, puede pasar un secreto en lugar de una contraseña al servidor de archivos de Windows.	No

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	¿Obligatorio?
`cifspassword`	Para el tipo de almacenamiento CIFS/SMB, si se requiere una contraseña para el servidor de archivos de Windows. Le recomendamos que utilice el `cifspassword_secret` parámetro en su lugar.	No

> **Nota:**
>
> Al ejecutar el `sr-create`comando, se recomienda utilizar el argumento en lugar `device-config:cifspassword_secret`de especificar la contraseña en la línea de comandos. Para obtener más información, consulte Secretos.

Para los repositorios de almacenamiento que almacenan una biblioteca de ISO, el `content-type` parámetro se debe establecer en `iso`, por ejemplo:

```
1     xe sr-create host-uuid=valid_uuid content-type=iso  type=iso name-
          label="Example ISO SR" \
2       device-config:location=<path_to_mount> device-config:type=nfs_iso
3 <!--NeedCopy-->
```

Puede usar NFS o SMB para montar la ISO SR. Para obtener más información sobre el uso de estos tipos de SR, consulte NFS y SMB .

Le recomendamos que utilice la versión 3 de SMB para montar ISO SR en el servidor de archivos de Windows. La versión 3 se selecciona de forma predeterminada porque es más segura y sólida que la versión 1.0 para pymes. Sin embargo, puede montar ISO SR mediante SMB versión 1 con el siguiente comando:

```
1      xe sr-create content-type=iso type=iso shared=true device-config:
          location=<path_to_mount>
2      device-config:username=<username> device-config:cifspassword=<
          password> \
3      device-config:type=cifs device-config:vers=1.0 name-label="Example
           ISO SR"
4 <!--NeedCopy-->
```

Compatibilidad con iSCSI de software

XenServer admite SR compartidos en los LUNs iSCSI. iSCSI se admite mediante el iniciador iSCSI de software iSCSI abierto o mediante un adaptador de bus de host (HBA) iSCSI compatible. Los pasos

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

para usar HBA iSCSI son idénticos a los pasos para los HBA de canal de fibra. Ambos conjuntos de pasos se describen en Crear un LVM compartido a través de Fibre Channel, Fibre Channel a través de Ethernet/HBA iSCSI o SAS SR.

La compatibilidad con iSCSI compartida mediante el iniciador iSCSI de software se implementa en función de Linux Volume Manager (LVM). Esta función proporciona los mismos beneficios de rendimiento que proporcionan los VDI de LVM en la carcasa del disco local. Los SR iSCSI compartidos que utilizan un iniciador de host basado en software pueden contribuir a la agilidad de las máquinas virtuales mediante la migración en vivo: las máquinas virtuales se pueden iniciar en cualquier host de XenServer de un grupo de recursos y migrar entre ellas sin que se note un tiempo de inactividad.

Los SR iSCSI utilizan todo el LUN especificado en el momento de la creación y no pueden abarcar más de un LUN. Se proporciona soporte CHAP para la autenticación de clientes, tanto durante la inicialización del path de datos como durante las fases de descubrimiento de LUN.

> **Nota:**
>
> El tamaño de bloque de un LUN iSCSI debe ser de 512 bytes. Para usar el almacenamiento con bloques físicos de 4 KB, el almacenamiento también debe admitir la emulación de bloques de asignación de 512 bytes (el tamaño del bloque lógico debe ser de 512 bytes).

Configuración iSCSI del host de XenServer

Todos los iniciadores y destinos iSCSI deben tener un nombre único para garantizar que se puedan identificar de forma única en la red. Un iniciador tiene una dirección de iniciador iSCSI y un destino tiene una dirección de destino iSCSI. En conjunto, estos nombres se denominan nombres calificados iSCSI o IQN.

Los hosts XenServer admiten un único iniciador iSCSI que se crea y configura automáticamente con un IQN aleatorio durante la instalación del host. El iniciador único se puede usar para conectarse a varios destinos iSCSI al mismo tiempo.

Los destinos iSCSI suelen proporcionar control de acceso mediante listas IQN de iniciadores iSCSI. Todos los objetivos o LUNs iSCSI a los que accede el host de XenServer deben estar configurados para permitir el acceso del IQN iniciador del host. Del mismo modo, los objetivos/LUN que se van a utilizar como RA iSCSI compartidos deben configurarse para permitir el acceso de todos los IQN de host en el grupo de recursos.

> **Nota:**
>
> Los destinos iSCSI que no proporcionan control de acceso suelen restringir el acceso del LUN a un único iniciador para garantizar la integridad de los datos. Si se utiliza un LUN iSCSI como SR compartido entre varios hosts de un grupo, asegúrese de que el acceso de varios iniciadores esté habilitado para el LUN especificado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El valor del IQN del host de XenServer se puede ajustar mediante XenCenter o mediante la CLI con el siguiente comando cuando se utiliza el iniciador de software iSCSI:

```
1     xe host-param-set uuid=valid_host_id other-config:iscsi_iqn=
         new_initiator_iqn
2 <!--NeedCopy-->
```

> **Advertencia:**
>
> - Cada objetivo e iniciador iSCSI debe tener un IQN único. Si se utiliza un identificador IQN no único, puede producirse corrupción de datos o denegación de acceso a LUN.
> - No cambie el IQN del host de XenServer con los SR iSCSI conectados. Si lo hace, puede provocar fallas en la conexión con nuevos objetivos o SR existentes.

Almacenamiento FCoE de software (en desuso)

El software FCoE proporciona un marco estándar en el que los proveedores de hardware pueden conectar su NIC compatible con FCoE y obtener los mismos beneficios de un FCoE basado en hardware. Esta función elimina la necesidad de utilizar costosos HBA.

> **Nota:**
>
> El software FCoE está en desuso y se eliminará en una versión futura.

Antes de crear un almacenamiento FCoE de software, complete manualmente la configuración requerida para exponer un LUN al host. Esta configuración incluye la configuración de la estructura FCoE y la asignación de LUN al nombre mundial público (PWWN) de su SAN. Después de completar esta configuración, el LUN disponible se monta en el CNA del host como un dispositivo SCSI. El dispositivo SCSI se puede usar para acceder al LUN como si fuera un dispositivo SCSI conectado localmente. Para obtener información sobre cómo configurar el conmutador físico y el arreglo de discos para admitir FCoE, consulte la documentación proporcionada por el proveedor.

> **Nota:**
>
> El software FCoE se puede utilizar con Open vSwitch y Linux Bridge como back-end de la red.

Crear una SR de FCoE de software

Antes de crear una SR de FCoE de software, los clientes deben asegurarse de que haya NIC compatibles con FCoE conectadas al host.

Los parámetros de configuración del dispositivo para los SR de FCoE son:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	¿Obligatorio?
SCSIid	El identificador del bus SCSI del LUN de destino	Sí

Ejecute el siguiente comando para crear una SR de FCoE compartida:

```
    xe sr-create type=lvmofcoe \
    name-label="FCoE SR" shared=true device-config:SCSIid=SCSI_id
<!--NeedCopy-->
```

Adaptadores de bus host (HBA) de hardware

Esta sección cubre varias operaciones necesarias para administrar HBA SAS, Fibre Channel e iSCSI.

Configuración de HBA iSCSI QLogic de ejemplo

Para obtener más información sobre la configuración de los HBAs iSCSI y Fibre Channel QLogic, consulte el sitio web de Cavium.

Una vez que el HBA esté instalado físicamente en el host de XenServer, siga los siguientes pasos para configurar el HBA:

1. Establezca la configuración de redes IP para el HBA. En este ejemplo se asume el puerto DHCP y HBA 0. Especifique los valores adecuados si utiliza direcciones IP estáticas o un HBA multipuerto.

   ```
   /opt/QLogic_Corporation/SANsurferiCLI/iscli -ipdhcp 0
   <!--NeedCopy-->
   ```

2. Agregue un destino iSCSI persistente al puerto 0 del HBA.

   ```
   /opt/QLogic_Corporation/SANsurferiCLI/iscli -pa 0
      iscsi_target_ip_address
   <!--NeedCopy-->
   ```

3. Ejecute el comando `sr-probe` xe para forzar un nuevo análisis del Controller HBA y mostrar los LUNs disponibles. Para obtener más información, consulte Probar una SR y Crear una LVM compartida a través de Fibre Channel, Fibre Channel a través de Ethernet/HBA iSCSI o SAS SR.

Eliminar entradas de dispositivos SAS, FC o iSCSI basados en HBA

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Este paso no es obligatorio. Recomendamos que solo los usuarios avanzados realicen este proceso si es necesario.

Cada LUN basado en HBA tiene una entrada de ruta de dispositivo global correspondiente en `/dev/disk/by-scsibus` en el formato `<SCSIid>-<adapter>:<bus>:<target>:<lun>` y una ruta de dispositivo estándar en `/dev`. Para eliminar las entradas del dispositivo para los LUN que ya no se utilizan como SR, siga los siguientes pasos:

1. Use `sr-forget` o `sr-destroy`, según corresponda, para eliminar el SR de la base de datos del host de XenServer. Consulte Eliminar SR para obtener más información.
2. Elimine la configuración de zonas dentro de la SAN para el LUN deseado al host deseado.
3. Ejecute el comando `sr-probe` para determinar los valores ADAPTER, BUS, TARGET y LUN correspondientes al LUN que se va a quitar. Para obtener más información, sondee una SR.
4. Elimine las entradas del dispositivo con el siguiente comando:

```
echo "1" > /sys/class/scsi_device/adapter:bus:target:lun/device/
   delete
<!--NeedCopy-->
```

> **Advertencia:**
>
> Asegúrese de que está seguro de qué LUN va a eliminar. La eliminación accidental de un LUN requerido para la operación del host, como el dispositivo de arranque o raíz, hace que el host quede inutilizable.

Almacenamiento LVM compartido

El tipo LVM compartido representa los discos como volúmenes lógicos dentro de un grupo de volúmenes creado en un LUN iSCSI (FC o SAS).

> **Nota:**
>
> El tamaño de bloque de un LUN iSCSI debe ser de 512 bytes. Para usar el almacenamiento con bloques físicos de 4 KB, el almacenamiento también debe admitir la emulación de bloques de asignación de 512 bytes (el tamaño del bloque lógico debe ser de 512 bytes).

Cree un LVM compartido a través de SR iSCSI mediante el iniciador iSCSI de software

Parámetros de configuración del dispositivo para SRs LVMoiSCSI:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	¿Obligatorio?
`target`	La dirección IP o el nombre de host del archivador iSCSI que aloja el SR. También puede ser una lista de valores separados por comas.	Sí
`targetIQN`	La dirección de destino IQN del archivador iSCSI que aloja el SR	Sí
`SCSIid`	El identificador del bus SCSI del LUN de destino	Sí
`chapuser`	El nombre de usuario que se utilizará para la autenticación CHAP	No
`chappassword_secret`	(Recomendado) ID secreto de la contraseña que se utilizará para la autenticación CHAP. Pase un secreto en lugar de una contraseña.	No
`chappassword`	La contraseña que se utilizará para la autenticación CHAP. Le recomendamos que utilice el `chappassword_secret` parámetro en su lugar.	No
`port`	El número de puerto de red en el que se consultará el destino	No
`usediscoverynumber`	El índice de registros iSCSI específico que se va a utilizar	No
`incoming_chapuser`	El nombre de usuario que el filtro iSCSI utiliza para autenticarse en el host	No
`incoming_chappassword`	La contraseña que utiliza el filtro iSCSI para autenticarse en el host	No

> **Nota:**
>
> Al ejecutar el `sr-create`comando, se recomienda utilizar el argumento en lugar `device-config:chappassword_secret`de especificar la contraseña en la línea de comandos. Para

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> obtener más información, consulte Secretos.

Para crear una SR iSCSI LVMoiSCSI compartida en un LUN específico de un destino iSCSI, use el siguiente comando.

```
1     xe sr-create host-uuid=valid_uuid content-type=user \
2     name-label="Example shared LVM over iSCSI SR" shared=true \
3     device-config:target=target_ip= device-config:targetIQN=target_iqn=
          \
4     device-config:SCSIid=scsci_id \
5     type=lvmoiscsi
6 <!--NeedCopy-->
```

Cree un LVM compartido a través de Fibre Channel, Fibre Channel a través de Ethernet/HBA iSCSI o SAS SR

Los SR de tipo LVMoHBA se pueden crear y administrar mediante la CLI xe o XenCenter.

Parámetros de configuración del dispositivo para SRs de LVMoHBA:

Nombre del parámetro	Descripción	¿Obligatorio?
SCSIid	Identificador SCSI del dispositivo	Sí

Para crear una SR LVMoHBA compartida, lleve a cabo los siguientes pasos en cada host del grupo:

1. Divida uno o más LUNs en cada host de XenServer del grupo. Este proceso es muy específico para el equipo SAN en uso. Para obtener más información, consulte la documentación de su SAN.
2. Si es necesario, utilice la CLI del HBA incluida en el host de XenServer para configurar el HBA:
   - Emulex: /bin/sbin/ocmanager
   - FC de QLogic: /opt/QLogic_Corporation/SANsurferCLI
   - iSCSI de QLogic: /opt/QLogic_Corporation/SANsurferiCLI

   Para ver un ejemplo de la configuración de HBA iSCSI de QLogic, consulte *Adaptadores de bus de host (HBA) de hardware* en la sección anterior. Para obtener más información sobre los HBAs Fibre Channel e iSCSI, consulte los sitios web Broadcom y Cavium.
3. Utilice el comando sr-probe para determinar la ruta de acceso del dispositivo global del LUN de HBA. El comando sr-probe obliga a volver a analizar los HBAs instalados en el sistema para detectar los nuevos LUNs que se han asignado a una zona en el host. El comando devuelve una

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

lista de propiedades para cada LUN encontrado. Especifique el parámetro `host-uuid` para asegurarse de que el sondeo se produce en el host deseado.

La ruta global del dispositivo que se devuelve como propiedad `<path>` es común en todos los hosts del grupo. Por lo tanto, esta ruta debe utilizarse como valor para el parámetro `device-config:device` al crear el SR.

Si hay varios LUN presentes, utilice el proveedor, el tamaño del LUN, el número de serie del LUN o el ID SCSI de la propiedad `<path>` para identificar el LUN deseado.

```
xe sr-probe type=lvmohba \
host-uuid=1212c7b3-f333-4a8d-a6fb-80c5b79b5b31
Error code: SR_BACKEND_FAILURE_90
Error parameters: , The request is missing the device
   parameter, \
<?xml version="1.0" ?>
<Devlist>
    <BlockDevice>
        <path>
            /dev/disk/by-id/scsi-360
               a98000686669496734463876653 36f
        </path>
        <vendor>
            HITACHI
        </vendor>
        <serial>
            730157980002
        </serial>
        <size>
            80530636800
        </size>
        <adapter>
            4
        </adapter>
        <channel>
            0
        </channel>
        <id>
            4
        </id>
        <lun>
            2
        </lun>
        <hba>
            qla2xxx
        </hba>
    </BlockDevice>
    <Adapter>
        <host>
            Host4
        </host>
        <name>
            qla2xxx
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
            </name>
            <manufacturer>
                QLogic HBA Driver
            </manufacturer>
            <id>
                4
            </id>
        </Adapter>
    </Devlist>
<!--NeedCopy-->
```

4. En el coordinador de agrupaciones, cree el SR. Especifique la ruta de acceso global del dispositivo devuelta en la propiedad <path> de sr-probe. Los PBD se crean y conectan automáticamente para cada host del grupo.

```
    xe sr-create host-uuid=valid_uuid \
    content-type=user \
    name-label="Example shared LVM over HBA SR" shared=true \
    device-config:SCSIid=device_scsi_id type=lvmohba
<!--NeedCopy-->
```

> **Nota:**
>
> Puede utilizar la función Repair Storage Repair XenCenter para volver a intentar la creación de PBD y la conexión de partes de la operación sr-create. Esta función puede resultar valiosa en los casos en que la división en zonas del LUN era incorrecta para uno o más hosts de un grupo cuando se creó el SR. Corrija la división en zonas para los hosts afectados y utilice la función Reparar repositorio de almacenamiento en lugar de eliminar y volver a crear el SR.

Almacenamiento en bloques GFS2 compartido con aprovisionamiento fino

El Provisioning ligero utiliza mejor el almacenamiento disponible al asignar espacio de almacenamiento en disco a los VDI a medida que los datos se escriben en el disco vDisk, en lugar de asignar el tamaño virtual completo del VDI por adelantado. El Provisioning ligero le permite reducir significativamente la cantidad de espacio necesario en un arreglo de discos de almacenamiento compartido y, con ello, su coste total de propiedad (TCO).

El aprovisionamiento controlado para el almacenamiento en bloque compartido es de particular interés en los siguientes casos:

- Quieres aumentar la eficiencia del espacio. Las imágenes están escasamente asignadas y no densamente asignadas.
- Desea reducir la cantidad de operaciones de E/S por segundo en su cabina de almacenamiento. GFS2 SR es el primer tipo de SR que admite el almacenamiento en caché de lectura de almacenamiento en almacenamiento en bloque compartido.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Se usa una imagen base común para varias máquinas virtuales. Por lo general, las imágenes de las VM individuales utilizarán incluso menos espacio.
- Usas instantáneas. Cada instantánea es una imagen y ahora cada imagen es escasa.
- Su almacenamiento no admite NFS y solo admite almacenamiento en bloque. Si su almacenamiento admite NFS, le recomendamos que utilice NFS en lugar de GFS2.
- Desea crear VDI con un tamaño superior a 2 TiB. La GFS2 SR admite VDI de hasta 16 TiB de tamaño.

> **Nota:**
>
> Recomendamos no usar una SR de GFS2 con una VLAN debido a un problema conocido por el que no se pueden agregar ni quitar hosts en una agrupación en clústeres si la red del clúster está en una VLAN que no es de administración.

El tipo SR GFS2 compartido crea un sistema de archivos GFS2 en un LUN iSCSI o HBA. Los VDI se almacenan en el GFS2 SR como archivos en el formato de imagen QCOW2.

Para obtener más información sobre el uso del almacenamiento GFS2, consulte Almacenamiento en bloques GFS2 compartido con aprovisionamiento fino.

NFS y SMB

Los recursos compartidos en servidores NFS (que admiten cualquier versión de NFSv4 o NFSv3) o en servidores SMB (que admiten SMB 3) se pueden usar inmediatamente como SR para discos virtuales. Los VDI solo se almacenan en formato VHD de Microsoft. Además, dado que estos SR se pueden compartir, los VDI almacenados en SR compartidos permiten:

- Las máquinas virtuales se iniciarán en cualquier host de XenServer de un grupo de recursos
- Migración de máquinas virtuales entre hosts de XenServer en un grupo de recursos mediante migración en vivo (sin tiempos de inactividad apreciables)

> **Importante:**
>
> - La compatibilidad con SMB3 se limita a la capacidad de conectarse a un recurso compartido mediante el protocolo 3. Las funciones adicionales, como la conmutación por error transparente, dependen de la disponibilidad de las funciones en el núcleo Linux original y no se admiten en XenServer 8.
> - XenServer no admite SMB en clúster.
> - Para NFSv4, solo AUTH_SYS se admite el tipo de autenticación.
> - El almacenamiento para pequeñas y medianas empresas está disponible para los clientes de XenServer Premium Edition.
> - Se recomienda encarecidamente para el almacenamiento NFS y SMB que se utilice una red

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de almacenamiento dedicada, utilizando al menos dos enlaces conectados, idealmente a conmutadores de red independientes con fuentes de alimentación redundantes.
- Cuando utilice el almacenamiento SMB, no extraiga el recurso compartido del almacenamiento antes de desconectar el SMB SR.

Los VDI almacenados en SR basados en archivos se *aprovisionan con poca frecuencia*. El archivo de imagen se asigna a medida que la VM escribe datos en el disco. Este enfoque tiene la ventaja considerable de que los archivos de imagen de VM solo ocupan tanto espacio en el almacenamiento como se requiere. Por ejemplo, si se asigna una VDI de 100 GB para una máquina virtual y se instala un sistema operativo, el archivo VDI solo refleja el tamaño de los datos del sistema operativo escritos en el disco en lugar de los 100 GB completos.

Los archivos VHD también se pueden encadenar, lo que permite que dos VDI compartan datos comunes. En los casos en que se clona una máquina virtual basada en archivos, las máquinas virtuales resultantes comparten los datos en disco comunes en el momento de la clonación. Cada VM procede a realizar sus propios cambios en una versión aislada de copia en escritura de la VDI. Esta función permite que las VM basadas en archivos se clonen rápidamente a partir de plantillas, lo que facilita el aprovisionamiento y la implementación muy rápidos de nuevas VM.

Nota:

La longitud máxima admitida de las cadenas de VHD es de 30.

Las implementaciones de SR y VHD basadas en archivos en XenServer asumen que tienen el control total sobre el directorio SR del servidor de archivos. Los administradores no deben modificar el contenido del directorio de SR, ya que esta acción puede dañar el contenido de los VDI.

XenServer se ha ajustado para un almacenamiento de clase empresarial que utiliza RAM no volátil para proporcionar un reconocimiento rápido de las solicitudes de escritura y, al mismo tiempo, mantener un alto grado de protección de los datos contra errores. XenServer se ha probado exhaustivamente con dispositivos de almacenamiento FAS2020 y FAS3210 de Network Appliance, mediante Data OnTap 7.3 y 8.1

Advertencia:

Como los VDI en SR basados en archivos se crean como aprovisionamiento controlado, los administradores deben asegurarse de que los SR basados en archivos tengan suficiente espacio en disco para todos los VDI requeridos. Los hosts de XenServer no exigen que haya espacio necesario para los VDI en los SR basados en archivos.

Asegúrese de supervisar el espacio libre en su SR. Si el uso de SR aumenta hasta el 100%, fallan las escrituras posteriores de las VM. Estas escrituras fallidas pueden provocar que la VM se congele o se bloquee.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Crear una SR de NFS compartida (NFS)

Para crear una SR de NFS, debe proporcionar el nombre de host o la dirección IP del servidor NFS. Puede crear el RA en cualquier ruta de destino válida; use el comando `sr-probe` para mostrar una lista de rutas de destino válidas exportadas por el servidor.

En los escenarios en los que XenServer se usa con almacenamiento de gama baja, espera con cautela a que se acuse de recibo de todas las escrituras antes de pasar las confirmaciones a las máquinas virtuales. Este enfoque implica un coste de rendimiento notable y podría resolverse configurando el almacenamiento para que presente el punto de montaje SR como una exportación en modo asíncrono. Las exportaciones asíncronas reconocen escrituras que no están realmente en el disco. Considere cuidadosamente los riesgos de fracaso en estas situaciones.

> **Nota:**
>
> El servidor NFS debe estar configurado para exportar la ruta especificada a todos los hosts del grupo. Si no se realiza esta configuración, se produce un error en la creación de la SR y la conexión del registro PBD.

La implementación de NFS de XenServer usa TCP de forma predeterminada. Si su situación lo permite, puede configurar la implementación para que use UDP en casos en los que pueda haber un beneficio de rendimiento. Para realizar esta configuración, al crear un SR, especifique `useUDP=true` en el parámetro `device-config`.

Los siguientes parámetros `device-config` se utilizan con los SR de NFS:

Nombre del parámetro	Descripción	¿Obligatorio?
`server`	Dirección IP o nombre de host del servidor NFS	Sí
`serverpath`	Ruta, incluido el punto de montaje NFS, al servidor NFS que aloja el SR	Sí

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	¿Obligatorio?
`nfsversion`	Especifica la versión de NFS que se va a utilizar. Si especifica `nfsversion="4"`, el SR usa NFS v4.0, v4.1 o v4.2, según lo que esté disponible. Si quiere seleccionar una versión más específica de NFS, puede especificar `nfsversion="4.0"`, etc. Solo se puede especificar un valor para `nfsversion`.	No
`useUDP`	Configure el SR para que utilice UDP en lugar del TCP predeterminado.	No

Por ejemplo, para crear un SR de NFS compartido el `192.168.1.10:/export1`, utilizando cualquier versión 4 de NFS que esté disponible en el archivador, utilice el siguiente comando:

```
1     xe sr-create content-type=user \
2     name-label="shared NFS SR" shared=true \
3     device-config:server=192.168.1.10 device-config:serverpath=/export1
          type=nfs \
4     device-config:nfsversion="4"
5 <!--NeedCopy-->
```

Para crear un SR de NFS no compartido `192.168.1.10:/export1`, utilizando específicamente la versión 4.0 de NFS, ejecute el siguiente comando:

```
1     xe sr-create host-uuid=host_uuid content-type=user \
2     name-label="Non-shared NFS SR" \
3     device-config:server=192.168.1.10 device-config:serverpath=/export1
          type=nfs \
4     device-config:nfsversion="4.0"
5 <!--NeedCopy-->
```

Crear una SR de SMB compartida (SMB)

Para crear una SR de SMB, proporcione el nombre de host o la dirección IP del servidor SMB, la ruta completa del recurso compartido exportado y las credenciales apropiadas.

Parámetros de configuración de dispositivos para SR de SMB:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	¿Obligatorio?
`server`	Ruta completa para compartir en el servidor	Sí
`username`	Cuenta de usuario con acceso a RW para compartir	Opcional
`password_secret`	(Recomendado) ID secreto para la contraseña de la cuenta de usuario, que se puede usar en lugar de la contraseña.	Opcional
`password`	Contraseña de la cuenta de usuario. Le recomendamos que utilice el parámetro en su lugar`password_secret`.	Opcional

> **Nota:**
>
> Al ejecutar el `sr-create`comando, se recomienda utilizar el argumento en lugar `device-config:password_secret`de especificar la contraseña en la línea de comandos. Para obtener más información, consulte Secretos.

Por ejemplo, para crear un RA SMB compartido en `192.168.1.10:/share1`, use el siguiente comando:

```
1     xe sr-create content-type=user \
2     name-label="Example shared SMB SR" shared=true \
3     device-config:server=//192.168.1.10/share1 \
4     device-config:username=valid_username device-config:password_secret
         =valid_password_secret type=smb
5 <!--NeedCopy-->
```

Para crear una SR de SMB no compartida, ejecute el siguiente comando:

```
1     xe sr-create host-uuid=host_uuid content-type=user \
2     name-label="Non-shared SMB SR" \
3     device-config:server=//192.168.1.10/share1 \
4     device-config:username=valid_username device-config:password_secret
         =valid_password_secret type=smb
5 <!--NeedCopy-->
```

HBA LVM sobre hardware

El tipo de HBA LVM sobre hardware representa los discos como VHD en volúmenes lógicos dentro de un grupo de volúmenes creado en un LUN de HBA que proporciona, por ejemplo, soporte iSCSI o FC

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

basado en hardware.

Los hosts XenServer admiten SAN Fibre Channel a través de adaptadores de bus de host (HBA) Emulex o QLogic. Toda la configuración de canal de fibra requerida para exponer un LUN de canal de fibra al host debe completarse manualmente. Esta configuración incluye los dispositivos de almacenamiento, los dispositivos de red y el HBA dentro del host de XenServer. Una vez completada toda la configuración de FC, el HBA expone al host un dispositivo SCSI respaldado por el LUN de canal de fibra. El dispositivo SCSI se puede usar para acceder al LUN de canal de fibra como si fuera un dispositivo SCSI conectado localmente.

Use el comando `sr-probe` para enumerar los dispositivos SCSI respaldados por LUN presentes en el host. Este comando fuerza una exploración en busca de nuevos dispositivos SCSI respaldados por LUN. El valor de la ruta devuelto por `sr-probe` un dispositivo SCSI respaldado por LUN es uniforme en todos los hosts con acceso al LUN. Por lo tanto, este valor se debe usar al crear SR compartidas accesibles para todos los hosts de un grupo de recursos.

Las mismas funciones se aplican a los HBAs iSCSI QLogic.

Consulte Crear repositorios de almacenamiento para obtener más información sobre la creación de SR iSCSI y FC basadas en HBA compartidas.

> **Nota:**
>
> El soporte de XenServer para Fibre Channel no admite la asignación directa de un LUN a una máquina virtual. Los LUN basados en HBA deben asignarse al host y especificarse para su uso en un SR. Los VDI dentro de la SR se exponen a las VM como dispositivos de bloques estándar.
>
> El tamaño de bloque de un LVM sobre HBA LUN debe ser de 512 bytes. Para usar el almacenamiento con bloques físicos de 4 KB, el almacenamiento también debe admitir la emulación de bloques de asignación de 512 bytes (el tamaño del bloque lógico debe ser de 512 bytes).

---

layout: doc
description: “Thin provisioning better utilizes the available storage by allocating disk storage space to VDIs as data is written to the virtual disk, rather than allocating the full virtual size of the VDI in advance. The shared GFS2 type represents disks as a filesystem created on an iSCSI or HBA LUN.”
—

Almacenamiento en bloques GFS2 compartido con aprovisionamiento fino

El Provisioning ligero utiliza mejor el almacenamiento disponible al asignar espacio de almacenamiento en disco a los VDI a medida que los datos se escriben en el disco vDisk, en lugar de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

asignar el tamaño virtual completo del VDI por adelantado. El Provisioning ligero le permite reducir significativamente la cantidad de espacio necesario en un arreglo de discos de almacenamiento compartido y, con ello, su coste total de propiedad (TCO).

El aprovisionamiento controlado para el almacenamiento en bloque compartido es de particular interés en los siguientes casos:

- Quieres aumentar la eficiencia del espacio. Las imágenes están escasamente asignadas y no densamente asignadas.
- Desea reducir la cantidad de operaciones de E/S por segundo en su cabina de almacenamiento. GFS2 SR es el primer tipo de SR que admite el almacenamiento en caché de lectura de almacenamiento en almacenamiento en bloque compartido.
- Se usa una imagen base común para varias máquinas virtuales. Por lo general, las imágenes de las VM individuales utilizarán incluso menos espacio.
- Usas instantáneas. Cada instantánea es una imagen y ahora cada imagen es escasa.
- Desea crear VDI con un tamaño superior a 2 TiB. La GFS2 SR admite VDI de hasta 16 TiB de tamaño.
- Su almacenamiento no admite NFS ni SMB3 y solo admite el almacenamiento en bloques. Si su almacenamiento admite NFS o SMB3, le recomendamos que utilice estos tipos de SR en lugar de GFS2.
- Su almacenamiento no admite el aprovisionamiento ligero de LUNs. Si su almacenamiento utiliza LUNs de aprovisionamiento ligero, puede tener problemas y quedarse sin espacio al combinarlo con GFS2. La combinación de GFS2 con un LUN de aprovisionamiento ligero no ofrece muchas ventajas adicionales y no se recomienda.

> **Nota:**
>
> Recomendamos no usar una SR de GFS2 con una VLAN debido a un problema conocido por el que no se pueden agregar ni quitar hosts en una agrupación en clústeres si la red del clúster está en una VLAN que no es de administración.

El tipo GFS2 compartido representa los discos como un sistema de archivos creado en un LUN iSCSI o HBA. Los VDI almacenados en una SR GFS2 se almacenan en el formato de imagen QCOW2.

En este artículo se describe cómo configurar el entorno GFS2 mediante la CLI xe. Para configurar un entorno GFS2 mediante XenCenter, consulte la documentación del producto XenCenter.

1. Planifique su entorno GFS2

Para ofrecer las ventajas del aprovisionamiento ligero en el almacenamiento en bloques compartidos sin riesgo de pérdida de datos, su grupo debe ofrecer un buen nivel de confiabilidad y conectividad. Es crucial que los hosts de la agrupación de recursos que usa GFS2 puedan comunicarse entre sí de manera confiable. Para garantizar esto, XenServer requiere que utilice un grupo agrupado en clústeres con

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

su GFS2 SR. También le recomendamos que diseñe su entorno y configure las funciones de XenServer para proporcionar la mayor capacidad de recuperación y redundancia posible.

Antes de configurar el grupo de XenServer para que funcione con los SR de GFS2, revise los siguientes requisitos y recomendaciones para un entorno GFS2 ideal:

- **Recomendado:** configure una infraestructura de red redundante.
- **Recomendado:** Cree una red enlazada dedicada
- **Obligatorio:** configurar un grupo agrupado
- **Opcional:** aumentar la memoria de su dominio de control
- **Recomendado:** configurar múltiples rutas de almacenamiento
- **Obligatorio:** crear un GFS2 SR

Un grupo agrupado con SR de GFS2 tiene algunas diferencias de comportamiento con respecto a otros tipos de grupo y SR. Para obtener más información, consulte Restricciones.

2. Configurar una infraestructura de red redundante

Una red enlazada conecta dos o más NIC para crear un único canal para el tráfico de la red. Le recomendamos que utilice una red enlazada para el tráfico de su grupo agrupado. Sin embargo, antes de configurar la red enlazada, asegúrese de que la configuración del hardware de la red promueva la redundancia en la red enlazada. Considere la posibilidad de implementar tantas de estas recomendaciones como sea posible para su organización y su entorno.

Las siguientes prácticas recomendadas agregan resiliencia frente a fallos de software, hardware o alimentación que pueden afectar a los conmutadores de red.

- Asegúrese de tener conmutadores de red físicos independientes disponibles para su uso en la red enlazada, no solo puertos en el mismo conmutador.
- Asegúrese de que los conmutadores independientes obtengan energía de unidades de distribución de energía (PDU) diferentes e independientes.
- Si es posible, en su centro de datos, coloque las PDU en diferentes fases de la alimentación o incluso en las fuentes proporcionadas por diferentes empresas de servicios públicos.
- Considere la posibilidad de utilizar unidades de alimentación ininterrumpida para garantizar que los conmutadores y servidores de la red puedan seguir funcionando o realizar un apagado ordenado en caso de un corte de energía.

3. Cree una red vinculada dedicada

Es importante asegurarse de que los hosts de un grupo agrupado en clústeres puedan comunicarse entre sí de forma fiable. La creación de una red enlazada para el tráfico de este grupo aumenta la

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

resiliencia del grupo agrupado.

Una red enlazada crea un vínculo entre dos o más NIC para crear un único canal de alto rendimiento que el grupo agrupado en clústeres puede utilizar para el tráfico de latidos del clúster. Recomendamos encarecidamente que esta red enlazada no se utilice para ningún otro tráfico. Cree una red independiente para que el grupo la utilice para el tráfico de administración.

> **Advertencia:**
>
> Si decide no seguir esta recomendación, corre un mayor riesgo de perder los paquetes de red de administración de clústeres. La pérdida de paquetes de red de administración de clústeres puede provocar que el grupo agrupado pierda quórum y que algunos o todos los hosts del grupo se autobloqueen.
>
> Si el clúster está delimitado o tiene algún problema con esta configuración no recomendada, el servicio de soporte de XenServer podría pedirle que reproduzca el mismo problema en una configuración recomendada durante el transcurso de la investigación.

Para crear una red enlazada para utilizarla como red de agrupamiento:

1. Si tiene un firewall entre los hosts de su grupo, asegúrese de que los hosts puedan comunicarse en la red del clúster mediante los siguientes puertos:

   - TCP: 8892, 8896, 21064
   - UDP: 5404, 5405

   Para obtener más información, consulte Puertos de comunicación utilizados por XenServer.

2. Abra una consola en el host de XenServer que desee que actúe como coordinadora del grupo.

3. Cree una red para usarla con la NIC enlazada mediante el siguiente comando:

   ```
   xe network-create name-label=bond0
   <!--NeedCopy-->
   ```

   Se devuelve el UUID de la nueva red.

4. Encuentre los UUID de los PIF que se van a usar en el enlace mediante el siguiente comando:

   ```
   xe pif-list
   <!--NeedCopy-->
   ```

5. Cree su red enlazada en modo activo-activo, modo activo-pasivo o modo enlace LACP. Según el modo de enlace que quiera usar, realice una de las siguientes acciones:

   - Para configurar el enlace en modo activo-activo (predeterminado), utilice el comando `bond-create` para crear el enlace. Con comas para separar los parámetros, especifique el UUID de red recién creado y los UUID de los PIF que se van a unir:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe bond-create network-uuid=<network_uuid> /
    pif-uuids=<pif_uuid_1>,<pif_uuid_2>,<pif_uuid_3>,<
        pif_uuid_4>
<!--NeedCopy-->
```

Escriba dos UUID cuando vincule dos NIC y cuatro UUID cuando vincule cuatro NIC. El UUID del enlace se devuelve después de ejecutar el comando.

- Para configurar el enlace en modo activo-pasivo o enlace LACP, utilice la misma sintaxis, agregue el parámetro `mode` opcional y especifique `lacp` o `active-backup`:

```
xe bond-create network-uuid=<network_uuid> /
    pif-uuids=<pif_uuid_1>,<pif_uuid_2>,<pif_uuid_3>,<
        pif_uuid_4> /
    mode=balance-slb | active-backup | lacp
<!--NeedCopy-->
```

Después de crear la red enlazada en el coordinador del grupo, al unir otros hosts XenServer al grupo, la información de red y enlace se replica automáticamente en el servidor que se une.

Para obtener más información, consulte Redes.

> **Nota:**
>
> - Para cambiar la dirección IP de la red de clústeres mediante XenCenter, es necesario inhabilitar temporalmente la agrupación en clústeres y GFS2.
> - No cambie la vinculación de la red de clústeres mientras el clúster está activo y tiene máquinas virtuales en ejecución. Esta acción puede provocar que los hosts del clúster se reinicien por completo (valla).
> - Si tiene un conflicto de direcciones IP (varios hosts que tienen la misma dirección IP) en su red de clústeres que implica al menos un host con la agrupación en clústeres habilitada, el clúster no se forma correctamente y los hosts no pueden cercarlo cuando es necesario. Para solucionar este problema, resuelva el conflicto de direcciones IP.

Para probar los tiempos de conmutación por error de la red enlazada activa-pasiva:

En el caso de las redes enlazadas que utilizan el modo activo-pasivo, si el enlace activo falla, hay un período de conmutación por error en el que el enlace de red se interrumpe mientras el enlace pasivo pasa a estar activo. Si el tiempo que tarda la red enlazada activo-pasiva en realizar la conmutación por error supera el tiempo de espera del clúster, es posible que algunos o todos los hosts del grupo agrupado en clústeres sigan bloqueados.

Puede probar el tiempo de conmutación por error de la red enlazada obligando a la red a realizar la conmutación por error mediante uno de los métodos siguientes:

- Extrayendo físicamente los cables de red

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Al deshabilitar los puertos del switch en un enlace de red

Repita la prueba varias veces para asegurarse de que el resultado sea uniforme.

El valor de tiempo de espera del clúster de su grupo depende del número de hosts que haya en el clúster. Ejecute el siguiente comando para encontrar el `token-timeout` valor del pool en segundos:

```
xe cluster-param-get uuid=<cluster_uuid> param-name=token-timeout
```

Si es probable que el tiempo de conmutación por error sea mayor que el valor del tiempo de espera, es posible que la infraestructura y la configuración de la red no sean lo suficientemente confiables como para admitir un grupo agrupado en clústeres.

4. Configurar un grupo agrupado

Para usar el almacenamiento GFS2 compartido, el grupo de recursos de XenServer debe ser un grupo agrupado en clústeres. Habilite la agrupación en clústeres en su grupo antes de crear una SR GFS2.

Un grupo agrupado en clústeres es un grupo de hosts de XenServer que están más estrechamente conectados y coordinados que los hosts de grupos no agrupados en clústeres. Los hosts del clúster mantienen una comunicación constante entre sí en una red seleccionada. Todos los hosts del clúster conocen el estado de todos los hosts del clúster. Esta coordinación de host permite que el clúster controle el acceso al contenido de GFS2 SR. Para garantizar que el grupo agrupado permanezca siempre en comunicación, cada host de un clúster debe estar siempre en comunicación con al menos la mitad de los hosts del clúster (incluido él mismo). Este estado se conoce como anfitrión que tiene quórum. Si un host no tiene quórum, se reinicia con fuerza y se elimina del clúster. Esta acción se conoce como "esgrima".

Para obtener más información, consulte Grupos agrupados.

Antes de empezar a configurar el grupo agrupado, asegúrese de que se cumplen los siguientes requisitos previos:

- Planifique crear un grupo de entre 3 y 16 hosts.

  Siempre que sea posible, utilice un número impar de hosts en un grupo agrupado, ya que esto garantiza que los hosts siempre puedan determinar si tienen quorun. Le recomendamos que utilice la agrupación en clústeres solo en grupos que contengan al menos tres hosts, ya que los grupos de dos hosts son sensibles a la posibilidad de que se autoproteja todo el grupo.

  Los grupos agrupados solo admiten hasta 16 hosts por grupo.

- Todos los hosts XenServer del grupo agrupado deben tener al menos 2 GiB de memoria en el dominio de control.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Todos los hosts del clúster deben usar direcciones IP estáticas para la red del clúster.
- Si está agrupando un grupo existente, asegúrese de que la alta disponibilidad esté inhabilitada. Puede volver a habilitar la alta disponibilidad después de habilitar la agrupación en clústeres.

Para usar la CLI xe para crear un grupo en clúster:

1. Cree un grupo de recursos de al menos tres hosts de XenServer.

   Repita los siguientes pasos en cada host de XenServer que no sea el coordinador del grupo:

   a) Abra una consola en el host de XenServer.

   b) Une el host de XenServer al grupo en el coordinador del grupo mediante el siguiente comando:

   ```
   xe pool-join master-address=<master_address> /
       master-username=<administrators_username> /
       master-password=<password>
   <!--NeedCopy-->
   ```

   El valor del `master-address` parámetro debe establecerse en el nombre de dominio completo del host de XenServer que es el coordinador del grupo. `password` Debe ser la contraseña de administrador establecida cuando se instaló el coordinador de la agrupación.

   Para obtener más información, consulte Hosts y grupos de recursos.

2. Para cada PIF que pertenezca a esta red, defina `disallow-unplug=true`.

   a) Busque los UUID de los PIF que pertenecen a la red mediante el siguiente comando:

   ```
   xe pif-list
   <!--NeedCopy-->
   ```

   b) Ejecute el siguiente comando en un host de XenServer de su grupo de recursos:

   ```
   xe pif-param-set disallow-unplug=true uuid=<pif_uuid>
   <!--NeedCopy-->
   ```

3. Habilite la agrupación en clústeres en su grupo. Ejecute el siguiente comando en un host de XenServer de su grupo de recursos:

   ```
   xe cluster-pool-create network-uuid=<network_uuid>
   <!--NeedCopy-->
   ```

   Proporcione el UUID de la red enlazada que creó en un paso anterior.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Aumentar la memoria de su dominio de control

Si no tiene suficiente memoria de dominio de control en sus hosts, su agrupación puede experimentar inestabilidad en la red. La inestabilidad de la red puede causar problemas a una agrupación en clústeres con la SR de GFS2.

Es importante asegurarse de que su agrupación en clústeres tenga la cantidad adecuada de memoria de dominio de control. Para obtener información sobre cómo cambiar la cantidad de memoria del dominio de control y supervisar el comportamiento de la memoria, consulte Uso de memoria.

6. Configurar múltiples rutas de almacenamiento

Asegúrese de que las rutas múltiples de almacenamiento estén configuradas entre su grupo en clúster y su SR GFS2.

Las rutas múltiples enrutan el tráfico de almacenamiento a un dispositivo de almacenamiento a través de múltiples rutas para lograr redundancia. Todas las rutas pueden tener tráfico activo durante el funcionamiento normal, lo que se traduce en un aumento del rendimiento.

Antes de habilitar las rutas múltiples, compruebe que se cumplen estas afirmaciones:

- Su conmutador Ethernet o de fibra está configurado para que varios destinos estén disponibles en su servidor de almacenamiento.

  Por ejemplo, un back-end de almacenamiento iSCSI consultado por `sendtargets` en un portal determinado devuelve varios destinos, como en el siguiente ejemplo:

  ```
  iscsiadm -m discovery --type sendtargets --portal 192.168.0.161
  192.168.0.161:3260,1 iqn.strawberry:litchie
  192.168.0.204:3260,2 iqn.strawberry:litchie
  ```

  Sin embargo, puede realizar una configuración adicional para habilitar rutas múltiples iSCSI para arreglos que solo exponen un único destino. Para obtener más información, consulte Rutas múltiples iSCSI para arreglos que solo exponen un único objetivo.

- Solo para iSCSI, el dominio de control (dom0) tiene una dirección IP en cada subred utilizada por el almacenamiento de rutas múltiples.

  Asegúrese de que para cada ruta al almacenamiento tenga una NIC y que haya una dirección IP configurada en cada NIC. Por ejemplo, si quiere cuatro rutas a su almacenamiento, debe tener cuatro NIC que tengan una dirección IP configurada cada una.

- Solo para iSCSI, cada objetivo e iniciador iSCSI tiene un IQN único.
- Solo para iSCSI, los puertos de destino iSCSI funcionan en modo portal.
- Solo para HBA, hay varios HBA conectados a la estructura del conmutador.
- Si es posible, utilice varios conmutadores redundantes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para habilitar las rutas múltiples mediante la CLI xe

Le recomendamos que habilite las rutas múltiples para todos los hosts de su grupo *antes de* crear el SR. Si crea el SR antes de habilitar las rutas múltiples, debe poner sus hosts en modo de mantenimiento para habilitar las rutas múltiples.

1. Abra una consola en el host de XenServer.
2. Desconecte todos los PBD del host mediante el siguiente comando:

   ```
   xe pbd-unplug uuid=<pbd_uuid>
   <!--NeedCopy-->
   ```

   Puede usar el comando `xe pbd-list` para encontrar el UUID de los PBD.
3. Establezca el valor del parámetro `multipathing` en **`true`** mediante el siguiente comando:

   ```
   xe host-param-set uuid=<host uuid> multipathing=true
   <!--NeedCopy-->
   ```
4. Si hay SR existentes en los hosts que se ejecutan en el modo de ruta única y tienen varias rutas:
   - Migre o suspenda cualquier huésped en ejecución con discos virtuales en los SR afectados.
   - Conecte de nuevo el PBD de los RA afectados para volver a conectarlos mediante rutas múltiples:

     ```
     xe pbd-plug uuid=<pbd_uuid>
     <!--NeedCopy-->
     ```
5. Repita estos pasos para habilitar las rutas múltiples en todos los hosts del grupo.

Asegúrese de habilitar las rutas múltiples en todos los hosts del grupo. Todas las configuraciones de cableado y, en el caso de iSCSI, de subred deben coincidir con las NIC correspondientes de cada host.

Para obtener más información, consulte Múltiples rutas de almacenamiento.

7. Crear un GFS2 SR

Cree su GFS2 SR compartido en un LUN iSCSI o HBA que esté visible para todos los hosts de XenServer de su agrupación de recursos. No recomendamos usar un LUN de aprovisionamiento fino con GFS2. Sin embargo, si elige esta configuración, debe asegurarse de que el LUN siempre tenga suficiente espacio para permitir que XenServer escriba en él.

Puede agregar hasta 62 SR de GFS2 a un grupo agrupado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si ha utilizado anteriormente su dispositivo de almacenamiento basado en bloques para un aprovisionamiento denso con LVM, XenServer lo detectará. XenCenter le brinda la oportunidad de usar la partición LVM existente o de formatear el disco y configurar una partición GFS2.

Crear una SR GFS2 compartida a través de iSCSI

Puede crear GFS2 a través de SRs iSCSI mediante XenCenter. Para obtener más información, consulte Almacenamiento iSCSI de software en la documentación del producto XenCenter.

Como alternativa, puede usar la CLI xe para crear una SR GFS2 sobre iSCSI.

Parámetros de configuración de dispositivos para SRs GFS2:

Nombre del parámetro	Descripción	¿Obligatorio?
`provider`	La implementación del proveedor de bloques. En este caso, `iscsi`.	Sí
`target`	La dirección IP o el nombre de host del archivador iSCSI que aloja	Sí
`targetIQN`	El objetivo IQN del archivador iSCSI que aloja el SR	Sí
`SCSIid`	Identificador SCSI del dispositivo	Sí

Puede encontrar los valores que se van a usar para estos parámetros mediante el comando `xe sr-probe-ext`.

```
xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<
    config> sm-config:=<sm_config>
<!--NeedCopy-->
```

1. Comience por ejecutar el siguiente comando:

   ```
   xe sr-probe-ext type=gfs2 device-config:provider=iscsi
   <!--NeedCopy-->
   ```

   La salida del comando le pide que proporcione parámetros adicionales y le da una lista de valores posibles en cada paso.

2. Repita el comando y agregue nuevos parámetros cada vez.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Cuando el resultado del comando comienza con `Found the following complete configurations that can be used to create SRs:`, puede localizar el SR mediante el comando `xe sr-create` y los `device-config` parámetros que especificó.

   Ejemplo de salida :

   ‘‘‘

   Se encontraron las siguientes configuraciones completas que se pueden usar para crear SR:
   Configuración 0:
   scsiId:
   36001405852f77532a064687aea8a5b3f TargetIQN: iqn.2009-01.example.com:iscsi192a25d6 target: 198.51.100.27 provider: iscsi

   Configuration 0 extra information:
   ‘‘‘

Para crear una SR GFS2 compartida en un LUN específico de un destino iSCSI, ejecute el siguiente comando en un servidor de su grupo en clúster:

```
xe sr-create type=gfs2 name-label="Example GFS2 SR" --shared \
   device-config:provider=iscsi device-config:targetIQN=<target_iqns> \
   device-config:target=<portal_address> device-config:SCSIid=<scsci_id
      >
```

Si no se puede acceder al destino iSCSI mientras los sistemas de archivos GFS2 están montados, es posible que algunos hosts del grupo agrupado en clústeres se reinicien con fuerza (valla).

Para obtener más información sobre cómo trabajar con SR iSCSI, consulte Compatibilidad con iSCSI de software.

Crear una GFS2 compartida a través de HBA SR

Puede crear GFS2 a través de SR de HBA mediante XenCenter. Para obtener más información, consulte Almacenamiento de HBA de hardware en la documentación del producto XenCenter.

Como alternativa, puede usar la CLI xe para crear una GFS2 a través de HBA SR.

Parámetros de configuración de dispositivos para SRs GFS2:

Nombre del parámetro	Descripción	¿Obligatorio?
`provider`	La implementación del proveedor de bloques. En este caso, `hba`.	Sí
`SCSIid`	Identificador SCSI del dispositivo	Sí

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puede encontrar los valores que se van a usar para el parámetro ScsiId mediante el comando `xe sr-probe-ext`.

```
xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<
    config> sm-config:=<sm_config>
```

1. Comience por ejecutar el siguiente comando:

   ```
   xe sr-probe-ext type=gfs2 device-config:provider=hba
   ```

   La salida del comando le pide que proporcione parámetros adicionales y le da una lista de valores posibles en cada paso.

2. Repita el comando y agregue nuevos parámetros cada vez.

3. Cuando el resultado del comando comienza con `Found the following complete configurations that can be used to create SRs:`, puede localizar el SR mediante el comando `xe sr-create` y los `device-config` parámetros que especificó.

   Ejemplo de salida :

   “‘

   Se encontraron las siguientes configuraciones completas que se pueden usar para crear SR:
   Configuración 0:
   scsiId:
   36001405852f77532a064687aea8a5b3f TargetIQN: iqn.2009-01.example.com:iscsi192a25d6 target: 198.51.100.27 provider: iscsi

   Configuration 0 extra information:
   “‘

Para crear una SR GFS2 compartida en un LUN específico de un destino de HBA, ejecute el siguiente comando en un servidor de su grupo agrupado en clúster:

```
xe sr-create type=gfs2 name-label="Example GFS2 SR" --shared \
  device-config:provider=hba device-config:SCSIid=<device_scsi_id>
<!--NeedCopy-->
```

Para obtener más información sobre cómo trabajar con SR de HBA, consulte Adaptadores de bus de host de hardware.

¿Qué sigue?

Ahora que ha configurado su entorno de GFS2, es importante que mantenga la estabilidad de su grupo agrupado asegurándose de que tiene quórum. Para obtener más información, consulte Administrar su grupo agrupado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si tiene problemas con su entorno de GFS2, consulte Solucionar problemasde grupos agrupados en clústeres.

Puede gestionar su GFS2 SR de la misma forma que lo hace con otros SR. Por ejemplo, puede agregar capacidad a la matriz de almacenamiento para aumentar el tamaño del LUN. Para obtener más información, consulte Expansión de LUN en vivo.

Limitaciones

El almacenamiento GFS2 compartido tiene actualmente las siguientes restricciones:

- Al igual que con cualquier SR de aprovisionamiento ligero, si el uso de SR de GFS2 aumenta hasta el 100%, fallan las escrituras posteriores de las VM. Estas escrituras fallidas pueden provocar fallos en la máquina virtual, posibles daños en los datos o ambas cosas.
- XenCenter muestra una alerta cuando el uso de SR aumenta hasta un 80%. Asegúrese de supervisar su GFS2 SR para detectar esta alerta y tomar las medidas apropiadas si lo ve. En una GFS2 SR, el uso elevado provoca una degradación del rendimiento. Le recomendamos que mantenga su uso de SR por debajo del 80%.
- La migración de máquinas virtuales con migración de almacenamiento (en vivo o sin conexión) no es compatible con las máquinas virtuales cuyas VDI están en un SR GFS2. Tampoco puede migrar VDI de otro tipo de SR a un SR GFS2.
- El transporte de FCoE no es compatible con los SR GFS2.
- Recortar/desasignar no se admite en los SR de GFS2.
- Los SR de GFS2 no admiten CHAP.
- Las métricas de rendimiento no están disponibles para los SR de GFS2 y los discos en estos SR.
- El seguimiento de bloques modificados no es compatible con los VDI almacenados en SRs de GFS2.
- No puede exportar VDI de más de 2 TiB como VHD u OVA/OVF. Sin embargo, puede exportar máquinas virtuales con VDI de más de 2 TiB en formato XVA.
- No recomendamos usar un LUN de aprovisionamiento fino con GFS2. Sin embargo, si elige esta configuración, debe asegurarse de que el LUN siempre tenga suficiente espacio para permitir que XenServer escriba en él.
- No puede tener más de 62 SR GFS2 en su agrupación.
- Los grupos agrupados solo admiten hasta 16 hosts por grupo.
- Para habilitar la alta disponibilidad en su agrupación en clústeres, la SR de latido debe ser una SR de GFS2.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Para el tráfico de clústeres, le recomendamos encarecidamente que utilice una red enlazada que utilice al menos dos conmutadores de red diferentes. No utilice esta red para ningún otro propósito.
- Para cambiar la dirección IP de la red de clústeres mediante XenCenter, es necesario inhabilitar temporalmente la agrupación en clústeres y GFS2.
- No cambie la vinculación de la red de clústeres mientras el clúster está activo y tiene máquinas virtuales en ejecución. Esta acción puede provocar que los hosts del clúster se reinicien por completo (valla).
- Si tiene un conflicto de direcciones IP (varios hosts que tienen la misma dirección IP) en su red de clústeres que implica al menos un host con la agrupación en clústeres habilitada, el clúster no se forma correctamente y los hosts no pueden cercarlo cuando es necesario. Para solucionar este problema, resuelva el conflicto de direcciones IP.

---

layout: doc
description: Create and manage storage repositories in your XenServer environment.—

Administrar repositorios de almacenamiento

En esta sección se describe la creación de tipos de repositorios de almacenamiento y su puesta a disposición del host de XenServer. También cubre varias operaciones requeridas en la administración continua de repositorios de almacenamiento (SR), incluida la migración de VDI en vivo.

Crear repositorios de almacenamiento

En esta sección se explica cómo crear repositorios de almacenamiento (SR) de diferentes tipos y ponerlos a disposición del host de XenServer. Los ejemplos proporcionados cubren la creación de SRs mediante la CLI xe. Para obtener más información sobre el uso del asistente **Nuevo repositorio de almacenamiento** para agregar SR mediante XenCenter, consulte la documentación de XenCenter.

> **Nota:**
>
> Los SR locales de tipo `lvm`, `ext` y `xfs` solo se pueden crear mediante la CLI xe. Después de la creación, puede administrar todos los tipos de SR mediante XenCenter o la CLI xe.

Hay dos pasos básicos para crear un repositorio de almacenamiento para usarlo en un host mediante la CLI:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Pruebe el tipo de SR para determinar los valores de los parámetros requeridos.
2. Cree el SR para inicializar el objeto SR y los objetos PBD asociados, conectar los PBD y activar el SR.

Estos pasos difieren en detalle según el tipo de SR que se esté creando. En todos los ejemplos, el comando `sr-create` devuelve el UUID de la SR creada si tiene éxito.

Los SR se pueden *destruir* cuando ya no se usan para liberar el dispositivo físico. También se pueden *olvidar* los SR para separar el SR de un host de XenServer y conectarlo a otro. Para obtener más información, consulte *Eliminación de SR* en la siguiente sección.

Sonda una SR

El comando `sr-probe` se puede usar de las siguientes maneras:

- Para identificar parámetros desconocidos para usarlos en la creación de un SR
- Para devolver una lista de los SR existentes

En ambos casos, `sr-probe` funciona especificando un tipo de SR y uno o más parámetros `device-config` para ese tipo de SR. Si se proporciona un conjunto de parámetros incompleto, el comando `sr-probe` devuelve un mensaje de error que indica que faltan parámetros y las posibles opciones para los parámetros que faltan. Cuando se suministra un conjunto completo de parámetros, se devuelve una lista de los SR existentes. Todos los resultados de `sr-probe` se devuelven como XML.

Por ejemplo, un objetivo iSCSI conocido se puede sondear especificando su nombre o dirección IP. Se devuelve el conjunto de IQN disponibles en el objetivo:

```
    xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10

    Error code: SR_BACKEND_FAILURE_96
    Error parameters: , The request is missing or has an incorrect
       target IQN parameter, \
    <?xml version="1.0" ?>
    <iscsi-target-iqns>
        <TGT>
            <Index>
                0
            </Index>
            <IPAddress>
                192.168.1.10
            </IPAddress>
            <TargetIQN>
                iqn.192.168.1.10:filer1
            </TargetIQN>
        </TGT>
    </iscsi-target-iqns>
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Al volver a sondear el mismo destino y especificar el nombre/dirección IP y el IQN deseado, se devuelve el conjunto de SCSIids (LUN) disponibles en el objetivo/IQN.

```
    xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10  \
    device-config:targetIQN=iqn.192.168.1.10:filer1

    Error code: SR_BACKEND_FAILURE_107
    Error parameters: , The SCSIid parameter is missing or incorrect, \
    <?xml version="1.0" ?>
    <iscsi-target>
        <LUN>
            <vendor>
                IET
            </vendor>
            <LUNid>
                0
            </LUNid>
            <size>
                42949672960
            </size>
            <SCSIid>
                149455400000000000000000002000000b70200000f000000
            </SCSIid>
        </LUN>
    </iscsi-target>
<!--NeedCopy-->
```

Al sondear el mismo destino y suministrar los tres parámetros, se devuelve una lista de los SR que existen en el LUN, si los hay.

```
    xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10  \
    device-config:targetIQN=192.168.1.10:filer1 \
    device-config:SCSIid=149455400000000000000000002000000
       b70200000f000000

    <?xml version="1.0" ?>
    <SRlist>
        <SR>
            <UUID>
                3f6e1ebd-8687-0315-f9d3-b02ab3adc4a6
            </UUID>
            <Devlist>
                /dev/disk/by-id/scsi-149455400000000000000000002000000
                   b70200000f000000
            </Devlist>
        </SR>
    </SRlist>
<!--NeedCopy-->
```

Se pueden probar los siguientes parámetros para cada tipo de SR:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Tipo SR	Los parámetros device-config, en orden de dependencia	¿Se puede sondear?	¿Requerido para sr-create?
lvmoiscsi	target	No	Sí
	chapuser	No	No
	chappassword	No	No
	targetIQN	Sí	Sí
	SCSIid	Sí	Sí
lvmohba	SCSIid	Sí	Sí
lvmofcoe	SCSIid	Sí	Sí
nfs	server	No	Sí
	serverpath	Sí	Sí
smb	server	No	Sí
	username	No	No
	password	No	No
lvm	device	No	Sí
ext	device	No	Sí

Para obtener información sobre cómo probar un SR de GFS2, consulte Crear un SR de GFS2.

Eliminar SRs

Un repositorio de almacenamiento (SR) se puede eliminar temporal o permanentemente.

Separar: interrumpe la asociación entre el dispositivo de almacenamiento y el grupo o el host (PBD Unplug). El SR (y sus VDI) se vuelven inaccesibles. Se conservan el contenido de los VDI y la metainformación utilizada por las VM para acceder a los VDI. La separación se puede usar cuando desconecta temporalmente un SR, por ejemplo, para mantenimiento. Un SR separado se puede volver a conectar más tarde.

Olvídese: conserva el contenido de la SR en el disco físico, pero la información que conecta una máquina virtual a sus VDI se elimina permanentemente. Por ejemplo, le permite volver a conectar el SR a otro host de XenServer sin eliminar ninguno de los contenidos del SR.

Destruir: elimina el contenido del SR del disco físico.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Cuando utilice el almacenamiento SMB, no extraiga el recurso compartido del almacenamiento antes de desconectar el SMB SR.

Para Destroy or Forget, el PBD conectado al SR debe desconectarse del host.

1. Desenchufe el PBD para desconectar el SR del host XenServer correspondiente:

```
xe pbd-unplug uuid=pbd_uuid
<!--NeedCopy-->
```

2. Utilice el comando `sr-destroy` para eliminar una SR. El comando destruye el SR, elimina el SR y el PBD correspondiente de la base de datos host de XenServer y elimina el contenido del SR del disco físico:

```
xe sr-destroy uuid=sr_uuid
<!--NeedCopy-->
```

3. Use el comando `sr-forget` para olvidar una SR. El comando elimina el SR y el PBD correspondiente de la base de datos host de XenServer, pero deja intacto el contenido del SR real en el medio físico:

```
xe sr-forget uuid=sr_uuid
<!--NeedCopy-->
```

> **Nota:**
>
> El objeto de software correspondiente al SR puede tardar algún tiempo en recogerse como basura.

Presentar una SR

Para volver a introducir una SR *olvidada* anteriormente, cree un PBD. Conecte manualmente el PBD a los hosts de XenServer correspondientes para activar el SR.

En el siguiente ejemplo se presenta una SR de tipo `lvmoiscsi`.

1. Sondear el SR existente para determinar su UUID:

```
xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10 \
    device-config:targetIQN=192.168.1.10:filer1 \
    device-config:SCSIid=149455400000000000000000002000000
       b70200000f000000
<!--NeedCopy-->
```

2. Introduzca el UUID de SR existente devuelto por el comando `sr-probe`. Se devuelve el UUID del nuevo SR:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe sr-introduce content-type=user name-label="Example Shared LVM
    over iSCSI SR" \
     shared=true uuid=valid_sr_uuid type=lvmoiscsi
<!--NeedCopy-->
```

3. Crea un PBD para acompañar al SR. Se devuelve el UUID del nuevo PBD:

```
xe pbd-create type=lvmoiscsi host-uuid=valid_uuid sr-uuid=
    valid_sr_uuid \
     device-config:target=192.168.0.1 \
     device-config:targetIQN=192.168.1.10:filer1 \
     device-config:SCSIid=149455400000000000000000002000000
        b70200000f000000
<!--NeedCopy-->
```

4. Enchufe el PBD para conectar el SR:

```
xe pbd-plug uuid=pbd_uuid
<!--NeedCopy-->
```

5. Compruebe el estado del conector PBD. Si se hace correctamente, la propiedad `currently-attached` es true:

```
xe pbd-list sr-uuid=sr_uuid
<!--NeedCopy-->
```

> **Nota:**
>
> Realice los pasos 3 a 5 para cada host del grupo de recursos. Estos pasos también se pueden realizar con la función Repair Storage Repository en XenCenter.

Expansión de LUNs

Para cumplir con los requisitos de capacidad, es posible que deba agregar capacidad a la matriz de almacenamiento para aumentar el tamaño del LUN aprovisionado para el host de XenServer. La expansión de LUN en vivo le permite aumentar el tamaño del LUN sin ningún tiempo de inactividad de la VM.

Después de agregar más capacidad a su arreglo de almacenamiento, introduzca,

```
xe sr-scan sr-uuid=sr_uuid
<!--NeedCopy-->
```

Este comando vuelve a escanear el SR y se agrega cualquier capacidad adicional y se pone a disposición.

Esta operación también está disponible en XenCenter. Seleccione la SR para cambiar el tamaño y, a continuación, haga clic en **Reanalizar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Advertencias:**
>
> - No es posible reducir ni truncar los LUN. Reducir el tamaño del LUN en el arreglo de almacenamiento puede provocar la pérdida de datos.

Migración de VDI en vivo

La migración de VDI en vivo permite al administrador reubicar la imagen de disco vDisk (VDI) de VM sin apagar la VM. Esta función permite realizar operaciones administrativas tales como:

- Trasladar una VM desde un almacenamiento local barato a un almacenamiento rápido, resistente y respaldado por matrices.
- Mover una VM de un entorno de desarrollo a un entorno de producción.
- Moverse entre niveles de almacenamiento cuando una VM está limitada por la capacidad de almacenamiento.
- Realizar actualizaciones de arreglos de almacenamiento.

Limitaciones y advertencias

La migración de VDI en vivo está sujeta a las siguientes limitaciones y advertencias:

- Debe haber suficiente espacio en disco disponible en el repositorio de destino.

Para mover discos virtuales mediante XenCenter

1. En el panel **Recursos**, seleccione la SR en la que está almacenado el disco virtual y, a continuación, haga clic en la ficha **Almacenamiento**.
2. En la lista **Discos virtuales**, seleccione el disco virtual que quiere mover y, a continuación, haga clic en **Mover**.
3. En el cuadro de diálogo **Mover disco vDisk**, seleccione el SR de destino al que quiere mover el VDI.

   > **Nota:**
   >
   > Asegúrese de que la SR tenga espacio suficiente para otro disco virtual: el espacio disponible se muestra en la lista de SR disponibles.

4. Haga clic en **Mover** para mover el disco vDisk.

Para ver la referencia de la CLI, consulte `vdi-pool-migrate`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Migración de VDI en frío entre SR (migración fuera de línea)

Los VDI asociados a una VM se pueden copiar de un SR a otro para adaptarse a los requisitos de mantenimiento o a las configuraciones de almacenamiento en niveles. XenCenter le permite copiar una VM y todos sus VDI en el mismo SR o en uno diferente. Se puede usar una combinación de XenCenter y la CLI xe para copiar VDI individuales.

Para ver la referencia de la CLI, consulte `vm-migrate`.

Copie todos los VDI de una VM en un SR diferente

La función XenCenter Copy VM crea copias de todos los VDI para una VM seleccionada en el mismo SR o en uno diferente. La VM y los VDI de origen no se ven afectados de forma predeterminada. Para mover la máquina virtual a la SR seleccionada en lugar de crear una copia, seleccione la opción Eliminar máquina virtual original en el cuadro de diálogo Copiar máquina virtual.

1. Apague la VM.
2. En XenCenter, seleccione la VM y, a continuación, seleccione la **VM** > Opción **Copiar VM**
3. Seleccione el SR de destino deseado.

Copiar VDI individuales en un SR diferente

Se puede usar una combinación de la CLI xe y XenCenter para copiar VDI individuales entre SR.

1. Apague la VM.
2. Use la CLI xe para identificar los UUID de los VDI que se van a mover. Si la máquina virtual tiene una unidad de DVD, `vdi-uuid` aparece como `not in database` y se puede ignorar.

```
xe vbd-list vm-uuid=valid_vm_uuid
<!--NeedCopy-->
```

> **Nota:**
>
> El comando `vbd-list` muestra los UUID de VBD y VDI. Asegúrese de grabar los UUID de VDI en lugar de los UUID de VBD.

3. En XenCenter, seleccione la ficha **Almacenamiento de VM**. Para mover cada VDI, seleccione la VDI y haga clic en el botón **Desconectar**. Este paso también se puede realizar mediante el comando `vbd-destroy`.

> **Nota:**
>
> Si usa el comando `vbd-destroy` para desconectar los UUID de VDI, primero compruebe si el VBD tiene el parámetro `other-config:owner` establecido en **`true`**. Defina este

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> parámetro en **false**. Al emitir el comando vbd-destroy con other-config:owner =**true**, también se destruye la VDI asociada.

4. Use el comando vdi-copy para copiar cada uno de los VDI de VM para moverlos al SR deseado.

```
xe vdi-copy uuid=valid_vdi_uuid sr-uuid=valid_sr_uuid
<!--NeedCopy-->
```

5. En XenCenter, seleccione la ficha **Almacenamiento de VM**. Haga clic en el botón **Adjuntar** y seleccione los VDI del nuevo SR. Este paso también se puede realizar con el comando vbd-create.
6. Para eliminar los VDI originales, seleccione la ficha **Almacenamiento** del SR original en XenCenter. Los VDI originales se enumeran con un valor vacío para el campo VM. Use el botón **Eliminar** para eliminar la VDI.

Convertir SR de canal de fibra local en SR compartidos

Use la CLI xe y la función **Repair Storage Repair** de XenCenter para convertir un SR de FC local en un SR de FC compartido:

1. Actualice todos los hosts del grupo de recursos a XenServer 8.
2. Asegúrese de que todos los hosts del grupo tengan el LUN de SR dividido en zonas de manera adecuada. Consulte Sondear un SR para obtener más información sobre el uso del comando sr-probe para verificar que el LUN esté presente en cada host.
3. Convertir el SR en compartido:

```
xe sr-param-set shared=true uuid=local_fc_sr
<!--NeedCopy-->
```

4. El SR se mueve del nivel de host al nivel de grupo en XenCenter, lo que indica que ahora se comparte. El SR se marca con un signo de exclamación rojo para indicar que no está conectado en todos los hosts del grupo.
5. Seleccione el SR y, a continuación, seleccione el **almacenamiento** > Opción **Reparar repositorio de almacenamiento**.
6. Haga clic en **Reparar** para crear y conectar un PBD para cada host del grupo.

Recupere espacio para el almacenamiento basado en bloques en el arreglo de discos de reserva mediante el uso de descarte

Puede utilizar la recuperación de espacio para liberar bloques no utilizados en un LUN de aprovisionamiento reducido. Una vez liberado el espacio, el arreglo de almacenamiento puede reutilizar este

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

espacio recuperado.

> **Nota:**
>
> La recuperación de espacio solo está disponible en algunos tipos de arreglos de almacenamiento. Para determinar si su arreglo admite esta función y si necesita una configuración específica, consulte la Lista de compatibilidad de hardware y la documentación específica del proveedor de almacenamiento.

Para recuperar el espacio mediante XenCenter:

1. Seleccione la vista de **infraestructura** y, a continuación, elija el host o el grupo conectado al SR.
2. Haga clic en la ficha **Almacenamiento**.
3. Seleccione el SR en la lista y haga clic en **Recuperar espacio libre**.
4. Haga clic en **Sí** para confirmar la operación.
5. Haga clic en **Notificaciones** y luego en **Eventos** para ver el estado de la operación.

Para obtener más información, presione `F1`en XenCenter para acceder a la ayuda en línea.

Para recuperar espacio mediante la CLI xe, puede usar el siguiente comando:

```
xe host-call-plugin host-uuid=host_uuid \
    plugin=trim fn=do_trim args:sr_uuid=sr_uuid
```

> **Notas:**
>
> - La operación solo está disponible para SRs basados en LVM que se basan en LUNs aprovisionados con poco aprovisionamiento en el arreglo de discos. Las SSD locales también se pueden beneficiar de la recuperación de espacio.
> - La recuperación de espacio no es necesaria para los SR basados en archivos, como NFS y EXT3/EXT4. El botón **Reclamar espacio libre** no está disponible en XenCenter para estos tipos de SR.
> - Si ejecuta el comando xe de recuperación de espacio para un RA basado en archivos o un RA basado en LVM con aprovisionamiento grueso, el comando devuelve un error.
> - La recuperación de espacio es una operación intensiva y puede provocar una degradación en el rendimiento del arreglo de discos de almacenamiento. Por lo tanto, solo inicie esta operación cuando se requiera la recuperación de espacio en la matriz. Le recomendamos que programe este trabajo fuera de las horas pico de demanda de arreglos de discos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Recuperar espacio automáticamente al eliminar instantáneas

Al eliminar instantáneas con XenServer, el espacio asignado a los SR basados en LVM se recupera automáticamente y no es necesario reiniciar la máquina virtual. Esta operación se conoce como "fusión en línea". La fusión en línea se aplica a todos los tipos de SR.

En ciertos casos, es posible que la recuperación automática de espacio no pueda continuar. Le recomendamos que utilice la herramienta de fusión sin conexión en estos casos:

- En condiciones en las que el rendimiento de E/S de una VM es considerable
- En condiciones en las que no se reclama espacio después de un período

> **Notas:**
>
> - La ejecución de la herramienta de fusión sin conexión provoca cierto tiempo de inactividad para la máquina virtual, debido a las operaciones de suspensión o reanudación realizadas.
> - Antes de ejecutar la herramienta, elimine las instantáneas y los clones que ya no quiera. La herramienta recupera tanto espacio como sea posible dadas las instantáneas o clones restantes. Si quiere recuperar todo el espacio, elimine todas las instantáneas y los clones.
> - Los discos de VM deben estar en almacenamiento compartido o local para un único host. Las VM con discos en ambos tipos de almacenamiento no se pueden combinar.

Recupera espacio con la herramienta de fusión sin conexión

Habilite los objetos ocultos mediante XenCenter. Haga clic en **Ver** > Objetos **ocultos**. En el panel Recurso, seleccione la máquina virtual para la que quiere obtener el UUID. El UUID se muestra en la ficha **General**.

En el panel **Recursos**, seleccione el coordinador del grupo de recursos (el primer host de la lista). La ficha **General** muestra el UUID. Si no usa un grupo de recursos, seleccione el host de la VM.

1. Abra una consola en el host y ejecute el siguiente comando:

```
xe host-call-plugin host-uuid=host-UUID \
    plugin=coalesce-leaf fn=leaf-coalesce args:vm_uuid=VM-UUID
<!--NeedCopy-->
```

   Por ejemplo, si el UUID de VM es 9bad4022-2c2d-dee6-abf5-1b6195b1dad5 y el UUID de host es b8722062-de95-4d95-9baa-a5fe343898ea, ejecute el siguiente comando:

```
xe host-call-plugin host-uuid=b8722062-de95-4d95-9baa-a5fe343898ea
     \
    plugin=coalesce-leaf fn=leaf-coalesce args:vm_uuid=9bad4022-2
       c2d-dee6-abf5-1b6195b1dad5
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Este comando suspende la VM (a menos que ya esté apagada), inicia el proceso de recuperación de espacio y, a continuación, reanuda la VM.

> **Notas:**
>
> Le recomendamos que apague o suspenda la máquina virtual manualmente antes de ejecutar la herramienta de fusión fuera de línea. Puede apagar o suspender la máquina virtual mediante XenCenter o la CLI de XenServer. Si ejecuta la herramienta de fusión en una máquina virtual en ejecución, la herramienta suspende automáticamente la máquina virtual, realiza las operaciones de fusión de VDI necesarias y reanuda la máquina virtual. Es posible que las VM ágiles se reinicien en un host diferente.
>
> Si las imágenes de disco virtual (VDI) que se van a fusionar se encuentran en un almacenamiento compartido, debe ejecutar la herramienta de fusión fuera de línea en el coordinador del grupo.
>
> Si los VDI que se van a fusionar se encuentran en un almacenamiento local, ejecute la herramienta de fusión fuera de línea en el host al que está conectado el almacenamiento local.

Trabajando con E/S de disco

Puede configurar el programador de E/S del disco y los ajustes de prioridad de E/S del disco para cambiar el rendimiento de los discos.

> **Nota:**
>
> Las capacidades de E/S de disco descritas en esta sección no se aplican al almacenamiento de EqualLogic, NetApp ni NFS.

Ajustar el programador de E/S de disco

Para obtener un rendimiento general, el programador de discos predeterminado `noop` se aplica a todos los tipos de SR nuevos. El programador `noop` proporciona el rendimiento más justo para las máquinas virtuales de la competencia que acceden al mismo dispositivo.

1. Ajuste el programador de discos mediante el siguiente comando:

```
xe sr-param-set other-config:scheduler=<option> uuid=<sr_uuid>
<!--NeedCopy-->
```

   El valor de `<option>` puede ser uno de los siguientes términos: `noop`, `cfq` o `deadline`.

2. Desenchufe y vuelva a conectar el PBD correspondiente para que el parámetro del programador surta efecto.

```
xe pbd-unplug uuid=<pbd_uuid>
xe pbd-plug uuid=<pbd_uuid>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
3 <!--NeedCopy-->
```

Para aplicar la priorización de las solicitudes de E/S del disco, anule la configuración predeterminada y asigne el programador de discos `cfq` al SR.

Priorización de solicitudes de E/S de discos virtuales

Los discos virtuales tienen una configuración de prioridad de solicitud de E/S opcional. Puede usar esta configuración para priorizar las E/S en el disco de una máquina virtual en particular sobre los demás.

Antes de configurar cualquier parámetro de prioridad de solicitud de E/S de disco para un VBD, asegúrese de que el programador de discos para el SR esté configurado correctamente. El parámetro del planificador debe configurarse en `cfq` en el SR y el PBD asociado desenchufados y reconectados. Para obtener información sobre cómo ajustar el programador, consulte Ajustar el programador de E/S del disco.

En el caso de la SR compartida, en la que varios hosts acceden al mismo LUN, la configuración de prioridad se aplica a los VBD que acceden al LUN desde el mismo host. Esta configuración no se aplica a todos los anfitriones del grupo.

El host emite una solicitud al almacenamiento remoto, pero el almacenamiento remoto realiza la priorización de la solicitud.

Configuración de los parámetros de solicitud de E/S del disco Esta configuración se puede aplicar a los discos virtuales existentes mediante el comando `xe vbd-param-set` con los siguientes parámetros:

- `qos_algorithm_type`: Este parámetro se debe establecer en el valor `ionice`, que es el único algoritmo admitido para los discos virtuales.
- `qos_algorithm_param`: Utilice este parámetro para configurar pares clave/valor. Para los discos virtuales, `qos_algorithm_param` toma una clave `sched` y, según el valor, también requiere una clave **`class`**.

  La clave `qos_algorithm_param:sched` puede tener uno de los valores siguientes:

  - `sched=rt` o `sched=real-time`: Este valor establece el parámetro de programación en prioridad en tiempo real, lo que requiere un parámetro **`class`** para establecer un valor.
  - `sched=idle`: Este valor establece el parámetro de programación en prioridad de inactividad, que no requiere ningún parámetro **`class`** para establecer ningún valor.
  - `sched=anything`: Este valor establece el parámetro de programación como prioridad de máximo esfuerzo, lo que requiere un parámetro **`class`** para establecer un valor.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La clave `qos_algorithm_param:class` puede tener uno de los siguientes valores:

- Una de las siguientes palabras clave: `highest`, `high`, `normal`, `low`, `lowest`.
- Un número entero entre 0 y 7, donde 7 es la prioridad más alta y 0 es la más baja. Por ejemplo, a las solicitudes de E/S con una prioridad de 5 se les da prioridad sobre las solicitudes de E/S con una prioridad de 2.

Ejemplo Por ejemplo, los siguientes comandos de CLI configuran el VBD del disco virtual para que utilice la prioridad en tiempo real 5:

```
xe vbd-param-set uuid=<vbd_uuid> qos_algorithm_type=ionice
xe vbd-param-set uuid=<vbd_uuid> qos_algorithm_params:sched=rt
xe vbd-param-set uuid=<vbd_uuid> qos_algorithm_params:class=5
xe sr-param-set uuid=<sr_uuid> other-config:scheduler=cfq
xe pbd-unplug uuid=<pbd_uuid>
xe pbd-plug uuid=<pbd_uuid>
<!--NeedCopy-->
```

Rutas múltiples de almacenamiento

November 8, 2023

El soporte de múltiples rutas dinámicas está disponible para back-ends de almacenamiento iSCSI y Fibre Channel.

XenServer usa múltiples rutas nativas de Linux (DM-MP), la solución genérica de múltiples rutas de Linux, como su controlador de múltiples rutas. Sin embargo, XenServer complementa este controlador con funciones adicionales para que XenServer pueda reconocer las funciones específicas del proveedor de los dispositivos de almacenamiento.

La configuración de múltiples rutas proporciona redundancia para el tráfico de almacenamiento remoto si hay una pérdida de conectividad parcial. Las rutas múltiples redirigen el tráfico de almacenamiento a un dispositivo de almacenamiento a través de varias rutas para obtener redundancia y aumentar el rendimiento. Puede usar hasta 16 rutas en un único LUN. Las rutas múltiples son una configuración activa-activa. De forma predeterminada, las rutas múltiples utilizan el equilibrio de carga por turnos o multibus según el tipo de arreglo de almacenamiento. Todas las rutas tienen tráfico activo en ellas durante el funcionamiento normal, lo que se traduce en un mayor rendimiento.

> **Importante:**
>
> Le recomendamos que habilite las rutas múltiples para todos los hosts de su grupo *antes de* crear el SR. Si crea el SR antes de habilitar las rutas múltiples, debe poner sus hosts en modo de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> mantenimiento para habilitar las rutas múltiples.

La vinculación de NIC también puede proporcionar redundancia para el tráfico de almacenamiento. Para el almacenamiento iSCSI, recomendamos configurar rutas múltiples en lugar de vinculación NIC siempre que sea posible.

Las rutas múltiples no son efectivas en los siguientes casos:

- Dispositivos de almacenamiento NFS
- Tiene un número limitado de NIC y necesita redirigir el tráfico iSCSI y el tráfico de archivos (NFS o SMB) a través de la misma NIC

En estos casos, considere utilizar la vinculación NIC en su lugar. Para obtener más información sobre la vinculación de NIC, consulte Redes.

Requisitos previos

Antes de habilitar las rutas múltiples, compruebe que se cumplen estas afirmaciones:

- Hay varios destinos disponibles en su servidor de almacenamiento.

  Por ejemplo, un back-end de almacenamiento iSCSI consultado por `sendtargets` en un portal determinado devuelve varios destinos, como en el siguiente ejemplo:

  ```
  iscsiadm -m discovery --type sendtargets --portal 192.168.0.161
  192.168.0.161:3260,1 iqn.strawberry:litchie
  192.168.0.204:3260,2 iqn.strawberry:litchie
  ```

  Sin embargo, puede realizar una configuración adicional para habilitar rutas múltiples iSCSI para arreglos que solo exponen un único destino. Para obtener más información, consulte Rutas múltiples iSCSI para arreglos que solo exponen un único objetivo.

- Solo para iSCSI, el dominio de control (dom0) tiene una dirección IP en cada subred utilizada por el almacenamiento de rutas múltiples.

  Asegúrese de que para cada ruta al almacenamiento que quiera tener, tenga una NIC y que haya una dirección IP configurada en cada NIC. Por ejemplo, si quiere cuatro rutas a su almacenamiento, debe tener cuatro NIC que tengan una dirección IP configurada cada una.

- Solo para iSCSI, cada objetivo e iniciador iSCSI tiene un IQN único.
- Solo para iSCSI, los puertos de destino iSCSI funcionan en modo portal.
- Solo para HBA, hay varios HBA conectados a la estructura del conmutador.

Habilitar multipathing

Puede habilitar las rutas múltiples en XenCenter o en la CLI xe.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para habilitar las rutas múltiples mediante XenCenter

1. En el panel Recursos de **XenCenter**, haga clic con el botón derecho en el host y **elija**Entrar en modo de mantenimiento.
2. Espere a que el anfitrión vuelva a aparecer en el panel **Recursos** con el icono del modo de mantenimiento (un cuadrado azul) antes de continuar.
3. En la ficha **General** del anfitrión, haga clic en **Propiedades** y, a continuación, vaya a la ficha **Múltiples rutas.**
4. Para habilitar las rutas múltiples, marque la casilla **Habilitar rutas múltiples en este servidor**.
5. Haga clic en **Aceptar** para aplicar el nuevo parámetro. Se produce una breve demora mientras XenCenter guarda la nueva configuración de almacenamiento.
6. En el panel **Recursos**, haga clic con el botón derecho en el host y elija **Salir del modo de mantenimiento**.
7. Repita estos pasos para habilitar las rutas múltiples en todos los hosts del grupo.

Asegúrese de habilitar las rutas múltiples en todos los hosts del grupo. Todas las configuraciones de cableado y, en el caso de iSCSI, de subred deben coincidir con las NIC correspondientes de cada host.

Para habilitar las rutas múltiples mediante la CLI xe

1. Abra una consola en el host de XenServer.
2. Desconecte todos los PBD del host mediante el siguiente comando:

```
xe pbd-unplug uuid=<pbd_uuid>
<!--NeedCopy-->
```

   Puede usar el comando `xe pbd-list` para encontrar el UUID de los PBD.

3. Establezca el valor del parámetro `multipathing` en **`true`** mediante el siguiente comando:

```
xe host-param-set uuid=<host uuid> multipathing=true
<!--NeedCopy-->
```

4. Si hay SR existentes en el servidor que se ejecutan en modo de ruta única pero que tienen varias rutas:
   - Migrar o suspender cualquier huésped en ejecución con discos virtuales en los SR afectados
   - Conecte de nuevo el PBD de los RA afectados para volver a conectarlos mediante rutas múltiples:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe pbd-plug uuid=<pbd_uuid>
<!--NeedCopy-->
```

5. Repita estos pasos para habilitar las rutas múltiples en todos los hosts del grupo.

Asegúrese de habilitar las rutas múltiples en todos los hosts del grupo. Todas las configuraciones de cableado y, en el caso de iSCSI, de subred deben coincidir con las NIC correspondientes de cada host.

Inhabilitar rutas múltiples

Puede inhabilitar las rutas múltiples en XenCenter o en la CLI xe.

Para inhabilitar las rutas múltiples mediante XenCenter

1. En el panel Recursos de **XenCenter**, haga clic con el botón derecho en el host y **elija**Entrar en modo de mantenimiento.
2. Espere a que el anfitrión vuelva a aparecer en el panel **Recursos** con el icono del modo de mantenimiento (un cuadrado azul) antes de continuar.
3. En la ficha **General** del anfitrión, haga clic en **Propiedades** y, a continuación, vaya a la ficha **Múltiples rutas.**
4. Para inhabilitar las rutas múltiples, desmarque la casilla **Habilitar rutas múltiples en este servidor**.
5. Haga clic en **Aceptar** para aplicar el nuevo parámetro. Se produce una breve demora mientras XenCenter guarda la nueva configuración de almacenamiento.
6. En el panel **Recursos**, haga clic con el botón derecho en el host y elija **Salir del modo de mantenimiento**.
7. Repita estos pasos para configurar las rutas múltiples en todos los hosts del grupo.

Para inhabilitar las rutas múltiples mediante la CLI xe

1. Abra una consola en el host de XenServer.
2. Desconecte todos los PBD del host mediante el siguiente comando:

   ```
   xe pbd-unplug uuid=<pbd_uuid>
   <!--NeedCopy-->
   ```

   Puede usar el comando `xe pbd-list` para encontrar el UUID de los PBD.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Establezca el valor del parámetro `multipathing` en **`false`** mediante el siguiente comando:

```
xe host-param-set uuid=<host uuid> multipathing=false
<!--NeedCopy-->
```

4. Si hay SR existentes en el servidor que se ejecutan en modo de ruta única pero que tienen varias rutas:

   - Migrar o suspender cualquier huésped en ejecución con discos virtuales en los SR afectados
   - Desconecte y vuelva a conectar el PBD de los SR afectados para volver a conectarlos mediante rutas múltiples:

```
xe pbd-plug uuid=<pbd_uuid>
<!--NeedCopy-->
```

5. Repita estos pasos para inhabilitar las rutas múltiples en todos los hosts del grupo.

Configurar rutas múltiples

Para realizar una configuración multiruta adicional, cree archivos con el sufijo `.conf` en el directorio `/etc/multipath/conf.d`. Agregue la configuración adicional en estos archivos. Multipath busca en el directorio alfabéticamente los archivos que terminen en `.conf` y lee la información de configuración de los mismos.

No modifique el archivo `/etc/multipath.conf`. Las actualizaciones de XenServer sobrescriben este archivo.

Herramientas multirruta

La compatibilidad con rutas múltiples en XenServer se basa en el asignador de dispositivos `multipathd components`. La API de Storage Manager gestiona la activación y desactivación de nodos de rutas múltiples automáticamente. A diferencia de las herramientas `dm-multipath` estándar de Linux, los nodos de asignación de dispositivos no se crean automáticamente para todos los LUN del sistema. Los nodos de asignación de dispositivos solo se aprovisionan cuando la capa de administración del almacenamiento de información utiliza los LUNs de forma activa. Por lo tanto, no es necesario utilizar ninguna de las herramientas de la CLI de `dm-multipath` para consultar o actualizar los nodos de la tabla DM en XenServer.

Si es necesario consultar manualmente el estado de las tablas del asignador de dispositivos o enumerar nodos de rutas múltiples del asignador de dispositivos activos en el sistema, utilice la utilidad `mpathutil`:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
mpathutil list
<!--NeedCopy-->
```

```
mpathutil status
<!--NeedCopy-->
```

Rutas múltiples iSCSI para arreglos que solo exponen un único objetivo

Puede configurar XenServer para que utilice múltiples rutas iSCSI con matrices de almacenamiento que solo expongan un único destino iSCSI y un IQN, a través de una dirección IP. Por ejemplo, puede seguir estos pasos para configurar las cabinas de almacenamiento unificadas Dell EqualLogic serie PS y FS.

De forma predeterminada, XenServer establece solo una conexión por destino iSCSI. Por lo tanto, con la configuración predeterminada, la recomendación es utilizar la vinculación NIC para lograr la conmutación por error y el equilibrio de carga. El procedimiento de configuración descrito en esta sección describe una configuración alternativa, en la que se establecen varias conexiones iSCSI para un único objetivo iSCSI. No se requiere la vinculación de NIC.

> **Nota:**
>
> La siguiente configuración solo se admite para servidores que están conectados exclusivamente a arreglos de almacenamiento que exponen solo un único objetivo iSCSI. Estas matrices de almacenamiento deben cumplir con los requisitos para este procedimiento con XenServer.

Para configurar rutas múltiples:

1. Realice una copia de seguridad de los datos que quiera proteger.
2. En el panel Recursos de **XenCenter**, haga clic con el botón derecho en el host y **elija**Entrar en modo de mantenimiento.
3. Espere a que el anfitrión vuelva a aparecer en el panel **Recursos** con el icono del modo de mantenimiento (un cuadrado azul) antes de continuar.
4. En la ficha **General** del anfitrión, haga clic en **Propiedades** y, a continuación, vaya a la ficha **Múltiples rutas.**
5. Para habilitar las rutas múltiples, marque la casilla **Habilitar rutas múltiples en este servidor**.
6. Haga clic en **Aceptar** para aplicar el nuevo parámetro. Se produce una breve demora mientras XenCenter guarda la nueva configuración de almacenamiento.
7. En la consola host, configure de dos a cuatro interfaces iSCSI abiertas. Cada interfaz iSCSI se usa para establecer una ruta independiente. Los siguientes pasos muestran el proceso para dos interfaces:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a) Configure dos interfaces iSCSI, ejecute estos comandos:

```
iscsiadm -m iface --op new -I c_iface1
iscsiadm -m iface --op new -I c_iface2
```

Asegúrese de que los nombres de las interfaces tengan el prefijo `c_`. Si las interfaces no utilizan este estándar de nomenclatura, se ignoran y, en su lugar, se utiliza la interfaz predeterminada.

> **Nota:**
>
> Esta configuración hace que la interfaz predeterminada se use para todas las conexiones. Esto indica que todas las conexiones se establecen mediante una sola interfaz.

b) Enlazar las interfaces iSCSI a xenbr1 y xenbr2 mediante estos comandos:

```
iscsiadm -m iface --op update -I c_iface1 -n iface.
   net_ifacename -v xenbr1
iscsiadm -m iface --op update -I c_iface2 -n iface.
   net_ifacename -v xenbr2
```

> **Nota:**
>
> Esta configuración supone que las interfaces de red configuradas para el dominio de control (incluidos xenbr1 y xenbr2) y xenbr0 se utilizan para la administración. También se supone que las tarjetas NIC que se utilizan para la red de almacenamiento son NIC1 y NIC2.
> Si no es así, consulte la topología de red para descubrir las interfaces de red y las tarjetas NIC que se van a utilizar en estos comandos.

8. En el panel Recursos de **XenCenter**, haga clic con el botón derecho en el host y **seleccione**Salir del modo de mantenimiento. No reanude las VM todavía.
9. En la consola host, ejecute los siguientes comandos para detectar las sesiones e iniciar sesión en ellas:

```
iscsiadm -m discovery -t st -p <IP of SAN>
iscsiadm -m node -L all
```

10. Elimine las entradas obsoletas que contienen información de sesión antigua mediante estos comandos:

```
cd /var/lib/iscsi/send_targets/<IP of SAN and port, use ls command
    to check that>
rm -rf <iqn of SAN target for that particular LUN>

cd /var/lib/iscsi/nodes/
rm -rf <entries for that particular SAN>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

11. Desconecte el LUN y conéctelo de nuevo. Puede hacerlo de estas maneras:

    - Tras completar los pasos anteriores en todos los hosts de un grupo, puede usar XenCenter para separar y volver a conectar el LUN de todo el grupo.
    - Como alternativa, puede desconectar y destruir el PBD de cada host y, a continuación, reparar el SR.

      a) Ejecute los siguientes comandos para desconectar y destruir el PBD:

         i. Busque el UUID del RA:

         ```
         xe sr-list
         ```

         ii. Obtenga la lista de PBD asociados con el RA:

         ```
         xe pbd-list sr-uuid=<sr_uuid>
         ```

         iii. En el resultado del comando anterior, busque el UUID del PBD del repositorio de almacenamiento iSCSI con un identificador SCSI que no coincida.

         iv. Desenchufe y destruya el PBD que identificó.

         ```
         xe pbd-unplug uuid=<pbd_uuid>
         xe pbd-destroy uuid=<pbd_uuid>
         ```

      b) Repare el almacenamiento en XenCenter.

12. Ahora puede reanudar sus máquinas virtuales.

Almacenamiento en caché de lectura

November 28, 2023

El almacenamiento en caché de lectura mejora el rendimiento del disco de una VM, ya que, después de la lectura inicial desde el disco externo, los datos se almacenan en caché en la memoria libre del host. Mejora el rendimiento en situaciones en las que muchas VM se clonan en una sola VM base, ya que reduce drásticamente la cantidad de bloques leídos del disco. Por ejemplo, en los entornos de Citrix Virtual Desktops, los entornos de Machine Creation Services (MCS).

La mejora del rendimiento se puede ver cuando los datos se leen del disco más de una vez, ya que se almacenan en caché en la memoria. Este cambio se nota sobre todo en la degradación del servicio que se produce durante situaciones de E/S intensas. Por ejemplo, en las siguientes situaciones:

- Cuando un número significativo de usuarios finales arranca en un plazo muy limitado (tormenta de arranque)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Cuando se programa un número significativo de máquinas virtuales para ejecutar análisis de malware al mismo tiempo (tormentas de antivirus).

El almacenamiento en caché de lectura está habilitado de forma predeterminada cuando tiene el tipo de licencia apropiado.

> **Nota:**
>
> El almacenamiento en caché de lectura está disponible para los clientes de XenServer Premium Edition.

Habilitar e inhabilitar el almacenamiento en caché de lectura

Para los SR basados en archivos, como los tipos SR NFS y EXT3/EXT4, el almacenamiento en caché de lectura está habilitado de forma predeterminada. El almacenamiento en caché de lectura está inhabilitado para todos los demás SRs.

Para inhabilitar el almacenamiento en caché de lectura para un SR específico mediante la CLI xe, ejecute el siguiente comando:

```
xe sr-param-set uuid=sr-uuid other-config:o_direct=true
<!--NeedCopy-->
```

Para inhabilitar el almacenamiento en caché de lectura para una SR específica mediante XenCenter, vaya al cuadro de diálogo **Propiedades** de la SR. En la ficha **Leer caché**, puede seleccionar habilitar o inhabilitar el almacenamiento en caché de lectura.

Para obtener más información, consulte Cambio de las propiedades de SR.

Limitaciones

- El almacenamiento en caché de lectura solo está disponible para SR NFS y EXT3/EXT4. No está disponible para otros tipos de SR.
- El almacenamiento en caché de lectura solo se aplica a los VDI y los VDI principales de solo lectura. Estos VDI existen donde las máquinas virtuales se crean a partir de "clonación rápida" o instantáneas de disco. Las mayores mejoras de rendimiento se pueden ver cuando se clonan muchas máquinas virtuales a partir de una sola imagen "dorada".
- Las mejoras de rendimiento dependen de la cantidad de memoria libre disponible en el dominio de control del host (dom0). El aumento de la cantidad de memoria dom0 permite que se asigne más memoria a la memoria caché de lectura. Para obtener información sobre cómo configurar la memoria dom0, consulte CTX134951.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Cuando se activa el almacenamiento en caché de lectura de memoria, un error de caché hace que las E/S se serialicen. A veces, esto puede resultar más caro que desactivar el almacenamiento en caché de lectura, ya que con el almacenamiento en caché de lectura desactivado se pueden paralelizar las E/S. Para reducir el impacto de las pérdidas de caché, aumente la cantidad de memoria dom0 disponible o desactive el almacenamiento en caché de lectura para el SR.

Comparación con IntelliCache

IntelliCache y el almacenamiento en caché de lectura basado en memoria son, en algunos aspectos, complementarios. IntelliCache no solo almacena en caché en un nivel diferente, sino que también almacena en caché las escrituras además de las lecturas. IntelliCache almacena en caché las lecturas de la red en un disco local. El almacenamiento en caché de lectura en memoria almacena en caché las lecturas de la red o el disco en la memoria del host. La ventaja del almacenamiento en caché de lectura en memoria es que la memoria sigue siendo un orden de magnitud más rápida que un disco de estado sólido (SSD). Mejora el rendimiento en tormentas de arranque y otras situaciones de E/S intensas.

Tanto el almacenamiento en caché de lectura como IntelliCache se pueden habilitar simultáneamente. En este caso, IntelliCache almacena en caché las lecturas de la red en un disco local. Las lecturas de ese disco local se almacenan en caché en la memoria con el almacenamiento en caché de lectura.

Establecer el tamaño de memoria caché de lectura

El rendimiento de la caché de lectura se puede optimizar proporcionando más memoria al dominio de control de XenServer (dom0).

> **Importante:**
>
> Establezca el tamaño de la memoria caché de lectura en TODOS los hosts del grupo individualmente para la optimización. Cualquier cambio posterior en el tamaño de la memoria caché de lectura también se debe establecer en todos los hosts del grupo.

En el host de XenServer, abra un shell local e inicie sesión como root.

Para establecer el tamaño de la memoria caché de lectura, ejecute el siguiente comando:

```
/opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=nnM,max:nnM
<!--NeedCopy-->
```

Defina los valores iniciales y máximos en el mismo valor. Por ejemplo, para establecer la memoria dom0 en 20.480 MiB:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
/opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=20480M,max:20480M
<!--NeedCopy-->
```

> **Importante:**
>
> Reinicie todos los hosts después de cambiar el tamaño de la memoria caché de lectura.

¿Cómo ver la asignación de memoria actual de dom0?

Para ver la configuración de memoria dom0 actual, introduzca:

```
free -m
<!--NeedCopy-->
```

La salida de `free -m` muestra la configuración actual de la memoria dom0. El valor puede ser inferior al esperado debido a varios gastos generales. La siguiente tabla de ejemplo muestra la salida de un host con dom0 establecido en 2.6 GiB

```
|                     | Total  | Used | Free  | Shared | Buffer/cache |
    Available |
|---------------------|--------|------|-------|--------|--------------|----------

| Mem:                | 2450   | 339  | 1556  | 9      | 554          |
    2019      |
| Swap:               | 1023   | 0    | 1023  |        |              |
                |
<!--NeedCopy-->
```

¿Qué rango de valores se puede utilizar? Como el dominio de control de XenServer (dom0) es de 64 bits, se pueden usar valores grandes, por ejemplo, 32 768 MiB. Sin embargo, le recomendamos que **no reduzca la memoria dom0 por debajo de 1 GiB**.

Notas de pantalla de XenCenter

Se puede considerar que toda la memoria del host comprende el hipervisor Xen, dom0, las máquinas virtuales y la memoria libre. A pesar de que dom0 y la memoria de VM suelen tener un tamaño fijo, el hipervisor Xen utiliza una cantidad variable de memoria. La cantidad de memoria utilizada depende de varios factores. Estos factores incluyen la cantidad de máquinas virtuales que se ejecutan en el host en cualquier momento y la forma en que se configuran esas máquinas virtuales. No es posible limitar la cantidad de memoria que usa Xen. Limitar la cantidad de memoria puede provocar que Xen se quede sin memoria e impedir que se inicien nuevas VM, incluso cuando el host tenga memoria libre.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para ver la memoria asignada a un host, en XenCenter, seleccione el host y, a continuación, haga clic en la ficha **Memoria**.

El campo XenServer muestra la *suma* de la memoria asignada a dom0 *y* a la memoria Xen. Por lo tanto, la cantidad de memoria que se muestra puede ser mayor que la especificada por el administrador. El tamaño de la memoria puede variar al iniciar y detener las VM, incluso cuando el administrador ha establecido un tamaño fijo para dom0.

Descripción general de gráficos

January 17, 2024

En esta sección se proporciona información general sobre la entrega virtual de aplicaciones y estaciones de trabajo gráficas profesionales en 3D en XenServer. Las ofertas incluyen GPU PassThrough (para GPU NVIDIA, AMD e Intel) y GPU compartidas basadas en hardware con NVIDIA vGPU™ e Intel GVT-G™.

La virtualización de gráficos está disponible para los clientes de XenServer Premium Edition. Para obtener más información sobre las ediciones de XenServer y saber cómo actualizarlas, visite el sitio web de XenServer. Para obtener más información, consulte Licencias.

PassThrough de GPU

En un sistema virtualizado, la mayoría de los componentes del sistema físico se comparten. El hipervisor representa estos componentes como varias instancias virtuales para varios clientes. Una GPU de paso no se abstrae en absoluto, sino que sigue siendo un dispositivo físico. Cada máquina virtual (VM) alojada tiene su propia GPU dedicada, lo que elimina la abstracción del software y la penalización de rendimiento que conlleva.

XenServer le permite asignar una GPU física (en el host de XenServer) a una máquina virtual Windows o Linux que se ejecute en el mismo host. Esta función de paso a través de GPU está diseñada para usuarios avanzados de gráficos, como diseñadores de CAD.

GPU compartida (vGPU)

La GPU compartida (vGPU) permite que varias máquinas virtuales utilicen una GPU física de forma simultánea. Como se usa una parte de una GPU física, el rendimiento es mayor que el de los gráficos emulados y no se necesita una tarjeta por VM. Esta función permite la optimización de recursos, lo que aumenta el rendimiento de la VM. Los comandos gráficos de cada máquina virtual se pasan directamente a la GPU, sin que el hipervisor los traduzca.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Varias GPU compartidas (vGPU)

Varias vGPU permiten que una sola VM utilice varias GPU virtuales al mismo tiempo. Solo se pueden utilizar determinados perfiles de vGPU y todas las vGPU conectadas a una sola máquina virtual deben ser del mismo tipo. Estas vGPU adicionales se pueden usar para realizar un procesamiento computacional. Para obtener más información sobre la cantidad de vGPU compatibles con una sola VM, consulte Límites de configuración.

Esta función solo está disponible para las GPU NVIDIA. Para obtener más información sobre las GPU físicas que admiten la función de varias vGPU, consulte la documentación de NVIDIA.

Asistencia del proveedor

En la siguiente tabla se muestra el soporte para invitados de las funciones de transferencia de GPU, GPU compartida (vGPU) y GPU compartida múltiple (vGPU):

	Transferencia de GPU para máquinas virtuales de Windows	Transferencia de GPU para máquinas virtuales Linux	GPU compartida (vGPU) para máquinas virtuales Windows	GPU compartida (vGPU) para máquinas virtuales Linux	Varias GPU compartidas (vGPU) para máquinas virtuales de Windows	Varias GPU compartidas (vGPU) para máquinas virtuales Linux
AMD	SÍ					
Intel	SÍ		SÍ (en desuso)			
NVIDIA	SÍ	SÍ	SÍ	SÍ	SÍ (ver nota)	SÍ (ver nota)

> **Nota:**
>
> - Solo algunos de los sistemas operativos invitados admiten varias vGPU. Para obtener más información, consulte Restricciones y soporte de invitados.
> - Solo algunos de los sistemas operativos invitados admiten la migración en vivo de vGPU. Para obtener más información, consulte Soporte del proveedor.

Es posible que necesite una suscripción de proveedor o una licencia en función de la tarjeta gráfica utilizada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Migración en vivo de vGPU

La migración en vivo de vGPU permite que una VM que usa una GPU virtual realice una migración en vivo, una migración de almacenamiento en vivo o una suspensión de VM. Las VM con capacidades de migración en vivo de vGPU se pueden migrar para evitar el tiempo de inactividad.

La migración en vivo de vGPU también le permite realizar actualizaciones sucesivas de grupos en grupos que hospedan máquinas virtuales habilitadas para vGPU. Para obtener más información, consulte Actualizaciones progresivas de grupos.

Para usar la migración en vivo de vGPU o la suspensión de VM, la VM debe ejecutarse en una tarjeta gráfica que admita esta función. La VM también debe tener instalados los controladores compatibles del proveedor de la GPU.

> **Advertencia:**
>
> El tamaño del estado de la GPU en el controlador de NVIDIA puede provocar un tiempo de inactividad de 5 segundos o más durante la migración en vivo de la vGPU.

Se aplican las siguientes restricciones cuando se usa la migración en vivo de vGPU:

- La migración en vivo no es compatible con el paso a través de GPU.
- Las VM deben tener instalados los controladores de vGPU adecuados para que sean compatibles con las funciones de migración en vivo de vGPU. Los controladores para invitados deben instalarse para todos los invitados que usen la función vGPU.
- Las operaciones de reinicio y apagado en una VM no se admiten mientras hay una migración en curso. Estas operaciones pueden provocar un error en la migración.
- Las VM de Linux no son compatibles con ninguna función de migración en vivo de vGPU.
- La migración en vivo del dispositivo Equilibrio de carga de trabajo no es compatible con las VM habilitadas para vGPU. El dispositivo Equilibrio de carga de trabajo no puede planificar la capacidad de las máquinas virtuales que tienen una vGPU conectada.
- Después de migrar una VM mediante la migración en vivo de vGPU, es posible que la consola VNC invitada se dañe. Use ICA, RDP u otro método basado en red para acceder a las VM después de que se haya realizado una migración en vivo de vGPU.
- La migración de VDI utiliza la migración en vivo, por lo tanto, requiere suficiente espacio de vGPU en el host para hacer una copia de la instancia de vGPU en el host. Si las GPU físicas se utilizan por completo, es posible que la migración de VDI no sea posible.

Asistencia del proveedor

En la siguiente tabla se muestra la compatibilidad con la migración en vivo de vGPU:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	Transferencia de GPU para máquinas virtuales de Windows	Transferencia de GPU para máquinas virtuales Linux	GPU compartida (vGPU) para máquinas virtuales Windows	GPU compartida (vGPU) para máquinas virtuales Linux	Varias GPU compar-tidas (vGPU) para máquinas virtuales de Windows	Varias GPU compar-tidas (vGPU) para máquinas virtuales Linux
NVIDIA			SÍ		SÍ	

Para obtener más información sobre las tarjetas gráficas que admiten esta función, consulte las secciones específicas del proveedor de esta guía. Los clientes pueden necesitar una suscripción de proveedor o una licencia en función de la tarjeta gráfica utilizada.

Apoyo y restricciones a los huéspedes

XenServer admite los siguientes sistemas operativos invitados para las GPU virtuales.

Tecnología de GPU virtual de NVIDIA

Los sistemas operativos marcados con un asterisco (*) también admiten varias vGPU.

Invitados Windows:

- Windows 10 (64 bits) *
- Windows 11 (64 bits) *
- Windows Server 2016 (64 bits) *
- Windows Server 2019 (64 bits) *
- Windows Server 2022 (64 bits) *

Invitados de Linux:

- RHEL 7 (*)
- RHEL 8 (*)
- RHEL 9 *
- CentOS 7
- CentOS Stream 9
- Ubuntu 18.04 * (obsoleto)
- Ubuntu 20.04 *
- Ubuntu 22.04 *
- Rocky Linux 8 *

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Rocky Linux 9 *

Intel GVT-g (obsoleto)

Invitados Windows:

- Windows 10 (64 bits)
- Windows Server 2016 (64 bits)

Limitaciones

- Las máquinas virtuales con una GPU virtual no son compatibles con el control dinámico de memoria.
- XenServer detecta y agrupa automáticamente las GPU físicas idénticas en los hosts del mismo grupo. Si se asigna a un grupo de GPU, se puede iniciar una VM en cualquier host del grupo que tenga una GPU disponible en el grupo.
- Todas las soluciones gráficas (NVIDIA vGPU, Intel GVT-D, Intel GVT-G y vGPU pass-Through) se pueden utilizar en un entorno que utilice alta disponibilidad. Sin embargo, las máquinas virtuales que usan estas soluciones de gráficos no se pueden proteger con alta disponibilidad. Estas máquinas virtuales se pueden reiniciar según el mejor esfuerzo mientras haya hosts con los recursos gratuitos adecuados.

Preparar el host para gráficos

February 23, 2024

En esta sección se proporcionan instrucciones paso a paso sobre cómo preparar XenServer para las tecnologías de virtualización gráfica compatibles. Las ofertas incluyen NVIDIA vGPU, Intel gVT-D e Intel gVT-g.

Tecnología de GPU virtual de NVIDIA

La vGPU de NVIDIA permite que varias máquinas virtuales (VM) tengan acceso directo y simultáneo a una sola GPU física. Utiliza controladores gráficos NVIDIA implementados en sistemas operativos no virtualizados. Las GPU físicas de NVIDIA pueden admitir varios dispositivos de GPU virtuales (vGPU). Para ofrecer este soporte, la GPU física debe estar bajo el control de NVIDIA Virtual GPU Manager, que

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

se ejecuta en el dominio de control de XenServer (dom0). Las vGPU se pueden asignar directamente a las VM.

Las VM usan GPU virtuales como una GPU física por la que ha pasado el hipervisor. Un controlador NVIDIA cargado en la VM proporciona acceso directo a la GPU para rutas rápidas críticas para el rendimiento. También proporciona una interfaz paravirtualizada para el administrador de GPU virtual de NVIDIA.

> **Importante:**
>
> Para asegurarse de disponer siempre de las últimas correcciones funcionales y de seguridad, asegúrese de instalar el paquete de software vGPU de NVIDIA más reciente para XenServer (compuesto por el administrador de GPU virtual de NVIDIA para XenServer y los controladores de NVIDIA) y manténgalo actualizado a la última versión proporcionada por NVIDIA. Para obtener más información, consulte la documentación de NVIDIA.
>
> Los controladores NVIDIA más recientes están disponibles en NVIDIA NVOnline.

La vGPU de NVIDIA es compatible con la función HDX 3D Pro de Citrix Virtual Apps and Desktops o Citrix DaaS. Para obtener más información, consulte HDX 3D Pro.

Nota de licencia

NVIDIA vGPU está disponible para los clientes de XenServer Premium Edition. Para obtener más información sobre las ediciones de XenServer y saber cómo actualizarlas, visite el sitio web de XenServer. Para obtener más información, consulte Licencias.

Según la tarjeta gráfica NVIDIA utilizada, es posible que necesites una suscripción a NVIDIA o una licencia.

Para obtener información sobre la licencia de tarjetas NVIDIA, consulte el sitio web de NVIDIA.

Tipos de vGPU NVIDIA disponibles

Las tarjetas NVIDIA GRID contienen varias unidades de procesamiento gráfico (GPU). Por ejemplo, las tarjetas TESLA M10 contienen cuatro GPU GM107GL y las tarjetas TESLA M60 contienen dos GPU GM204GL. Cada GPU física puede alojar varios tipos diferentes de GPU virtual (vGPU). Los tipos de vGPU tienen una cantidad fija de búfer de fotogramas, cantidad de cabezales de pantalla compatibles y resoluciones máximas, y están dirigidos a diferentes clases de carga de trabajo.

Para obtener una lista de las tarjetas NVIDIA admitidas más recientemente, consulte la Lista de compatibilidad de hardware y la información del producto NVIDIA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Todas las vGPU alojadas en una GPU física al mismo tiempo **deben ser del mismo tipo.** Sin embargo, no hay ninguna restricción correspondiente para las GPU físicas en la misma tarjeta. Esta restricción es automática y puede provocar problemas inesperados de planificación de capacidad.

Requisitos del sistema de vGPU de NVIDIA

- Tarjeta NVIDIA GRID:
  - Para obtener una lista de las tarjetas NVIDIA admitidas más recientemente, consulte la Lista de compatibilidad de hardware y la información del producto NVIDIA.
- En función de la tarjeta gráfica NVIDIA utilizada, es posible que necesites una suscripción o una licencia de NVIDIA. Para obtener más información, consulte la información del producto NVIDIA.
- Según la tarjeta gráfica NVIDIA, es posible que deba asegurarse de que la tarjeta esté configurada en el modo correcto. Para obtener más información, consulte la documentación de NVIDIA.
- XenServer Premium Edition.
- Un host capaz de alojar XenServer y las tarjetas NVIDIA compatibles.
- Paquete de software NVIDIA vGPU para XenServer, compuesto por NVIDIA Virtual GPU Manager para XenServer y controladores NVIDIA.

  > **Nota:**
  >
  > Consulta la documentación del software NVIDIA Virtual GPU disponible en el sitio web de NVIDIA. Regístrese en NVIDIA para acceder a estos componentes.

- Para ejecutar Citrix Virtual Desktops con máquinas virtuales que ejecutan NVIDIA vGPU, también necesita: Citrix Virtual Desktops 7.6 o posterior, instalación completa.
- Para las vGPU NVIDIA Ampere y todas las generaciones futuras, debe habilitar SR-IOV en el firmware del sistema.

Migración en vivo de vGPU

XenServer permite el uso de la migración en vivo, la migración en vivo del almacenamiento y la capacidad de suspender y reanudar las máquinas virtuales habilitadas para NVIDIA vGPU.

Para usar las funciones de migración en vivo de vGPU, migración de almacenamiento en vivo o Suspender, cumpla los siguientes requisitos:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Una tarjeta NVIDIA GRID, familia Maxwell o posterior.
- Un administrador de GPU virtual de NVIDIA para XenServer con migración en vivo habilitada. Para obtener más información, consulte la documentación de NVIDIA.
- Una máquina virtual de Windows que tiene instalados controladores de vGPU habilitados para migración en vivo de NVIDIA.

La migración en vivo de vGPU permite el uso de la migración en vivo dentro de un grupo, la migración en vivo entre grupos, la migración en vivo del almacenamiento y la suspensión/reanudación de máquinas virtuales habilitadas para vGPU.

Resumen de preparación

1. Instale XenServer
2. Instale el administrador de GPU virtual de NVIDIA para XenServer
3. Reinicie el host de XenServer

Instalación en XenServer

XenServer está disponible para su descarga en la página de descargas de XenServer.

Instale lo siguiente:

- **ISO de instalación básica de XenServer**
- **Consola de administración de Windows XenCenter**

Para obtener más información, consulte Instalación.

Nota de licencia

vGPU está disponible para los clientes de XenServer Premium Edition. Para obtener más información sobre las ediciones de XenServer y saber cómo actualizarlas, visite el sitio web de XenServer. Para obtener más información, consulte Licencias.

Según la tarjeta gráfica NVIDIA utilizada, es posible que necesites una suscripción a NVIDIA o una licencia. Para obtener más información, consulte Información del producto NVIDIA.

Para obtener información sobre las licencias de tarjetas NVIDIA, consulte el sitio web de NVIDIA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Instale el administrador de vGPU de NVIDIA para XenServer

Instale el software de GPU virtual NVIDIA que está disponible en NVIDIA. El software de GPU virtual NVIDIA se compone de:

- Administrador de GPU virtual NVIDIA
- Controlador de pantalla de Windows (el controlador de pantalla de Windows depende de la versión de Windows)

El **administrador de GPU virtual de NVIDIA** se ejecuta en el dominio de control de XenServer (dom0). Se proporciona como paquete complementario o como archivo RPM. Para obtener más información sobre la instalación, consulte la documentación del software de GPU virtual de NVIDIA.

La actualización se puede instalar en uno de los siguientes métodos:

- Usar XenCenter (**Tools**) > **Instalar actualización** > **Seleccione el paquete de actualización o suplementario del disco**)
- Use el comando `xe-install-supplemental-pack` xe de la CLI.

> **Nota:**
>
> Si va a instalar el administrador de GPU virtual de NVIDIA con un archivo RPM, asegúrese de copiar el archivo RPM en dom0 y, a continuación, realizar la instalación.

1. Use el comando rpm para instalar el paquete:

```
rpm -iv <vgpu_manager_rpm_filename>
<!--NeedCopy-->
```

2. Reinicie el host de XenServer:

```
shutdown -r now
<!--NeedCopy-->
```

3. Tras reiniciar el host de XenServer, compruebe que el software se ha instalado y cargado correctamente comprobando el controlador del kernel de NVIDIA:

```
[root@xenserver ~]#lsmod |grep nvidia
    nvidia            8152994 0
<!--NeedCopy-->
```

4. Verifique que el controlador del kernel de NVIDIA pueda comunicarse correctamente con las GPU físicas de NVIDIA en su host. Ejecute el comando `nvidia-smi` para generar una lista de las GPU de su plataforma similar a:

```
[root@xenserver ~]# nvidia-smi

    Thu Jan 26 13:48:50 2017
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
+-----------------------------------------------------------------------------+
NVIDIA-SMI 367.64  Driver Version: 367.64                 |
-------------------------------+----------------------+----------------------+
 GPU Name    Persistence-M| Bus-Id   Disp.A | Volatile Uncorr. ECC|
Fan Temp  Perf  Pwr:Usage/Cap| Memory-Usage | GPU-Util  Compute M.|
===============================+======================+======================

|  0 Tesla M60       On | 0000:05:00.0    Off|   Off |
| N/A  33C  P8    24W / 150W |   7249MiB /  8191MiB |      0%  Default  |
+-------------------------------+----------------------+----------------------

|  1 Tesla M60       On | 0000:09:00.0    Off |  Off |
| N/A  36C  P8    24W / 150W |   7249MiB /  8191MiB |      0%  Default  |
+-------------------------------+----------------------+----------------------

|  2 Tesla M60       On | 0000:85:00.0    Off |  Off |
| N/A  36C  P8    23W / 150W |   19MiB /  8191MiB |        0%  Default  |
+-------------------------------+----------------------+----------------------

|  3 Tesla M60       On | 0000:89:00.0    Off |  Off |
| N/A  37C    P8    23W / 150W |     14MiB /  8191MiB |    0%  Default  |
+-------------------------------+----------------------+----------------------

+-----------------------------------------------------------------------------+

| Processes:                  GPU Memory |
| GPU    PID  Type  Process name    Usage   |
|=============================================================================

| No running compute processes found |
+-----------------------------------------------------------------------------+

<!--NeedCopy-->
```

Nota:

Cuando utilice NVIDIA vGPU con servidores XenServer que tengan más de 768 GB de RAM, agregue el parámetro `iommu=dom0-passthrough` a la línea de comandos de Xen:

a) Ejecute el siguiente comando en el dominio de control (Dom0):

```
/opt/xensource/libexec/xen-cmdline –-set-xen iommu=dom0-passthrough
```

b) Reinicie el host.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Intel GVT-d y GVT-g

XenServer es compatible con la GPU virtual (GVT-g) de Intel, una solución de aceleración de gráficos que no requiere hardware adicional. Utiliza la función Intel Iris Pro integrada en ciertos procesadores Intel y un controlador de GPU Intel estándar instalado en la VM.

Para garantizar que siempre dispone de las últimas correcciones funcionales y de seguridad, asegúrese de instalar todas las actualizaciones proporcionadas por Intel para los controladores de sus máquinas virtuales y el firmware de su host.

Intel GVT-d y GVT-g son compatibles con las funciones HDX 3D Pro de Citrix Virtual Apps and Desktops o Citrix DaaS. Para obtener más información, consulte HDX 3D Pro.

> **Nota:**
>
> Como la función de gráficos Intel Iris Pro está integrada en los procesadores, las aplicaciones con uso intensivo de la CPU pueden provocar que la energía se desvíe de la GPU. Como resultado, es posible que no experimente una aceleración de gráficos completa como lo hace con las cargas de trabajo que requieren un uso intensivo de la GPU.

Configuración y requisitos del sistema Intel GVT-G (en desuso)

Para utilizar Intel GVT-g, el host XenServer debe tener el siguiente hardware:

- Una CPU que tiene gráficos Iris Pro. Esta CPU debe aparecer como compatible con gráficos en la lista de compatibilidad de hardware
- Una placa madre que tiene un conjunto de chips con gráficos habilitados. Por ejemplo, C226 para CPU Xeon E3 v4 o C236 para CPU Xeon E3 v5.

> **Nota:**
>
> Asegúrese de reiniciar los hosts al cambiar entre la transferencia de GPU Intel (GVT-d) y la GPU virtual Intel (GVT-g).

Al configurar Intel GVT-g, la cantidad de GPU virtuales Intel compatibles con un host XenServer específico depende del tamaño de la barra de GPU. El tamaño de la barra de la GPU se denomina "tamaño de apertura"en el firmware del sistema. Le recomendamos que establezca el tamaño de apertura en 1024 MB para admitir un máximo de siete GPU virtuales por host.

Si configura el tamaño de Aperture en 256 MB, solo se puede iniciar una máquina virtual en el host. Si se establece en 512 MB, solo se iniciarán tres máquinas virtuales en el host de XenServer. No se admite un tamaño de apertura superior a 1024 MB y **no** aumenta la cantidad de máquinas virtuales que se inician en un host.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Habilitar el paso a través de GPU Intel

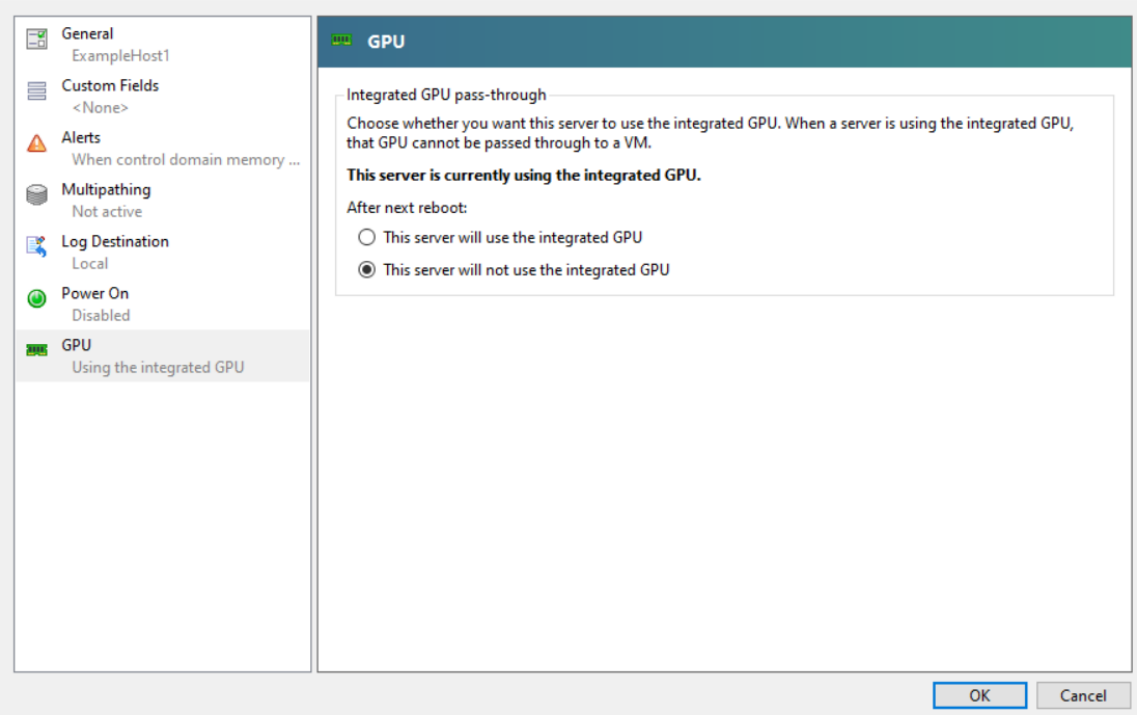
XenServer admite la función de transferencia de GPU para las máquinas virtuales de Windows que utilizan un dispositivo GPU integrado de Intel.

- Para obtener más información sobre las versiones de Windows compatibles con la transferencia de GPU Intel, consulte Gráficos.
- Para obtener más información sobre el hardware compatible, consulte la Lista de compatibilidad de hardware.

Cuando se utiliza una GPU Intel en servidores Intel, el dominio de control (dom0) del servidor XenServer tiene acceso al dispositivo GPU integrado. En tales casos, la GPU está disponible para la transferencia. Para usar la función de transferencia de GPU de Intel en los servidores Intel, inhabilite la conexión entre dom0 y la GPU antes de pasar a través de la GPU a la VM.

Para inhabilitar esta conexión, siga estos pasos:

1. En el panel **Recursos**, elija el host de XenServer.
2. En la ficha **General**, haga clic en **Propiedades**y, en el panel izquierdo, haga clic en **GPU**.
3. En la sección **Paso a través de GPU integrada**, seleccione **Este servidor no usará la GPU integrada**.



   Este paso inhabilita la conexión entre dom0 y el dispositivo GPU integrado Intel.

4. Haga clic en **Aceptar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Reinicie el host de XenServer para que los cambios surtan efecto.

   La GPU Intel ahora está visible en la lista de tipos de GPU durante la creación de una nueva VM y en la ficha **Propiedades** de la VM.

   > **Nota:**
   >
   > La salida de consola externa del host XenServer (por ejemplo, VGA, HDMI, DP) no estará disponible después de inhabilitar la conexión entre dom0 y la GPU.

Crear máquinas virtuales habilitadas para vGPU

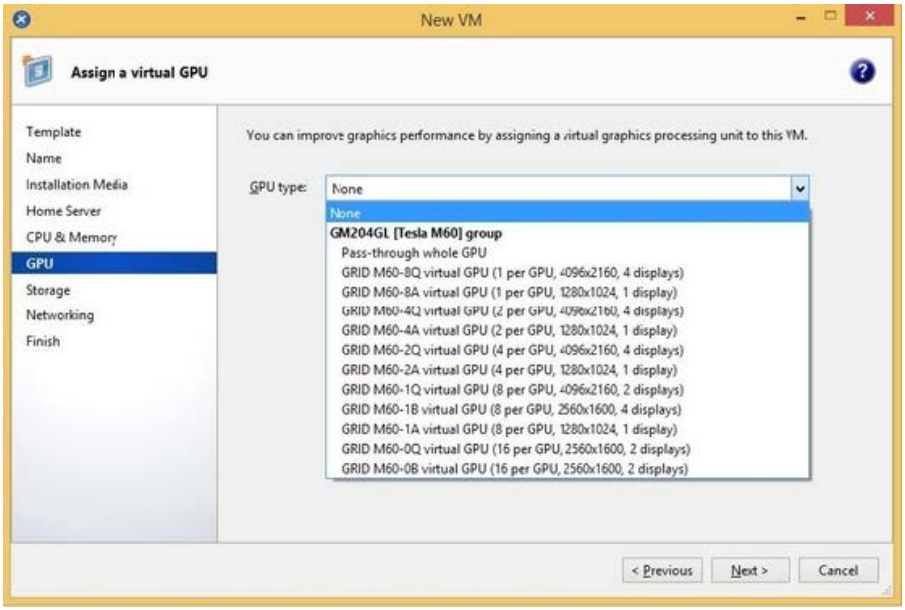
February 23, 2024

En esta sección se proporcionan instrucciones paso a paso sobre cómo crear una GPU virtual o una VM habilitada para paso a través de GPU.

> **Nota:**
>
> Si utiliza la función de transferencia de GPU Intel, consulte primero la sección *Habilitación de la transferencia de GPU Intel para obtener más información sobre la configuración y, a* continuación, complete los pasos siguientes.

1. Cree una máquina virtual con XenCenter. Seleccione el host en el panel Recursos y, a continuación, seleccione **Nueva VM** en el menú VM.
2. Siga las instrucciones de la configuración de la **nueva máquina virtual** y seleccione los **medios de instalación**, el **servidor doméstico**y **la CPU y la memoria**.
3. Los hosts habilitados para GPU muestran una página de configuración de **GPU** :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Haga clic en **Agregar**. En la lista **Tipo de GPU**, seleccione **Transferencia de GPU completa** o un tipo de GPU virtual.

   Los tipos de GPU virtuales no disponibles aparecen atenuados.

   Si quiere asignar varias vGPU a su VM, asegúrese de seleccionar un tipo de vGPU que admita varias vGPU. Repita este paso para agregar más vGPU del mismo tipo.

5. Haga clic en **Siguiente** para configurar **Almacenamiento** y, a continuación, **Redes**.

6. Después de completar la configuración, haga clic en **Crear ahora**.

Instalación de XenServer VM Tools

Sin los controladores de almacenamiento y redes optimizados que proporcionan las herramientas de máquinas virtuales de XenServer, las aplicaciones gráficas remotas que se ejecutan en la vGPU de NVIDIA **no** ofrecen el máximo rendimiento.

- Si su máquina virtual es una máquina virtual de Windows, debe instalar XenServer VM Tools para Windows en su máquina virtual. Para obtener más información, consulte Instalar XenServer VM Tools para Windows.
- Si su máquina virtual es una máquina virtual Linux, puede instalar XenServer VM Tools for Linux en su máquina virtual. Para obtener más información, consulte Instalar XenServer VM Tools para Linux.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Instale los controladores para invitados

Al ver la consola de VM en XenCenter, la VM normalmente se inicia en el escritorio en modo VGA con una resolución de 800 x 600. Los controles de resolución de pantalla estándar de Windows se pueden usar para aumentar la resolución a otras resoluciones estándar. (**Panel de control > Pantalla > Resolución de pantalla**)

> **Nota:**
>
> Cuando utilice la transferencia de GPU, le recomendamos que instale los controladores integrados en el servidor invitado a través de RDP o VNC a través de la red. Es decir, no a través de XenCenter.

Para garantizar que siempre tenga las últimas correcciones funcionales y de seguridad, asegúrese de llevar siempre las actualizaciones más recientes a los controladores invitados.

Instale los controladores de NVIDIA

Para habilitar el funcionamiento de vGPU (como para una GPU NVIDIA física), instale los controladores NVIDIA en la VM.

En la siguiente sección se proporciona una descripción general del procedimiento. Para obtener instrucciones detalladas, consulte la documentación del software de GPU virtual de NVIDIA.

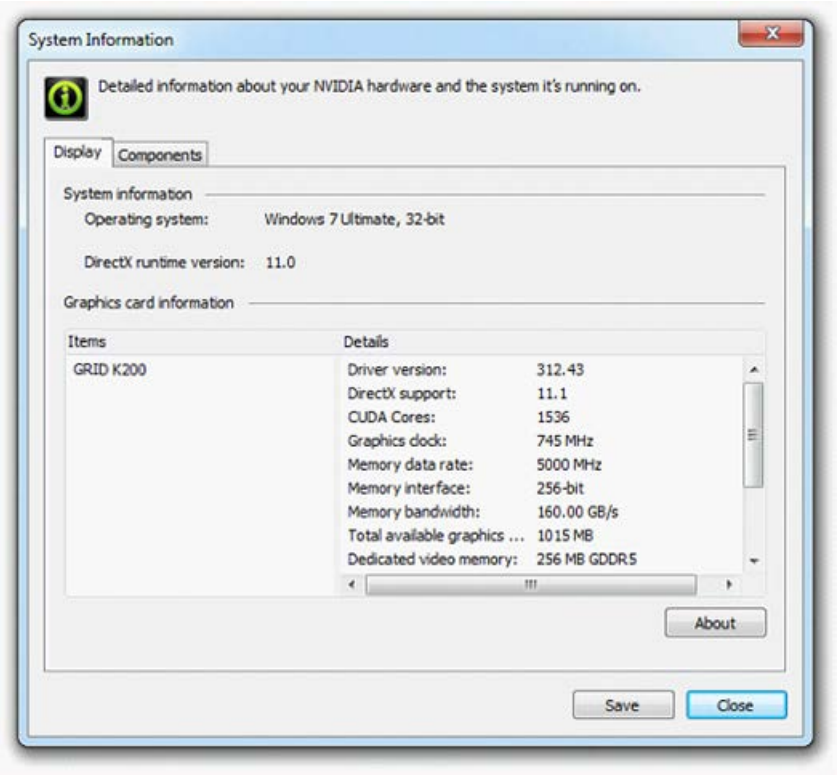
1. Inicie la VM. En el panel **Recursos**, haga clic con el botón derecho en la VM y haga clic en **Iniciar**.

   Durante este proceso de inicio, XenServer asigna dinámicamente una vGPU a la máquina virtual.

2. Siga las pantallas de instalación del sistema operativo Windows.
3. Cuando finalice la instalación del sistema operativo, reinicie la VM.
4. Instale el controlador apropiado para la GPU dentro del invitado. El siguiente ejemplo muestra el caso específico de la instalación en invitado de los controladores NVIDIA GRID.
5. Copie el paquete de controladores de Windows de 64 bits de NVIDIA en la máquina virtual, abra el archivo zip y ejecute setup.exe.
6. Siga los pasos del instalador para instalar el controlador.
7. Una vez completada la instalación del controlador, es posible que se le pida que reinicie la VM. Seleccione **Reiniciar ahora** para reiniciar la máquina virtual de inmediato, o bien, salga del paquete del instalador y reinicie la máquina virtual cuando esté lista. Cuando se inicia la VM, se inicia en un escritorio de Windows.
8. Para verificar que el controlador de NVIDIA se está ejecutando, haga clic con el botón secundario en el escritorio y seleccione **Panel de control de NVIDIA**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

9. En el Panel de control de NVIDIA, seleccione **Información del sistema**. Esta interfaz muestra el tipo de GPU que utiliza la máquina virtual, sus funciones y la versión del controlador de NVIDIA en uso:



> **Nota:**
>
> Según la tarjeta gráfica NVIDIA utilizada, es posible que necesites una suscripción o una licencia de NVIDIA. Para obtener más información, consulte la información del producto NVIDIA.

La VM ahora está lista para ejecutar la gama completa de aplicaciones gráficas DirectX y OpenGL compatibles con la GPU.

Para máquinas virtuales Linux

En su máquina virtual Linux, instale el controlador según las instrucciones de las guías de usuario de NVIDIA.

Si su máquina virtual Linux arranca en modo de arranque seguro UEFI, es posible que deba tomar medidas adicionales para firmar el controlador. Para obtener más información, consulte Instalar controladores de terceros en su máquina virtual Linux de arranque seguro.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

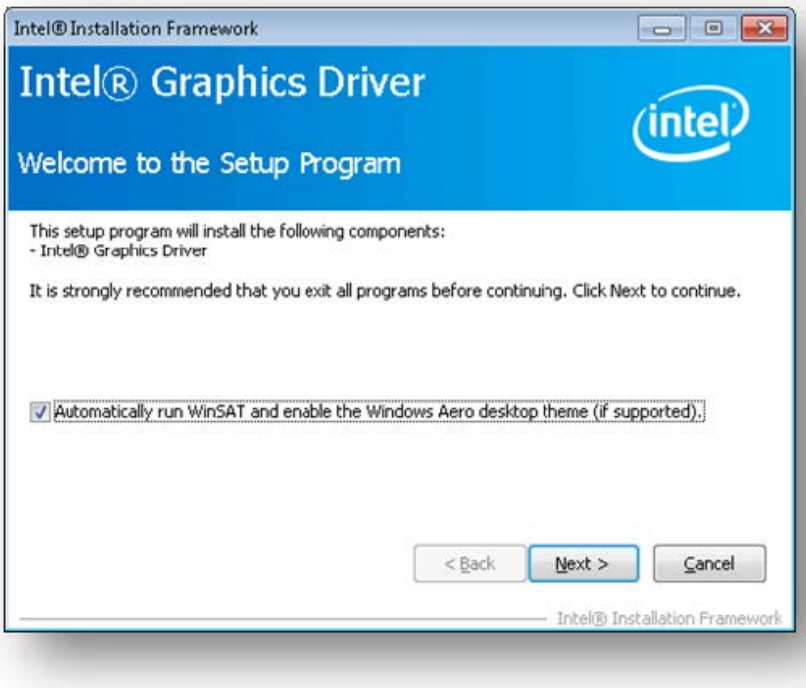
Instalación de los controladores Intel (obsoletos)

Para habilitar el funcionamiento de la GPU, instale los controladores Intel en la VM.

1. Inicie la **máquina virtual**. En el panel **Recursos**, haga clic con el botón derecho en la VM y haga clic en **Iniciar**.

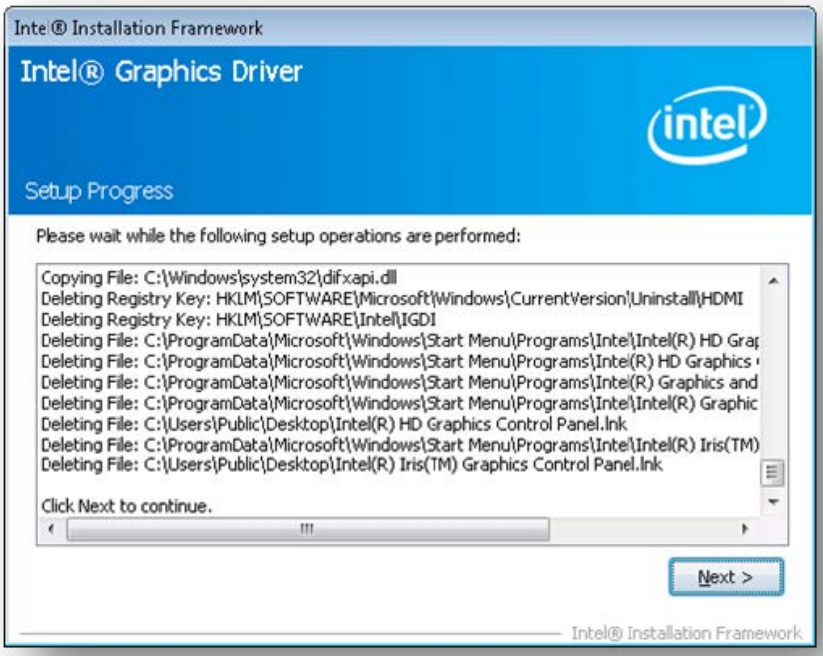
   Durante este proceso de arranque, XenServer asigna dinámicamente una GPU a la máquina virtual.

2. Siga las pantallas de instalación del sistema operativo Windows.
3. Cuando finalice la instalación del sistema operativo, reinicie la VM.
4. Copie el controlador Intel Windows de 64 bits (controlador de gráficos Intel) en la máquina virtual.
5. Ejecute el programa de configuración del **controlador de gráficos Intel**.
6. Seleccione **Ejecutar WinSAT automáticamente**y, a continuación, haga clic en **Siguiente**.



7. Para aceptar el Acuerdo de licencia, haga clic en **Sí**y, en la pantalla Información del archivo Léame, haga clic en **Siguiente**.
8. Espere hasta que se completen las operaciones de configuración. Cuando se le solicite, haga clic en **Siguiente**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



9. Para completar la instalación, se le pedirá que reinicie la VM. Seleccione **Sí**, deseo reiniciar este equipo ahora y haga clic en **Finalizar**.
10. Después de que la VM se reinicie, compruebe que los gráficos funcionan correctamente. Abra el Administrador de dispositivos de Windows, expanda **Adaptadores de pantalla**y asegúrese de que el adaptador de gráficos Intel no tenga ningún símbolo de advertencia.

> **Nota:**
>
> Puede obtener los controladores más recientes en el sitio web de Intel.

---

layout: doc
description: Configure the amount of memory allocated to the control domain (dom0) of a XenServer host.—

Uso de memoria

Dos componentes contribuyen al consumo de memoria del host de XenServer. Primero, la memoria consumida por el propio hipervisor Xen. En segundo lugar, está la memoria consumida por el *dominio de control* del host. También conocido como “Domain0”o “dom0”, el dominio de control es una

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

máquina virtual Linux segura y con privilegios que ejecuta la pila de herramientas de administración de XenServer (XAPI). Además de proporcionar funciones de administración de XenServer, el dominio de control también ejecuta la pila de controladores que proporciona acceso a las máquinas virtuales creadas por el usuario a los dispositivos físicos.

Memoria de dominio de control

La cantidad de memoria asignada al dominio de control se ajusta automáticamente y se basa en la cantidad de memoria física en el host físico. De forma predeterminada, XenServer asigna **1 GiB más el 5% de la memoria física total** al dominio de control, hasta un máximo inicial de 8 GiB.

> **Nota:**
>
> La cantidad indicada en la sección XenServer de XenCenter incluye la memoria utilizada por el dominio de control (dom0), el propio hipervisor Xen y el kernel que se bloquea. Por lo tanto, la cantidad de memoria informada en XenCenter puede superar estos valores. La cantidad de memoria utilizada por el hipervisor es mayor para los hosts que utilizan más memoria.

Cambiar la cantidad de memoria asignada al dominio de control

Puede cambiar la cantidad de memoria asignada a dom0 mediante XenCenter o mediante la línea de comandos. Si aumenta la cantidad de memoria asignada al dominio de control por encima de la cantidad asignada de forma predeterminada, esta acción provoca que haya menos memoria disponible para las VM.

Es posible que necesite aumentar la cantidad de memoria asignada al dominio de control de un host de XenServer en los siguientes casos:

- Está ejecutando muchas máquinas virtuales en el host
- Está utilizando PVS-Accelerator
- Está utilizando el almacenamiento en caché de lectura

> **Importante:**
>
> Si utiliza una SR de GFS2 y alguno de estos casos también se aplica a su entorno, debe aumentar la cantidad de memoria del dominio de control. Una memoria insuficiente del dominio de control puede provocar inestabilidad en la red y problemas en las agrupaciones en clústeres con la SR de GFS2.

La cantidad de memoria que se debe asignar al dominio de control depende de su entorno y de los requisitos de sus máquinas virtuales.

Puede supervisar las siguientes métricas para determinar si la cantidad de memoria de dominio de control es apropiada para su entorno y qué efectos tienen los cambios que realice:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Actividad de intercambio:** Si el dominio de control se está intercambiando, aumente la memoria del dominio de control.
- **Modo Tapdisk:puede supervisar si los discos Tapdisk están en modo de poca memoria desde la pestaña Rendimiento de XenCenter del host.**Seleccione**Acciones**>**Nuevo gráfico**y elija el gráfico**Tapdisks en modo de memoria baja**. Si un tapdisk está en modo de memoria baja, aumente la memoria del dominio de control.
- **Presión de caché de página:** Use el comando `top` para supervisar la métrica `buff/cache` . Si este número llega a ser demasiado bajo, es posible que quiera aumentar la memoria del dominio de control.

Cambiar la memoria dom0 mediante XenCenter

Para obtener información sobre cómo cambiar la memoria dom0 mediante XenCenter, consulte Cambiar la memoria de dominio de control en la documentación de XenCenter.

> **Nota:**
>
> No puede usar XenCenter para reducir la memoria dom0 por debajo del valor que se estableció inicialmente durante la instalación de XenServer. Para realizar este cambio, debe usar la línea de comandos.

Cambiar la memoria dom0 mediante la línea de comandos

> **Nota:**
>
> En hosts con memoria más pequeña (menos de 16 GiB), es posible que quiera reducir la memoria asignada al dominio de control a un valor inferior al valor predeterminado de la instalación. Puede usar la línea de comandos para realizar este cambio. Sin embargo, le recomendamos que **no reduzca la memoria dom0 por debajo de 1 GiB** y que realice esta operación bajo la dirección del equipo de soporte.

1. En el host de XenServer, abra un shell local e inicie sesión como root.
2. Escriba lo siguiente:

```
/opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=<nn>M,max:<
   nn>M
<!--NeedCopy-->
```

   Donde <nn> representa la cantidad de memoria, en MiB, que se asignará a dom0.

3. Reinicie el host de XenServer mediante XenCenter o el comando `reboot` de la consola de XenServer.

   Cuando el host se reinicie, en la consola de XenServer, ejecute `free` el comando para comprobar la nueva configuración de memoria.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Cuánta memoria hay disponible para las VM?

Para averiguar cuánta memoria del host está disponible para asignarla a las máquinas virtuales, busque el valor de la memoria libre del host ejecutando `memory-free`. A continuación, escriba el comando `vm-compute-maximum-memory` para obtener la cantidad real de memoria libre que se puede asignar a la VM. Por ejemplo:

```
xe host-list uuid=host_uuid params=memory-free
xe vm-compute-maximum-memory vm=vm_name total=host_memory_free_value
<!--NeedCopy-->
```

---

layout: doc
description: Use performance metrics exposed through Round Robin Databases (RRDs) to monitor your XenServer environment.—

Supervise y administre su implementación

XenServer proporciona una supervisión detallada de las métricas de rendimiento. Estas métricas incluyen información de CPU, memoria, disco, red, estado C/estado P y almacenamiento. Cuando corresponda, estas métricas están disponibles por host y por VM. Estas métricas están disponibles directamente o se puede acceder a ellas y verlas gráficamente en XenCenter u otras aplicaciones de terceros.

XenServer también proporciona alertas del sistema y del rendimiento. Las alertas son notificaciones que se producen en respuesta a eventos del sistema seleccionados. Estas notificaciones también se producen cuando uno de los siguientes valores supera un umbral específico en un host administrado, VM o repositorio de almacenamiento: uso de la CPU, uso de la red, uso de la memoria, uso de la memoria del dominio de control, rendimiento del almacenamiento o uso del disco de la máquina virtual. Puede configurar las alertas mediante la CLI xe o XenCenter. Para crear notificaciones basadas en cualquiera de las métricas de rendimiento de máquinas virtuales o hosts disponibles, consulte Alertas de rendimiento.

Supervise el rendimiento de XenServer

Los clientes pueden supervisar el rendimiento de sus hosts y máquinas virtuales (VM) de XenServer mediante las métricas expuestas en las bases de datos Round Robin (RRD). Estas métricas se pueden consultar a través de HTTP o a través de la herramienta RRD2CSV. Además, XenCenter usa estos datos

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

para producir gráficos de rendimiento del sistema. Para obtener más información, consulte Analizar y visualizar métricas.

En las tablas siguientes se enumeran todas las métricas de host y VM disponibles.

> **Notas:**
>
> - La latencia durante un período se define como la latencia promedio de las operaciones durante ese período.
> - La disponibilidad y la utilidad de ciertas métricas dependen de la SR y la CPU.
> - Las métricas de rendimiento no están disponibles para los SR de GFS2 y los discos en esos SR.

Métricas de host disponibles

Nombre de métrica	Descripción	Condición	Nombre de XenCenter
`avgqu_sz_<sr-uuid-short>`	Tamaño medio de cola de E/S (solicitudes).	Al menos un VBD conectado en `<sr-uuid-short>` de SR en el host	`sr-uuid-short` Tamaño de cola
`cpu<cpu>-C<cstate>`	Tiempo que la CPU `cpu` pasa en estado C `cstate` en milisegundos.	El estado C existe en la CPU	Estado C `cstate` de CPU `cpu`
`cpu<cpu>-P<pstate>`	Tiempo que la CPU `cpu` pasa en estado P `pstate` en milisegundos.	El estado P existe en la CPU	Estado P `pstate` de CPU `cpu`
`cpu<cpu>`	Utilización de CPU física `cpu` (fracción). Habilitado de forma predeterminada.	La CPU `cpu` existe	CPU `cpu`
`cpu_avg`	Utilización media de las CPU físicas (fracción). Habilitado de forma predeterminada.	Ninguno	CPU promedio

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre de métrica	Descripción	Condición	Nombre de XenCenter
hostload	Carga de host por CPU física, donde la carga se refiere a la cantidad de vCPU en estado de ejecución o ejecutables.	Ninguno	Carga de la CPU del host
inflight_<sr-uuid-**short**>	Número de solicitudes de E/S actualmente en curso. Habilitado de forma predeterminada.	Al menos un VBD conectado en sr de SR en el host	sr Solicitudes en proceso
io_throughput_read_<sr-uuidshort>	Datos leídos de SR (MiB/s).	Al menos un VBD conectado en sr de SR en el host	sr Rendimiento de lectura
io_throughput_write_<sr-uuidshort>	Datos escritos en el SR (MiB/s).	Al menos un VBD conectado en sr de SR en el host	sr Rendimiento de escritura
io_throughput_total_<sr-uuidshort>	Todas las E/S de SR (MiB/s).	Al menos un VBD conectado en sr de SR en el host	sr Rendimiento total
iops_read_<sr-uuid-**short**>	Lee las solicitudes por segundo.	Al menos un VBD conectado en sr de SR en el host	sr Leer IOPS
iops_write_<sr-uuid-**short**>	Solicitudes de escritura por segundo.	Al menos un VBD conectado en sr de SR en el host	sr Escritura de IOPS
iops_total_<sr-uuid-**short**>	Solicitudes de E/S por segundo.	Al menos un VBD conectado en sr de SR en el host	sr IOPS totales
iowait_<sr-uuid-**short**>	Porcentaje del tiempo de espera de E/S.	Al menos un VBD conectado en sr de SR en el host	sr E/S espera
latency_<sr-uuid-**short**>	Latencia de E/S promedio (milisegundos).	Al menos un VBD conectado en sr de SR en el host	sr Latencia

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre de métrica	Descripción	Condición	Nombre de XenCenter
`loadavg`	Promedio de carga de Domain0. Habilitada de forma predeterminada	Ninguno	Carga de dominio de control
`memory_free_kib`	Cantidad total de memoria libre (KiB). Habilitado de forma predeterminada.	Ninguno	*No está presente en XenCenter. Sustituido por memoria usada.*
La pila de herramientas no lo informa. Calculado por XenCenter.	Cantidad total de memoria utilizada (KiB). Habilitado de forma predeterminada.	Ninguno	Memoria usada
`memory_reclaimed`	Memoria del host recuperada por squeeze (B).	Ninguno	Memoria recuperada
`memory_reclaimed_max`	Memoria host disponible para recuperar con squeeze (B).	Ninguno	Memoria recuperada potencial
`memory_total_kib`	Cantidad total de memoria (KiB) en el host. Habilitado de forma predeterminada.	Ninguno	Memoria total
`network`/`latency`	Intervalo en segundos entre los dos últimos latidos transmitidos desde el anfitrión local a todos los servidores en línea. Inhabilitado de forma predeterminada.	HA habilitado	Latencia de red

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre de métrica	Descripción	Condición	Nombre de XenCenter
statefile/<vdi_uuid>/latency	Tiempo de respuesta en segundos del último acceso a archivos de estado desde el host local. Inhabilitado de forma predeterminada.	HA habilitado	Latencia de archivos de estado HA
pif_<pif>_rx	Bytes por segundo recibidos en la interfaz física pif. Habilitado de forma predeterminada.	Existe PIF	XenCenter-pifname Recibir (ver nota)
pif_<pif>_tx	Bytes por segundo enviados en la interfaz física pif. Habilitado de forma predeterminada.	Existe PIF	XenCenter-pifname Enviar (ver nota)
pif_<pif>_rx_errors	Recibir errores por segundo en la interfaz física pif. Inhabilitado de forma predeterminada.	Existe PIF	XenCenter-pifname Errores de recepción (ver nota)
pif_<pif>_tx_errors	Transmitir errores por segundo en la interfaz física pif. Inhabilitado de forma predeterminada	Existe PIF	XenCenter-pifname Errores de envío (ver nota)
pif_aggr_rx	Bytes por segundo recibidos en todas las interfaces físicas. Habilitado de forma predeterminada.	Ninguno	Recepción total de NIC
pif_aggr_tx	Bytes por segundo enviados en todas las interfaces físicas. Habilitado de forma predeterminada.	Ninguno	Envío NIC total

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre de métrica	Descripción	Condición	Nombre de XenCenter
pvsaccelerator_evicted	Bytes por segundo expulsados de la memoria caché	PVSAccelerator habilitado	Tasa de desalojos del acelerador de PV
pvsaccelerator_hits	Lecturas por segundo servidas desde la memoria caché	PVSAccelerator habilitado	Tasa de aciertos del acelerador PVS
pvsaccelerator_misses	Lecturas por segundo que no se pueden servir desde la memoria caché	PVSAccelerator habilitado	Tasa de fallos del acelerador PVS
pvsaccelerator_traffic_client	Bytes por segundo enviados por clientes PVS almacenados en caché	PVSAccelerator habilitado	PVS-Accelerator observó tráfico de red de los clientes
pvsaccelerator_traffic_server	Bytes por segundo enviados por servidores PVS almacenados en caché	PVSAccelerator habilitado	PVS-Accelerator observó tráfico de red desde los servidores
pvsaccelerator_reads_total	Lecturas por segundo observadas por la memoria caché	PVSAccelerator habilitado	Velocidad de lectura observada del acelerador PVS
pvsaccelerator_traffic_saved	Bytes por segundo enviados por PVSAccelerator en lugar del servidor PVS	PVSAccelerator habilitado	PVS-Accelerator ahorra tráfico de red
pvsaccelerator_space_utilization	Porcentaje de espacio utilizado por PVSAccelerator en este host, en comparación con el tamaño total del almacenamiento en caché	PVSAccelerator habilitado	Utilización del espacio del acelerador PVS
running_vcpus	La cantidad total de vCPU en ejecución	Ninguno	Cantidad de vCPU en ejecución

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre de métrica	Descripción	Condición	Nombre de XenCenter
running_domains	La cantidad total de dominios en ejecución, incluido dom0 (el dominio de control del host)	Ninguno	Cantidad de dominios en ejecución
sr_<sr>_cache_size	Tamaño en bytes de IntelliCache SR. Habilitado de forma predeterminada.	IntelliCache habilitado	Tamaño de caché de IntelliCache
sr_<sr>_cache_hits	Visitas de caché por segundo. Habilitado de forma predeterminada.	IntelliCache habilitado	Visitas de caché de IntelliCache
sr_<sr>_cache_misses	Fallos de caché por segundo. Habilitado de forma predeterminada.	IntelliCache habilitado	Falta de caché de IntelliCache
xapi_allocation_kib	Asignación de memoria (KiB) realizada por el demonio XAPI. Habilitado de forma predeterminada.	Ninguno	Asignación de memoria de
xapi_free_memory_kib	Memoria libre (KiB) disponible para el demonio XAPI. Habilitado de forma predeterminada.	Ninguno	Memoria de agente libre
xapi_healthcheck/latency	Tiempo de respuesta en segundos de la última llamada de supervisión de estado de XAPI en el host local. Inhabilitado de forma predeterminada.	Alta disponibilidad habilitada	Latencia de alta disponibilidad de XenServer

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre de métrica	Descripción	Condición	Nombre de XenCenter
xapi_live_memory_kib	Memoria en vivo (KiB) utilizada por el demonio XAPI. Habilitado de forma predeterminada.	Ninguno	Memoria del agente en vivo
xapi_memory_usage_kib	Memoria total (KiB) asignada utilizada por el demonio XAPI. Habilitado de forma predeterminada.	Ninguno	Uso de memoria del agente

Métricas de VM disponibles

Nombre de métrica	Descripción	Condición	Nombre de XenCenter
cpu<cpu>	Utilización de vCPU cpu (fracción). Habilitada de forma predeterminada	La vCPU cpu existe	CPU
cpu_usage	Uso de la CPU del dominio	Ninguno	cpu_usage
memory	Memoria asignada actualmente a la VM (bytes) .Habilitada de forma predeterminada	Ninguno	Memoria total
memory_target	Destino del controlador de globo de máquina virtual (bytes). Habilitada de forma predeterminada	Ninguno	Objetivo de memoria
memory_internal_free	Memoria utilizada según lo informado por el agente invitado (KiB). Habilitada de forma predeterminada	Ninguno	Memoria libre

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre de métrica	Descripción	Condición	Nombre de XenCenter
runstate_fullrun	Fracción de tiempo que se ejecutan todas las vCPU.	Ninguno	Ejecución completa de vCPU
runstate_full_contention	Fracción de tiempo que se pueden ejecutar todas las vCPU (es decir, esperando la CPU)	Ninguno	Contención completa de vCPUs
runstate_concurrency_hazard	Fracción de tiempo que algunas CPU virtuales se ejecutan y otras se pueden ejecutar	Ninguno	Riesgo de concurrencia de CPU
runstate_blocked	Fracción de tiempo que todas las vCPU están bloqueadas o sin conexión	Ninguno	vCPU inactivas
runstate_partial_run	Fracción de tiempo que algunas CPU virtuales se ejecutan y otras están bloqueadas	Ninguno	Ejecución parcial de vCPU
runstate_partial_contention	Fracción de tiempo que algunas CPU virtuales se pueden ejecutar y otras están bloqueadas	Ninguno	Conflicto parcial de vCPU
vbd_<vbd>_write	Escribe en el dispositivo vbd en bytes por segundo. Habilitada de forma predeterminada	El VBD vbd existe	Escritura vbd en disco
vbd_<vbd>_read	Lee desde el dispositivo vbd en bytes por segundo. Habilitado de forma predeterminada.	El VBD vbd existe	Lectura vbd de disco

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre de métrica	Descripción	Condición	Nombre de XenCenter
vbd_<vbd>_write_latency	Escribe en el dispositivo vbd en microsegundos.	El VBD vbd existe	Latencia de escritura en disco vbd
vbd_<vbd>_read_latency	Lee desde el dispositivo vbd en microsegundos.	El VBD vbd existe	Latencia de lectura de disco vbd
vbd <vbd>_iops_read	Lee las solicitudes por segundo.	Al menos un VBD conectado para VDI no ISO en el host	IOPS de lectura de disco vbd
vbd <vbd>_iops_write	Solicitudes de escritura por segundo.	Al menos un VBD conectado para VDI no ISO en el host	IOPS de escritura en disco vbd
vbd <vbd>_iops_total	Solicitudes de E/S por segundo.	Al menos un VBD conectado para VDI no ISO en el host	IOPS totales de disco vbd
vbd <vbd>_iowait	Porcentaje de tiempo de espera de I/0.	Al menos un VBD conectado para VDI no ISO en el host	Espera de E/S de disco vbd
vbd <vbd>_inflight	Número de solicitudes de E/S actualmente en curso.	Al menos un VBD conectado para VDI no ISO en el host	Solicitudes en proceso de disco vbd
vbd <vbd>_avgqu_sz	Tamaño de cola de E/S promedio.	Al menos un VBD conectado para VDI no ISO en el host	Tamaño de cola de disco vbd
vif_<vif>_rx	Bytes por segundo recibidos en el número de interfaz virtual vif. Habilitado de forma predeterminada.	La VIF vif existe	vif Recibir
vif_<vif>_tx	Bytes por segundo transmitidos en la interfaz virtual vif. Habilitado de forma predeterminada.	La VIF vif existe	vif Enviar

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre de métrica	Descripción	Condición	Nombre de XenCenter
vif_<vif>_rx_errors	Recibe errores por segundo en la interfaz virtual vif. Habilitado de forma predeterminada.	La VIF vif existe	vif Recibir errores
vif_<vif>_tx_errors	Transmite errores por segundo en la interfaz virtual vif Habilitado de forma predeterminada.	La VIF vif existe	vif Enviar errores

> **Nota:**
>
> El valor de <XenCenter-pif-name> puede ser cualquiera de los siguientes:
>
> - NIC <pif>: Si <pif> contiene pif_eth#, donde ## es 0—9
> - <pif>: Si <pif> contiene pif_eth#.## o pif_xenbr## o pif_bond##
> - <Internal> Network <pif>: Si <pif> contiene pif_xapi##, (tenga en cuenta que <Internal> aparece tal cual)
> - TAP <tap>: Si <pif> contiene pif_tap##
> - xapi Loopback: Si <pif> contiene pif_lo

Analice y visualice métricas

La ficha Rendimiento de XenCenter proporciona supervisión en tiempo real de las estadísticas de rendimiento en los grupos de recursos, además de las tendencias gráficas del rendimiento de las máquinas virtuales y físicas. Los gráficos que muestran la CPU, la memoria, la red y la E/S de disco se incluyen en la ficha Rendimiento de forma predeterminada. Puede agregar más métricas, cambiar el aspecto de las gráficas existentes o crear otras adicionales. Para obtener más información, consulte *Configuración de métricas* en la siguiente sección.

- Puede ver hasta 12 meses de datos de rendimiento y hacer zoom para observar más de cerca los picos de actividad.
- XenCenter puede generar alertas de rendimiento cuando el uso de CPU, memoria, E/S de red, E/S de almacenamiento o E/S de disco supera un umbral específico en un host, máquina virtual o SR. Para obtener más información, consulte *Alertas* en la siguiente sección.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Instale XenServer VM Tools para ver todos los datos de rendimiento de las máquinas virtuales.

Configurar gráficos de rendimiento **Para agregar un gráfico:**

1. En la ficha **Rendimiento**, haga clic en **Acciones** y, a continuación, en **Nuevo gráfico**. Se muestra el cuadro de diálogo Nuevo gráfico.
2. En el campo **Nombre**, introduzca un nombre para la gráfica.
3. En la lista de **Fuentes de datos**, seleccione las casillas de verificación de las fuentes de datos que quiere incluir en el gráfico.
4. Haga clic en **Guardar**.

Para modificar un gráfico existente:

1. Vaya a la ficha **Rendimiento** y seleccione el gráfico que quiere modificar.
2. Haga clic con el botón secundario en el gráfico y seleccione **Acciones**, o haga clic en el botón **Acciones**. A continuación, selecciona **Modificar gráfico**.
3. En la ventana de detalles del gráfico, realice los cambios necesarios y haga clic en **Aceptar**.

Configurar el tipo de gráfico Los datos de los gráficos de rendimiento se pueden mostrar como líneas o áreas. Para cambiar el tipo de gráfica:

1. En el menú **Herramientas**, haga clic en **Opciones** y seleccione **Gráficas**.
2. Para ver los datos de rendimiento como un gráfico de líneas, haga clic en la opción **Gráfico de líneas**.
3. Para ver los datos de rendimiento como un gráfico de área, haga clic en la opción **Gráfico de área**.
4. Haga clic en **OK** para guardar los cambios.

Los detalles completos para configurar y ver gráficos de rendimiento de XenCenter se pueden encontrar en la documentación de XenCenter en la sección Supervisión del rendimiento del sistema.

Configurar métricas

> **Nota:**
>
> Los estados C y P son funciones de administración de energía de algunos procesadores. El rango de estados disponibles depende de las capacidades físicas del host, así como de la configuración

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> de administración de energía.

Los comandos de host y VM devuelven lo siguiente:

- Descripción completa de la fuente de datos
- Las unidades aplicadas a la métrica
- El rango de valores posibles que se pueden usar

Por ejemplo:

```
    name_label: cpu0-C1
    name_description: Proportion of time CPU 0 spent in C-state 1
    enabled: true
    standard: true
    min: 0.000
    max: 1.000
    units: Percent
<!--NeedCopy-->
```

Habilitar una métrica específica La mayoría de las métricas están habilitadas y recopiladas de forma predeterminada. Para habilitar las métricas que no lo están, introduzca lo siguiente:

```
xe host-data-source-record data-source=metric name host=hostname
<!--NeedCopy-->
```

Desactivar una métrica específica Es posible que no quieras recopilar determinadas métricas con regularidad. Para inhabilitar una métrica previamente habilitada, introduzca lo siguiente:

```
xe host-data-source-forget data-source=metric name host=hostname
<!--NeedCopy-->
```

Mostrar una lista de métricas de host habilitadas actualmente Para enumerar las métricas de host que se están recopilando actualmente, introduce lo siguiente:

```
xe host-data-source-list host=hostname
<!--NeedCopy-->
```

Mostrar una lista de métricas de VM habilitadas actualmente Para alojar las métricas de VM que se recopilan actualmente, introduzca lo siguiente:

```
xe vm-data-source-list vm=vm_name
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Usar RRD

XenServer usa los RRD para almacenar las métricas de rendimiento. Estos RRD consisten en varios archivos Round Robin (RRA) en una base de datos de tamaño fijo.

Cada archivo de la base de datos muestrea su métrica particular en una granularidad específica:

- Cada 5 segundos durante 10 minutos
- Cada minuto de las últimas dos horas
- Cada hora de la semana pasada
- Todos los días del año pasado

El muestreo que se lleva a cabo cada cinco segundos registra los puntos de datos reales; sin embargo, los siguientes RRA utilizan funciones de consolidación en su lugar. Las funciones de consolidación que admite XenServer son:

- PROMEDIO
- MIN
- MÁXIMO

Existen RRD para máquinas virtuales individuales (incluida dom0) y para el host de XenServer. Los RRD de VM se almacenan en el host en el que se ejecutan o en el coordinador del grupo cuando no se están ejecutando. Por lo tanto, se debe conocer la ubicación de una VM para recuperar los datos de rendimiento asociados.

Para obtener información detallada sobre cómo usar los RRD de XenServer, consulte la Guía del kit de desarrollo de software de XenServer.

Analizar RRD mediante HTTP

Puede descargar los RRD a través de HTTP desde el host de XenServer especificado mediante el controlador HTTP registrado en o. `/host_rrd`/`vm_rrd` Ambas direcciones requieren autenticación mediante autenticación HTTP o proporcionando referencias de sesión de API de administración válidas como argumento de consulta. Por ejemplo:

Descargar un RRD de host.

```
wget http://server/host_rrd?session_id=OpaqueRef:SESSION HANDLE>
<!--NeedCopy-->
```

Descargar un RRD de VM.

```
wget http://server/vm_rrd?session_id=OpaqueRef:SESSION HANDLE>&uuid=VM
    UUID>
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ambas llamadas descargan XML en un formato que puede importarse en `rrdtool` para análisis o analizarse directamente.

Analizar los RRD mediante rrd2csv

Además de ver las métricas de rendimiento en XenCenter, la herramienta rrd2csv registra los RRD en formato de valores separados por comas (CSV). Se proporcionan páginas de manual y de ayuda. Para mostrar las páginas de manual o de ayuda de la herramienta rrd2csv, ejecute el siguiente comando:

```
man rrd2csv
<!--NeedCopy-->
```

O bien

```
rrd2csv --help
<!--NeedCopy-->
```

> **Nota:**
>
> Cuando se utilizan varias opciones, suminístrelas individualmente. Por ejemplo: para devolver tanto el UUID como la etiqueta de nombre asociada a una VM o un host, llama a rrd2csv como se muestra a continuación:
>
> `rrd2csv -u -n`
>
> El UUID devuelto es único y adecuado como clave principal; sin embargo, la etiqueta del nombre de una entidad puede no ser necesariamente única.

La página de manual (`rrd2csv --help`) es el texto de ayuda definitivo de la herramienta.

Alertas

Puede configurar XenServer para que genere alertas en función de cualquiera de las métricas de host o máquina virtual disponibles. Además, XenServer proporciona alertas preconfiguradas que se activan cuando los hosts se someten a determinadas condiciones y estados. Puede ver estas alertas mediante XenCenter o la CLI xe.

Ver alertas con XenCenter

Puede ver diferentes tipos de alertas en XenCenter si hace clic en **Notificaciones** y, a continuación, en **Alertas**. La vista Alertas muestra varios tipos de alertas, incluidas alertas de rendimiento, alertas del sistema y alertas de actualización de software.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Alertas de rendimiento

Las alertas de rendimiento se pueden generar cuando uno de los siguientes valores supera un umbral especificado en un host administrado, VM o repositorio de almacenamiento (SR): uso de CPU, uso de red, uso de memoria, uso de memoria de dominio de control, rendimiento de almacenamiento o uso de disco de VM.

De forma predeterminada, el intervalo de repetición de alertas se establece en 60 minutos, se puede modificar si es necesario. Las alertas se muestran en la página Alertas en el área Notificaciones de XenCenter. También puede configurar XenCenter para que envíe un correo electrónico para las alertas de rendimiento especificadas junto con otras alertas graves del sistema.

Las alertas personalizadas que se configuran mediante la CLI xe también se muestran en la página Alertas de XenCenter.

Cada alerta tiene un nivel de prioridad/gravedad correspondiente. Puede modificar estos niveles y, si lo quiere, elegir recibir un correo electrónico cuando se active la alerta. La prioridad/gravedad de la alerta predeterminada se establece en 3.

Prioridad	Nombre	Descripción	Alerta de correo electrónico predeterminada
1	Grave	Actúe ahora o los datos podrían perderse o corromperse permanentemente.	Sí
2	Mayor	Actúe ahora o algunos servicios pueden fallar.	Sí
3	Advertencia	Actúe ahora o un servicio puede verse afectado.	Sí
4	Menor	Observe que algo acaba de mejorar.	No
5	Información	Información diaria (inicio, parada, reanudación de VM, etc.)	No
?	Unknown	Error desconocido	No

Configurar alertas de rendimiento

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. En el panel **Recursos**, seleccione el host, la VM o el SR relevantes y, a continuación, haga clic en la ficha **General** y, a continuación, en **Propiedades**.
2. Seleccione la ficha **Alertas**. En la siguiente tabla se resumen las alertas que están disponibles para los hosts, las máquinas virtuales o los SR:

Nombre de alerta	Host	VM	SR	Descripción
Generar alertas de uso de la CPU	X	X		Defina el uso de la CPU y el umbral de tiempo que activan la alerta.
Generar alertas de uso de CPU en el dominio de control	X			Establezca el uso de CPU del dominio de control y el umbral de tiempo que desencadenan la alerta.
Generar alertas de uso de memoria	X			Establezca el uso de memoria y el umbral de tiempo que activan la alerta.
Genere alertas de uso de memoria en el dominio de control	X			Establezca el uso de la memoria del dominio de control y el umbral de tiempo que desencadenan la alerta.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre de alerta	Host	VM	SR	Descripción
Generar alertas de memoria disponible en el dominio de control	X			Establezca la memoria disponible del dominio de control y el umbral de tiempo que desencadenan la alerta.
Generar alertas de uso del disco		X		Establecer el uso del disco y el umbral de tiempo desencadenan la alerta.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre de alerta	Host	VM	SR	Descripción
Generar alertas de rendimiento del almacenamiento			X	Establezca el rendimiento del almacenamiento y el umbral de tiempo que desencadenan la alerta. Nota: Los dispositivos de bloqueo físico (PBD) representan la interfaz entre un host XenServer específico y un SR conectado. Cuando la actividad total de rendimiento SR de lectura/escritura en un PBD supera el umbral especificado, se generan alertas en el host conectado al PBD. A diferencia de otras alertas de host de XenServer, esta alerta debe configurarse en el SR.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Generar alertas de uso de la red	X	X	Establezca el uso de la red y el umbral de tiempo que activan la alerta.

Para cambiar el intervalo de repetición de alertas, introduzca el número de minutos en el cuadro **Intervalo de repetición de alertas**. Cuando se alcanza un umbral de alerta y se genera una alerta, no se genera otra alerta hasta después de que haya transcurrido el intervalo de repetición de alertas.

3. Haga clic en **OK** para guardar los cambios.

Para obtener detalles completos sobre cómo ver, filtrar y configurar la gravedad de las alertas de rendimiento, consulte Configuración de alertas de rendimiento en la documentación de XenCenter.

Alertas del sistema

En la siguiente tabla se muestran los eventos y condiciones del sistema que desencadenan una alerta para que se muestre en la página Alertas de XenCenter.

Nombre	Prioridad/gravedad	Descripción
license_expires_pronto	2	El contrato de licencia de XenServer vence pronto.
ha-statefile_lost	2	Se perdió el contacto con el repositorio de almacenamiento de alta disponibilidad, actúe pronto.
ha-heartbeat_approaching_timeout	5	La alta disponibilidad se acerca al tiempo de espera, el host puede reiniciarse a menos que se tomen medidas.
ha_statefile_approaching_timeout	5	La alta disponibilidad se acerca al tiempo de espera, el host puede reiniciarse a menos que se tomen medidas.
haxapi_healthcheck_approaching_timeout	5	La alta disponibilidad se acerca al tiempo de espera, el host puede reiniciarse a menos que se tomen medidas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre	Prioridad/gravedad	Descripción
ha_network_bonding_error	3	Pérdida potencial del servicio. Pérdida de red que envía latidos de alta disponibilidad.
ha_pool_overcommited	3	Pérdida potencial del servicio. La alta disponibilidad no puede garantizar la protección de las VM configuradas.
ha_poor_drop_en_plan_exists_for	3	La cobertura de alta disponibilidad ha disminuido, es más probable que falle y aún no hay pérdidas.
ha_protected_vm_restart_failed	2	Pérdida de servicio. La alta disponibilidad no pudo reiniciar una VM protegida.
ha_host_falló	3	La alta disponibilidad detectó un error en un host.
ha_host_was_cercado	4	La alta disponibilidad reinició un host para protegerlo contra la corrupción de la VM.
redo_log_healthy	4	El redo log de XAPI se ha recuperado de un error anterior.
redo_log_broken	3	El redo log de XAPI ha detectado un error.
ip_configured_pif_can_unplug	3	XAPI puede desconectar una NIC con configuración IP cuando se usa alta disponibilidad, lo que posiblemente provoque un error de alta disponibilidad.
error de host_sync_data_error	3	No se pudieron sincronizar las estadísticas de rendimiento de XenServer.
host_clock_skew_detected	3	El reloj del host no se sincroniza con otros hosts del grupo.
host_clock_went_backwards	1	El reloj del host está dañado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre	Prioridad/gravedad	Descripción
pool_master_transition	4	Se ha especificado un nuevo host como coordinador del grupo.
pbd_plug_failed_on_server_start	3	El host no se pudo conectar al almacenamiento en el momento del arranque.
auth_external_init_failed	2	El host no pudo habilitar la autenticación de AD externa.
auth_external_pool_non-homogeneous	2	Los hosts de un grupo tienen una configuración de autenticación de AD diferente.
multipath_period_alert	3	Se ha producido un error o se ha recuperado una ruta a un SR.
bond-status-changed	3	Un enlace de un enlace se ha desconectado o vuelto a conectar.

Alertas de actualización de software

- **XenCenter antiguo: XenServer** espera una versión más reciente, pero aún se puede conectar a la versión actual
- **XenCenter desactualizado: XenCenter** es demasiado antiguo para conectarse a XenServer
- **XenServer desactualizado: XenServer** es una versión antigua a la que el XenCenter actual no se puede conectar
- **Alerta de licencia caducada:** la licencia de XenServer ha caducado
- **Falta la alerta de IQN:** XenServer usa almacenamiento iSCSI pero el IQN del host está vacío
- **Alerta de IQN duplicados:** XenServer usa almacenamiento iSCSI y hay IQN de host duplicados

Configurar alertas de rendimiento mediante la CLI xe

> **Nota:**
>
> Los desencadenantes de las alertas se comprueban en un intervalo mínimo de cinco minutos. Este intervalo evita colocar una carga excesiva en el sistema para verificar estas condiciones e informar de falsos positivos. Si se establece un intervalo de repetición de alertas inferior a cinco minutos, las alertas se seguirán generando en el intervalo mínimo de cinco minutos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La perfmon herramienta de supervisión del rendimiento se ejecuta una vez cada cinco minutos y solicita actualizaciones de XenServer, cuya media es superior a un minuto. Estos valores predeterminados se pueden cambiar en /etc/sysconfig/perfmon.

La herramienta perfmon lee actualizaciones cada cinco minutos de variables de rendimiento que se ejecutan en el mismo host. Estas variables se separan en un grupo relacionado con el propio host y un grupo para cada VM que se ejecuta en ese host. Para cada máquina virtual y host, perfmon lee el parámetro other-config:perfmon y utiliza esta cadena para determinar qué variables supervisar y en qué circunstancias generar un mensaje.

Por ejemplo, a continuación se muestra un ejemplo de configuración de una alerta de "uso de CPU" de VM mediante la escritura de una cadena XML en el parámetro other-config:perfmon:

```
xe vm-param-set uuid=vm_uuid other-config:perfmon=\

'<config>
    <variable>
        <name value="cpu_usage"/>
        <alarm_trigger_level value="0.5"/>
    </variable>
</config>'
<!--NeedCopy-->
```

> **Nota:**
>
> Puede usar varios nodos variables.

Después de establecer la nueva configuración, use el siguiente comando para actualizar perfmon para cada host:

```
xe host-call-plugin host=host_uuid plugin=perfmon fn=refresh
<!--NeedCopy-->
```

Si no se realiza esta actualización, se produce una demora antes de que la nueva configuración surta efecto, ya que, de forma predeterminada, perfmon comprueba si hay nuevas configuraciones cada 30 minutos. Este valor predeterminado se puede cambiar en /etc/sysconfig/perfmon.

Elementos de VM válidos

- name: el nombre de la variable (sin valor predeterminado). Si el valor del nombre es cpu_usage, network_usage o disk_usage, los parámetros rrd_regex y alarm_trigger_sense no son obligatorios, ya que se utilizan los valores predeterminados para estos valores.
- alarm_priority: La prioridad de las alertas generadas (por defecto 3).
- alarm_trigger_level: El nivel de valor que desencadena una alerta (sin valor predeterminado).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- `alarm_trigger_sense`: El valor es `high` si `alarm_trigger_level` es un valor máximo; de lo contrario, es `low` si `alarm_trigger_level` es un valor mínimo (el valor predeterminado es `high`).
- `alarm_trigger_period`: El número de segundos que se pueden recibir valores (por encima o por debajo del umbral de alerta) antes de enviar una alerta (el valor predeterminado es`60`).
- `alarm_auto_inhibit_period`: el número de segundos en que se inhabilitará esta alerta después de que se envíe una alerta (el valor predeterminado es `3600`).
- `consolidation_fn`: Combina variables de rrd_updates en un valor. Para `cpu-usage` el valor predeterminado es `average`, para `fs_usage` el valor predeterminado es `get_percent_fs_usage` y para todos los demás es `sum`.
- `rrd_regex`: hace coincidir los nombres de las variables de `xe vm-data-sources-list uuid=vm_uuid`, para calcular los valores de rendimiento. Este parámetro tiene valores predeterminados para las variables nombradas:
  - cpu_usage
  - memory_internal_free
  - network_usage
  - disk_usage

Si se especifica, los valores de todos los elementos devueltos por `xe vm-data-source-list` cuyos nombres coinciden con la expresión regular especificada se consolidan mediante el método especificado como `consolidation_fn`.

Elementos host válidos

- `name`: el nombre de la variable (sin valor predeterminado).
- `alarm_priority`: La prioridad de las alertas generadas (por defecto 3).
- `alarm_trigger_level`: El nivel de valor que desencadena una alerta (sin valor predeterminado).
- `alarm_trigger_sense`: El valor es `high` cuando `alarm_trigger_level` es un valor máximo; de lo contrario, es `low` si `alarm_trigger_level` es un valor mínimo (el valor predeterminado es `high`).
- `alarm_trigger_period`: el número de segundos que se pueden recibir valores (por encima o por debajo del umbral de alerta) antes de que se envíe una alerta (predeterminado `60`).
- `alarm_auto_inhibit_period`: El número de segundos durante los que se inhabilita la alerta después de enviar una alerta. (valor predeterminado`3600`).
- `consolidation_fn`: Combina variables de `rrd_updates` en un solo valor (de forma predeterminada `sum` - o `average`).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- `rrd_regex`: Expresión regular para hacer coincidir los nombres de las variables devueltas por el comando `xe vm-data-source-list uuid=vm_uuid` y utilizarla para calcular el valor estadístico. Este parámetro tiene valores predeterminados para las siguientes variables con nombre:
  - cpu_usage
  - network_usage
  - memory_free_kib
  - sr_io_throughput_total_xxxxxxxx (donde `xxxxxxxx` son los primeros ocho caracteres del SR-UUID).

Rendimiento de SR: las alertas de rendimiento del almacenamiento se deben configurar en el SR en lugar de en el host. Por ejemplo:

```
xe sr-param-set uuid=sr_uuid other-config:perfmon=\
'<config>
    <variable>
        <name value="sr_io_throughput_total_per_host"/>
        <alarm_trigger_level value="0.01"/>
    </variable>
</config>'
<!--NeedCopy-->
```

Configuración de ejemplo genérica El siguiente ejemplo muestra una configuración genérica:

```
<config>
    <variable>
    <name value="NAME_CHOSEN_BY_USER"/>
    <alarm_trigger_level value="THRESHOLD_LEVEL_FOR_ALERT"/>
    <alarm_trigger_period value="
       RAISE_ALERT_AFTER_THIS_MANY_SECONDS_OF_BAD_VALUES"/>
    <alarm_priority value="PRIORITY_LEVEL"/>
    <alarm_trigger_sense value="HIGH_OR_LOW"/>
    <alarm_auto_inhibit_period value="
       MINIMUM_TIME_BETWEEN_ALERT_FROM_THIS_MONITOR"/>
    <consolidation_fn value="FUNCTION_FOR_COMBINING_VALUES"/>
    <rrd_regex value="REGULAR_EXPRESSION_TO_CHOOSE_DATASOURCE_METRIC"/>
    </variable>

    <variable>
    ...
    </variable>

    ...
</config>
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurar alertas por correo electrónico

Puede configurar XenServer para que envíe notificaciones por correo electrónico cuando los hosts de XenServer generen alertas. La utilidad mail-alarm de XenServer usa sSMTP para enviar estas notificaciones por correo electrónico. Puede habilitar las alertas de correo electrónico básicas mediante XenCenter o la interfaz de línea de comandos (CLI) xe. Para seguir configurando las alertas por correo electrónico, puede modificar el archivo `mail-alarm.conf` de configuración.

Utilice un servidor SMTP que no requiera autenticación. Los correos electrónicos enviados a través de servidores SMTP que requieren autenticación no se pueden entregar.

Habilitar alertas por correo electrónico mediante XenCenter

1. En el panel `Resources`, haga clic con el botón secundario en una agrupación y seleccione `Properties`.
2. En la ventana `Properties`, seleccione `Email Options`.
3. Seleccione la casilla `Send email alert notifications`. Introduzca su dirección de destino preferida para los correos electrónicos de notificación y los detalles del servidor SMTP.
4. Elige el idioma que prefieras de la lista `Mail language`. El idioma predeterminado para los correos electrónicos de alertas de rendimiento es el inglés.

Habilitar alertas de correo electrónico mediante la CLI xe

Para configurar las alertas por correo electrónico, especifique su dirección de destino preferida para los correos electrónicos de notificación y el servidor SMTP:

```
xe pool-param-set uuid=pool_uuid other-config:mail-destination=joe.
   bloggs@example.com
xe pool-param-set uuid=pool_uuid other-config:ssmtp-mailhub=smtp.
   example.com:<port>
<!--NeedCopy-->
```

XenServer configura automáticamente la dirección del remitente como. `noreply@<hostname>` Sin embargo, puede configurar la dirección del remitente de forma explícita:

```
xe pool-param-set uuid=pool_uuid other-config:mail-sender=
   serveralerts@example.com
<!--NeedCopy-->
```

Al activar las notificaciones por correo electrónico, recibirá una notificación por correo electrónico cuando se genere una alerta con una prioridad de 3 o más. Por lo tanto, el nivel de prioridad mínimo predeterminado es 3. Puede cambiar este valor predeterminado con el siguiente comando:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe pool-param-set uuid=pool_uuid other-config:mail-min-priority=level
<!--NeedCopy-->
```

> **Nota:**
>
> Algunos servidores SMTP solo reenvían correos con direcciones que usan FQDN. Si descubre que los correos electrónicos no se reenvían, puede que sea por este motivo. En ese caso, puede establecer el nombre de host del servidor en el FQDN para que esta dirección se use cuando se conecte a su servidor de correo.

Para configurar el idioma de los correos electrónicos de alertas de rendimiento:

```
xe pool-param-set uuid=pool_uuid other-config:mail-language=ja-JP
<!--NeedCopy-->
```

El idioma predeterminado para los correos electrónicos de alertas de rendimiento es el inglés.

Configuración adicional

Para seguir configurando la utilidad mail-alarm en XenServer, cree un `/etc/mail-alarm.conf` archivo que contenga lo siguiente:

```
root=postmaster
authUser=<username>
authPass=<password>
mailhub=@MAILHUB@
<!--NeedCopy-->
```

`/etc/mail-alarm.conf` es una plantilla proporcionada por el usuario para el archivo de configuración de sSMTP `ssmtp.conf` y se utiliza para todas las alertas generadas por los hosts de XenServer. Se compone de claves donde `key=@KEY@` y `@KEY@` se sustituye por el valor correspondiente de `ssmtp-key` en `pool.other_config`. A continuación, estos valores se pasan a ssmtp, lo que le permite controlar aspectos de la configuración de sSMTP mediante valores de `pool.other_config`. Observa cómo `@KEY@` (mayúsculas) se corresponde con `ssmtp-key` (minúsculas, con el prefijo `ssmtp-`).

Por ejemplo, si configura el servidor SMTP:

```
xe pool-param-set uuid=pool_uuid other-config:ssmtp-mailhub=smtp.
   example.com
<!--NeedCopy-->
```

y, a continuación, agregue lo siguiente a su archivo `/etc/mail-alarm.conf`:

```
mailhub=@MAILHUB@
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

`mailhub=@MAILHUB@` se convierte en `mailhub=smtp.example.com`.

Cada servidor SMTP puede diferir ligeramente en su configuración y puede requerir una configuración adicional. Para seguir configurando sSMTP, modifique su archivo de configuración `ssmtp.conf`. Al almacenar las claves relevantes en el archivo `mail-alarm.conf`, puede utilizar los valores de `pool.other_config` para configurar sSMTP. El siguiente extracto de la página principal de `ssmtp.conf` muestra la sintaxis correcta y las opciones disponibles:

```
NAME
    ssmtp.conf - ssmtp configuration file

DESCRIPTION
    ssmtp reads configuration data from /etc/ssmtp/ssmtp.conf The file con-
    tains keyword-argument pairs, one per line. Lines starting with '#'
    and empty lines are interpreted as comments.

The possible keywords and their meanings are as follows (both are case-
insensitive):

    Root
    The user that gets all mail for userids less than 1000. If blank,
    address rewriting is disabled.

    Mailhub
        The host to send mail to, in the form host | IP_addr port :
        <port>. The default port is 25.

    RewriteDomain
    The domain from which mail seems to come. For user authentication.

    Hostname
        The full qualified name of the host. If not specified, the host
        is queried for its hostname.

    FromLineOverride
        Specifies whether the From header of an email, if any, may over-
        ride the default domain. The default is "no".

    UseTLS
    Specifies whether ssmtp uses TLS to talk to the SMTP server.
    The default is "no".

    UseSTARTTLS
        Specifies whether ssmtp does a EHLO/STARTTLS before starting TLS
        negotiation. See RFC 2487.

    TLSCert
        The file name of an RSA certificate to use for TLS, if required.
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
41
42      AuthUser
43          The user name to use for SMTP AUTH. The default is blank, in
44          which case SMTP AUTH is not used.
45
46      AuthPass
47          The password to use for SMTP AUTH.
48
49      AuthMethod
50          The authorization method to use. If unset, plain text is used.
51          May also be set to "cram-md5".
52  <!--NeedCopy-->
```

Campos y etiquetas personalizados

XenCenter admite la creación de etiquetas y campos personalizados, lo que permite la organización y la búsqueda rápida de máquinas virtuales, almacenamiento, etc. Para obtener más información, consulte Supervisión del rendimiento del sistema.

Búsquedas personalizadas

XenCenter admite la creación de búsquedas personalizadas. Las búsquedas se pueden exportar e importar, y los resultados de una búsqueda se pueden mostrar en el panel de navegación. Para obtener más información, consulte Supervisión del rendimiento del sistema.

Determinar el rendimiento de adaptadores de bus físicos

Para los HBA FC, SAS e iSCSI, puede determinar el rendimiento de red de sus PBD mediante el siguiente procedimiento.

1. Enumera los PBD en un host.
2. Determine qué LUNs se redirigen a través de qué PBD.
3. Para cada PBD y SR, enumere los VBD que hacen referencia a los VDI en el SR.
4. Para todos los VBD activos que están conectados a las máquinas virtuales en el host, calcule el rendimiento combinado.

Para el almacenamiento iSCSI y NFS, consulte las estadísticas de su red para determinar si hay un cuello de botella de rendimiento en el arreglo de discos o si el PBD está saturado.

Supervisar los recursos del host y del dom0 con NRPE

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> La función NRPE está disponible para los clientes de XenServer Premium o Trial Edition. Para obtener más información sobre las licencias de XenServer, consulte Licencias. Para actualizar o comprar una licencia de XenServer, visite el sitio web de XenServer.

Los usuarios con la función de administrador de grupos pueden usar cualquier herramienta de supervisión de terceros que sea compatible con Nagios Remote Plugin Executor (NRPE) para supervisar los recursos que consumen el host de XenServer y dom0, el dominio de control del host.

Puede usar los siguientes complementos de verificación para monitorear los recursos del host y dom0:

Métrica	Nombre del cheque NRPE	Descripción	Umbral de advertencia predeterminado	Umbral crítico predeterminado	Datos de rendimiento devueltos
Carga de la CPU del host	check_host_load	Obtiene y comprueba la carga actual por CPU física del host, donde la carga hace referencia a la cantidad de vCPU en estado de ejecución o ejecutables.	3	4	Carga actual del sistema de la CPU del host (calculada tomando la carga promedio de la CPU física del host).
Uso de la CPU del host (%)	check_host_cpu	Obtiene y comprueba el promedio actual de uso general de CPU del host.	80%	90%	El porcentaje de CPU host que está libre actualmente y el porcentaje que está en uso.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Métrica	Nombre del cheque NRPE	Descripción	Umbral de advertencia predeterminado	Umbral crítico predeterminado	Datos de rendimiento devueltos
Uso de memoria del host (%)	check_host_memory	Obtiene y comprueba el uso actual de memoria del host.	80%	90%	El porcentaje de memoria del host que está libre actualmente y el porcentaje que está en uso.
Uso de vGPU en el host (%)	check_vgpu	Obtiene y comprueba todo el uso actual de vGPU de Nvidia en ejecución por parte del host.	80%	90%	El porcentaje de vGPU en ejecución que actualmente es gratuito y el porcentaje que está en uso.
Uso de memoria de vGPU del host (%)	check_vgpu_memory	Obtiene y comprueba todo el uso actual de memoria vGPU de Nvidia en ejecución (incluidas la memoria compartida y la memoria gráfica) del host.	80%	90%	El porcentaje de memoria de vGPU en ejecución (incluidas la memoria compartida y la memoria gráfica) que está libre actualmente y el porcentaje que está en uso.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Métrica	Nombre del cheque NRPE	Descripción	Umbral de advertencia predeterminado	Umbral crítico predeterminado	Datos de rendimiento devueltos
Carga de CPU Dom0	check_load	Obtiene y comprueba el promedio de carga actual del sistema por CPU de dom0, donde la carga hace referencia a la cantidad de procesos en ejecución o en estado ejecutable.	2.7,2.6,2.5	3.2,3.1,3	Los datos de carga de la CPU del host se calculan tomando el promedio de los últimos 1, 5 y 15 minutos.
Uso de CPU Dom0 (%)	check_cpu	Obtiene y comprueba el promedio actual de uso general de CPU de dom0.	80%	90%	El uso promedio general de CPU de dom0 como porcentaje.
Uso de memoria Dom0 (%)	comprobar_memoria	Obtiene y comprueba el uso actual de memoria de dom0.	80%	90%	El porcentaje de memoria dom0 que está libre actualmente y el porcentaje que está en uso.
Intercambio gratuito de Dom0 (%)	check_swap	Obtiene y comprueba el uso de intercambio actual de dom0.	20%	10%	El porcentaje de MB en dom0 que actualmente es gratuito.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Métrica	Nombre del cheque NRPE	Descripción	Umbral de advertencia predeterminado	Umbral crítico predeterminado	Datos de rendimiento devueltos
Espacio libre de la partición raíz Dom0 (%)	check_disk_root	Obtiene y comprueba el uso actual de la partición raíz de dom0.	20%	10%	El porcentaje de MB de la partición raíz dom0 que está libre actualmente.
Espacio libre de la partición de registro Dom0 (%)	check_disk_log	Obtiene y comprueba el uso actual de la partición de registro de dom0.	20%	10%	El porcentaje de MB de la partición de registro dom0 que está libre actualmente.
Estado de la pila de herramientas	check_xapi	Obtiene y comprueba el estado de la pila de herramientas de administración de XenServer (también denominada XAPI).			El tiempo de actividad de XAPI transcurrió en segundos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Métrica	Nombre del cheque NRPE	Descripción	Umbral de advertencia predeterminado	Umbral crítico predeterminado	Datos de rendimiento devueltos
Estado de rutas múltiples	check_multipath	Obtiene y comprueba el estado de las rutas de almacenamiento.			El estado de las rutas de almacenamiento. `OK` indica que todas las rutas están activas, `WARNING` indica que algunas rutas han fallado pero más de una está activa, `CRITICAL` indica que solo hay una ruta activa o que todas las rutas han fallado, `UNKNOWN` indica que las rutas múltiples del host están deshabilitadas y que no se puede obtener el estado de las rutas.

NRPE es un servicio local que se ejecuta en dom0 y escucha en el puerto TCP (predeterminado) 5666 las solicitudes de ejecución de comprobaciones de una herramienta de supervisión. Cuando llega

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

una solicitud, NRPE la analiza, busca el comando de comprobación correspondiente, incluidos los detalles del parámetro, en el archivo de configuración y, a continuación, lo ejecuta. El resultado de la comprobación se envía a la herramienta de supervisión, que almacena los resultados de las comprobaciones anteriores y proporciona un gráfico que muestra los datos históricos de rendimiento.

Requisitos previos

Para poder utilizar NRPE para supervisar los recursos del host y del dom0, la herramienta de supervisión que utilice debe cumplir los siguientes requisitos previos:

- La herramienta de monitoreo debe ser compatible con la versión 4.1.0 del NRPE.
- Para permitir la comunicación entre el NRPE y la herramienta de monitoreo, la herramienta de monitoreo debe admitir TLS 1.2 con cifrados `ECDHE-RSA-AES256-GCM-SHA384` y `ECDHE-RSA-AES128-GCM-SHA256`, y la curva EC es. `secp384r1`

Limitaciones

- Puede configurar los ajustes de NRPE para todo un grupo o para un host independiente que no forme parte de un grupo. Actualmente, no puede configurar los ajustes de NRPE para un host individual de un grupo.
- Si agrega un host a un grupo que ya tiene el NRPE habilitado y configurado en él, XenCenter no aplica automáticamente la configuración de NRPE del grupo al nuevo host. Debe volver a configurar los ajustes de NRPE en el grupo después de agregar el nuevo host o configurar el nuevo host con los mismos ajustes de NRPE antes de agregarlo al grupo.

  > **Nota:**
  >
  > Al reconfigurar los ajustes de NRPE en un grupo después de agregar un nuevo host, asegúrese de que el host esté en funcionamiento.

- Si se quita un host de un grupo con el NRPE habilitado y configurado en él, XenCenter no modifica la configuración de NPRE del host o del grupo.

Configurar NRPE mediante la CLI xe

Puede configurar NRPE mediante la CLI xe o XenCenter. Para obtener más información sobre cómo configurar NRPE mediante XenCenter, consulte Supervisar los recursos de host ydom0 con NRPE.

Tras realizar cambios de configuración en NRPE, reinicie el servicio NRPE mediante:

```
1 xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=restart
2 <!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Habilitar NRPE El NRPE está deshabilitado de forma predeterminada en XenServer. Para habilitar NRPE en el dominio de control de un host (dom0), ejecute los siguientes comandos en la CLI xe:

1. Obtenga el UUID de host del host que desea supervisar:

   ```
   xe host-list
   ```

2. Habilite NRPE en el host:

   ```
   xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=enable
   ```

   Si la operación se ejecuta correctamente, se genera este comando `Success`. Cuando XenServer se reinicia, NRPE se inicia automáticamente.

Para detener, iniciar, reiniciar o deshabilitar NRPE:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=<operation>
<!--NeedCopy-->
```

donde **la operación** es `stopstart`, `restart`, o `disable`.

Monitorización de servidores Se trata de una lista delimitada por comas de direcciones IP o nombres de host que pueden comunicarse con el daemon NRPE. También se admiten direcciones de red con máscara de bits (por ejemplo `192.168.1.0/24`).

Vea la lista actual de servidores de monitoreo:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=get-config
   args:allowed_hosts
<!--NeedCopy-->
```

Permita que la herramienta de monitoreo ejecute comprobaciones:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=set-config
   args:allowed_hosts=<IP address or hostname>
<!--NeedCopy-->
```

Consulte todos los ajustes de NRPE:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=get-config
<!--NeedCopy-->
```

Configure varios ajustes de NRPE:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=set-config
   args:allowed_hosts=<IP address or hostname> args:ssl_logging=<SSL
   log level> args:debug=<debug log level>
<!--NeedCopy-->
```

Registros

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Registro de depuración De forma predeterminada, el registro de depuración está deshabilitado.

Para comprobar si el registro de depuración está habilitado, ejecute el siguiente comando:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=get-config
   args:debug
<!--NeedCopy-->
```

Si `debug: 0` se devuelve, el registro de depuración está deshabilitado.

Para habilitar el registro de depuración:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=set-config
   args:debug=1
<!--NeedCopy-->
```

Registro SSL De forma predeterminada, el registro SSL está deshabilitado:

```
ssl_logging=0x00
<!--NeedCopy-->
```

Para comprobar si el registro SSL está habilitado, ejecute el siguiente comando:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=get-config
   args:ssl_logging
<!--NeedCopy-->
```

Para habilitar el registro SSL:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=set-config
   args:ssl_logging=0x2f
<!--NeedCopy-->
```

Umbrales críticos y de advertencia Para algunos de estos complementos de comprobación, puede establecer valores de umbral críticos y de advertencia de modo que, si el valor devuelto por un complemento de comprobación supera los valores de umbral, se genere una alerta. El umbral de advertencia indica un problema potencial y el umbral crítico indica un problema más grave que requiere atención inmediata. Aunque los valores predeterminados están establecidos para los umbrales críticos y de advertencia, puede ajustar los valores de los umbrales.

Para consultar los valores predeterminados de advertencia y umbral crítico para todas las comprobaciones, ejecute el siguiente comando xe de la CLI, que devuelve una lista de todas las comprobaciones y sus umbrales críticos y de advertencia asociados:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=get-threshold
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

También puede consultar los valores de umbral para una comprobación específica. Por ejemplo, para obtener los valores de advertencia y de umbral crítico del complemento `check_memory` check, ejecute el siguiente comando xe de la CLI:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=get-threshold
   args:check_memory
<!--NeedCopy-->
```

También puede cambiar el valor predeterminado de un umbral. Por ejemplo, para cambiar los valores de umbral predeterminados del complemento `check_memory` check, ejecute el siguiente comando xe de la CLI:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=set-threshold
   args:check_memory args:w=75 args:c=85
<!--NeedCopy-->
```

Supervisar los recursos de host y dom0 con SNMP

> **Nota:**
>
> La función SNMP está disponible para los clientes de XenServer Premium o Trial Edition. Para obtener más información sobre las licencias de XenServer, consulte Licencias. Para actualizar o comprar una licencia de XenServer, visite el sitio web de XenServer.

Con la función de administrador del grupo, puede usar SNMP para supervisar de forma remota los recursos consumidos por el host de XenServer y dom0, el dominio de control del host. Un administrador SNMP, también conocido como sistema de administración de redes (NMS), envía solicitudes de consulta a un agente SNMP que se ejecuta en un host de XenServer. El agente SNMP responde a estas solicitudes de consulta enviando los datos recopilados en varias métricas al NMS. Los datos que se pueden recopilar se definen mediante identificadores de objetos (OID) en un archivo de texto denominado base de datos de información de administración (MIB). Un OID representa una información medible específica sobre un dispositivo de red, como el uso de la CPU o la memoria.

También puede configurar capturas, que son mensajes iniciados por el agente que alertan al NMS de que se ha producido un evento específico en XenServer. Tanto las solicitudes de consulta como las capturas se pueden usar para supervisar el estado de los grupos de XenServer. Se definen como objetos de métrica y de captura y se identifican mediante los OID en un archivo MIB `XENSERVER-MIB.txt`, que se puede descargar desde la página de descargas de XenServer. En las tablas siguientes se proporciona información sobre estos objetos de métrica y de captura.

Objetos de métrica

Puede solicitar información específica sobre los hosts de XenServer mediante las métricas que se muestran en la tabla siguiente. El administrador de SNMP utiliza estas métricas al enviar solicitudes

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de consulta a un agente de SNMP y, por lo tanto, puede ver estos datos en su NMS.

Puede ver los datos devueltos por estos objetos de métrica desde su NMS o desde la CLI xe. Para consultar los objetos de métrica desde la CLI xe, ejecute `host-data-source-query` o `vm-data-source-query` proporcione la fuente de datos RRDD como valor para el parámetro `data-source`. Por ejemplo:

```
xe host-data-source-query data-source=cpu_avg host=<host UUID>
<!--NeedCopy-->
```

> **Nota:**
>
> De forma predeterminada, el NMS envía solicitudes de consulta de OID a los agentes SNMP a través del puerto 161.

Identificador de objeto (OID)	Fuente de datos RRDD	Datos devueltos	Tipo
.1.3.6.1.4.1.60953.1.1.1.1	`memory`	Memoria total de Dom0 en MB	Unsigned32
.1.3.6.1.4.1.60953.1.1.1.2	`memory_internal_free`	Memoria libre de Dom0 en MB	Unsigned32
.1.3.6.1.4.1.60953.1.1.1.3	`cpu_usage`	Uso de CPU de Dom0 como porcentaje	Flotante
.1.3.6.1.4.1.60953.1.1.1.4	`memory_total_kib`	Memoria total del host en MB	Unsigned32
.1.3.6.1.4.1.60953.1.1.1.5	`memory_free_kib`	Memoria libre del host en MB	Unsigned32
.1.3.6.1.4.1.60953.1.1.1.6	`cpu_avg`	Uso de la CPU del host como porcentaje	Flotante
.1.3.6.1.4.1.60953.1.1.1.7	(véase la nota 1)	Número de pCPU	Unsigned32
.1.3.6.1.4.1.60953.1.1.1.8	`running_vcpus`	Número de vCPU en ejecución	Unsigned32
.1.3.6.1.4.1.60953.1.1.1.9	`running_domains`	Número de máquinas virtuales en ejecución	Unsigned32

> **Notas:**
>
> 1. El nombre de una pCPU tiene el formato `cpu` seguido de un número. Para consultar la cantidad de pCPU desde la CLI xe, ejecute el siguiente comando:
>
>    ```
>    xe host-data-source-list host=<host UUID> | grep -E 'cpu[0-9]+
>    ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
$'
```

This returns a list of the CPU metrics that match the regular expression `cpu[0-9]+`.

Capturas

Las capturas son alertas que envía el agente SNMP para notificar al administrador de SNMP cuando se producen ciertos eventos, lo que le permite supervisar los hosts de XenServer e identificar los problemas con antelación. Puede configurar los ajustes de SNMP para generar una captura cuando se alcance un límite (por ejemplo, si el uso de la CPU del host es demasiado alto). Cuando se genera una captura, se envía a su NMS y se devuelven los siguientes campos como parte del objeto de captura.

> **Nota:**
>
> De forma predeterminada, el agente SNMP del host del coordinador del grupo envía capturas al NMS a través del puerto UPD 162.

Identificador de objeto (OID)	Nombre del campo	Tipo	Descripción
.1.3.6.1.4.1.60953.1.10.1.1	`operation`	Cadena	Puede ser uno de los valores siguientes: `add` o `del`. `operation` es `add` si XenServer genera una captura y la envía a su NMS (también se crea una alerta en XenCenter) o `del` si se destruye una alerta (por ejemplo, si se descarta una alerta).
.1.3.6.1.4.1.60953.1.10.1.2	`ref`	Cadena	La referencia del objeto de captura.
.1.3.6.1.4.1.60953.1.10.1.3	`uuid`	Cadena	El UUID del objeto de captura.
.1.3.6.1.4.1.60953.1.10.1.4	`name`	Cadena	El nombre del objeto de captura.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Identificador de objeto (OID)	Nombre del campo	Tipo	Descripción
.1.3.6.1.4.1.60953.1.10.1.5	`priority`	Número entero	La gravedad de la captura. Puede ser uno de los valores siguientes 1: Crítica, 2: Grave, 3: Advertencia, 4: Leve, 5: Información, `others`: Desconocida.
.1.3.6.1.4.1.60953.1.10.1.6	**`class`**	Cadena	La categoría de la captura generada. Puede ser uno de los valores siguientes: `VMHost`, `SR`, `Pool`, `VMPP`, `VMSS`, `PVS_proxy`, `VDI` o `Certificate`.
.1.3.6.1.4.1.60953.1.10.1.7	`obj-uuid`	Cadena	El UUID del objeto xapi de las distintas clases del campo **`class`**.
.1.3.6.1.4.1.60953.1.10.1.8	`timestamp`	Cadena	Hora en la que se genera la captura.
.1.3.6.1.4.1.60953.1.10.1.9	`body`	Cadena	Información detallada sobre el campo `name`.

Requisitos previos

- Todos los hosts de un grupo deben ejecutar la misma versión de XenServer y esta versión debe contener el plug-in de SNMP.

  > **Nota:**
  >
  > Si no puede ver la ficha **SNMP** en XenCenter, es posible que el host o un miembro del grupo no ejecute una versión de XenServer que admita SNMP. Actualice el host o el grupo a la versión más reciente de XenServer.

- El NMS que use debe ser compatible con SNMPv2c o SNMPv3.
- Su NMS y XenServer deben estar conectados a la red.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Limitaciones

- Puede configurar los parámetros de SNMP para un grupo completo o para un host independiente que no forme parte de un grupo. Actualmente, no puede configurar los parámetros de SNMP para un host individual de un grupo.
- Si agrega un host a un grupo que ya tiene SNMP habilitado y configurado, XenCenter no aplica automáticamente los parámetros de SNMP del grupo al nuevo host. Debe reconfigurar los parámetros de SNMP en el grupo después de agregar el nuevo host o configurar el nuevo host con los mismos parámetros de SNMP antes de agregarlo al grupo.

  > **Nota:**
  >
  > Al reconfigurar los parámetros de SNMP en un grupo después de agregar un nuevo host, asegúrese de que el host esté en funcionamiento y no en modo de mantenimiento.

- Antes de realizar una actualización sucesiva de grupos de Citrix Hypervisor 8.2 CU1 a XenServer 8 o de aplicar actualizaciones a los hosts y grupos de XenServer, haga una copia de seguridad de los siguientes archivos de configuración si los ha modificado manualmente antes y los necesita:
  - `/etc/snmp/snmpd.xs.conf`
  - `/etc/sysconfig/snmp`
  - `/var/lib/net-snmp/snmpd.conf`
- Cuando el agente SNMP está desconectado, no se pueden generar capturas. Por ejemplo, si se reinicia el agente SNMP o si el coordinador del grupo se reinicia o se vuelve a designar.

Configurar SNMP mediante la CLI xe

Puede configurar SNMP mediante la CLI xe o XenCenter. Para obtener más información sobre cómo configurar SNMP mediante XenCenter, consulte Supervisión de los recursos de host y dom0 con SNMP.

Objetos `result` Al configurar SNMP, todas las respuestas se devuelven en formato JSON. Si un comando se ejecuta correctamente, devuelve el par clave-valor `"code": 0`. Algunos comandos (como el comando `get-config`) devuelven un objeto JSON anidado llamado `result`. El objeto JSON `result` también es necesario para el comando `set-config` que se usa para actualizar la configuración de SNMP.

El objeto JSON `result` se compone de los siguientes objetos `common`, `agent` y `nmss`:

`common`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Campo	Valores permitidos	Valor predeterminado
`enabled`	`no` (inhabilitar el servicio SNMP) o `yes` (habilitar el servicio SNMP)	`no`
`debug_log`	`no` (inhabilitar el registro de depuración) o `yes` (habilitar el registro de depuración)	`no`
`max_nmss`	N/A (este campo es de solo lectura y especifica la cantidad máxima de NMS compatibles)	1

`agent`

Campo	Valores permitidos	Valor predeterminado
`v2c`	`no` (inhabilitar SNMPv2c) o `yes` (habilitar SNMPv2c)	`yes`
`community`	COMMON_STRING_TYPE (ver nota 1)	**`public`**
`v3`	`no` (inhabilitar v3) o `yes` (habilitar v3)	`no`
`user_name`	COMMON_STRING_TYPE (ver nota 1)	
`authentication_password`	COMMON_STRING_TYPE donde la longitud es >= 8 (ver nota 1)	
`authentication_protocol`	`MD5` o `SHA`	
`privacy_password`	COMMON_STRING_TYPE donde la longitud es >= 8 (ver nota 1)	
`privacy_protocol`	`DES` o `AES`	
`engine_id`	N/A (este campo es de solo lectura y se genera cuando el agente SNMP se inicia por primera vez)	

`nmss`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Campo	Valores permitidos	Valor predeterminado
`uuid`	UUID de NMS (se establece al configurar el receptor de capturas de NMS y este valor debe ser uniforme en todos los hosts de un grupo)	
`address`	Dirección IPv4 o nombre de host (FQDN) de NMS	
`port`	1 a 65535	162
`v2c`	`no` (inhabilitar SNMPv2c), `yes` (habilitar SNMPv2c) o admite SNMPv2c o v3.	`yes`
`community`	COMMON_STRING_TYPE (ver nota 1)	**`public`**
`v3`	`no` (inhabilitar la versión 3), `yes` (habilitar la versión 3) o admite SNMPv2c o SNMPv3.	`no`
`user_name`	COMMON_STRING_TYPE (ver nota 1)	
`authentication_password`	COMMON_STRING_TYPE donde la longitud es >= 8 (ver nota 1)	
`authentication_protocol`	`MD5` o `SHA`	
`privacy_password`	COMMON_STRING_TYPE donde la longitud es >= 8 (ver nota 1)	
`privacy_protocol`	`DES` o `AES`	

Notas:

1. COMMON_STRING_TYPE hace referencia a una cadena que cumple los siguientes requisitos:
   - Cualquier combinación de letras, números, guiones (-), punto (.), libra (#), arroba (@), igual a (=), dos puntos (:) o caracteres de subrayado (_).
   - Longitud entre 6 y 32, ambos incluidos.
2. Las contraseñas no se almacenan en texto simple en ningún archivo de configuración de XenServer. Se convierten en una clave localizada y se almacenan. El comando `get`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> `-config` muestra la contraseña como una constante oculta compuesta de asteriscos (*).

Configurar el servicio SNMP Obtenga el estado del servicio SNMP:

```
xe host-call-plugin host-uuid=<host-uuid> plugin=snmp fn=status
<!--NeedCopy-->
```

Inicie, detenga o reinicie el servicio SNMP:

```
xe host-call-plugin host-uuid=<host-uuid> plugin=snmp fn=<operation>
<!--NeedCopy-->
```

donde la **operación**es `start`, `stop` o `restart`.

Obtenga los detalles de configuración de SNMP:

```
xe host-call-plugin host-uuid=<host-uuid> plugin=snmp fn=get-config
<!--NeedCopy-->
```

Si se ejecuta correctamente, este comando devuelve el par clave-valor `"code": 0` y el objeto JSON `result` que contiene los detalles de configuración del servicio SNMP. Por ejemplo:

```
"code": 0,
  "result": {

    "common": {

      "enabled": "no",
      "debug_log": "no",
      "max_nmss": 1
     }
 ,
    "agent": {

      "v2c": "yes",
      "v3": "no",
      "community": "public",
      "user_name": "",
      "authentication_password": "",
      "authentication_protocol": "",
      "privacy_password": "",
      "privacy_protocol": "",
      "engine_id": "<engine_id>"
     }
 ,
    "nmss": []
   }

<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Copie el objeto JSON `result` en su editor de textos preferido y elimine todos los caracteres de nueva línea (**\n**) del archivo. Actualice los campos con los detalles de configuración de SNMP. Para configurar el NMS, consulte la documentación de NMS y especifique los valores de los campos necesarios para el objeto `nmss`. Para obtener más información, consulte los objetos enumerados anteriormente.

Para configurar el servicio SNMP, ejecute el comando `set-config` y proporcione el objeto JSON `result` modificado como un valor de parámetro para el parámetro `args:config`.

Defina la configuración de SNMP:

```
xe host-call-plugin host-uuid=<host-uuid> plugin=snmp fn=set-config
   args:config='<result>'
<!--NeedCopy-->
```

donde el **resultado** es el objeto JSON `result` devuelto por el comando `get-config` que copió y modificó.

> **Nota:**
>
> Para configurar SNMP para todo un grupo, debe ejecutar el comando `set-config` para cada host del grupo.

Si los cambios de configuración se realizan correctamente, el comando devuelve el par clave-valor `"code": 0`. Si los cambios de configuración no se realizan correctamente, el comando `set-config` devuelve uno de los siguientes pares clave-valor que indican que se ha producido un error:

- `"code": 1`: Cadena de error común. Por ejemplo, una excepción desconocida.
- `"code": 2`: Cadena de error (falta un parámetro).
- `"code": 3`: Devuelve un objeto `message` en forma de lista donde cada elemento tiene el formato de `[field_path, key, value, error string]`.

También puede enviar una captura SNMP de prueba a su NMS para verificar que la información del receptor de capturas especificada es correcta.

Enviar una captura SNMP de prueba:

```
xe host-call-plugin host-uuid=<host-uuid> plugin=snmp fn=send-test-trap
    args:config='{
 "nmss":[{
 "uuid":"<uuid>","address":"<address>","port":162,"v2c":"yes","v3":"no
    ","community":"public","user_name":"<user_name>","
    authentication_password":"<authentication_password>","
    authentication_protocol":"<authentication_protocol>","
    privacy_password":"<privacy_password>","privacy_protocol":"<
    privacy_protocol>" }
 ] }
 '
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Este comando envía una captura de prueba a su NMS con los comandos `msg_name` de `TEST_TRAP` y `msg_body` de `This is a test trap from XenServer pool "<pool name>"to verify the NMS Trap Receiver configuration.`

Si no recibe la captura de prueba, vuelva a comprobar la configuración de SNMP. Si no funciona, el comando `send-test-trap` también devuelve uno de los siguientes pares clave-valor que indican que se ha producido un error:

- `"code":` 1: Cadena de error común. Por ejemplo, una excepción desconocida.
- `"code":` 2: Cadena de error (falta un parámetro).
- `"code":` 3: Devuelve un objeto `message` en forma de lista donde cada elemento tiene el formato de `[field_path, key, value, error string]`.
- `"code":` 4: Devuelve un objeto `message` en forma de lista donde cada elemento tiene el formato de `[nms address, nms port, error string]`.

Supervisa el uso de la CPU

November 28, 2023

La cantidad óptima de vCPU por PCPU en un host depende del caso de uso. Durante la operación, asegúrese de supervisar el rendimiento del entorno de XenServer y ajustar la configuración en consecuencia.

Términos y condiciones

En esta área, hay varios términos que a veces se usan indistintamente. En este artículo, utilizamos los siguientes términos y significados:

- **CPU (CPU física):** el hardware físico conectado a un socket de procesador.
- **Núcleo:** Una unidad de procesamiento físico, capaz de realizar un subproceso de ejecución independiente, que contiene todas las unidades funcionales necesarias para soportar esa ejecución.
- **Hyperthread:** Unidad de procesamiento físico, capaz de ejecutar un subproceso independiente, que comparte algunas unidades funcionales con otro hiperhilo (también denominado "subproceso hermano").
- **CPU lógica (pCPU):** Unidad capaz de crear un subproceso de ejecución independiente que incluye un conjunto de registros y un puntero de instrucciones. En un sistema con hyperthreads habilitados, se trata de un hyperthread. En otros casos, es un núcleo.
- **PCPU del host**: el número total de CPU lógicas del host.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **vCPU (CPU virtual)**: CPU lógica virtualizada. Se trata de una unidad lógica capaz de ejecutar un subproceso de ejecución independiente, que se proporciona a las máquinas virtuales. En XenServer, las vCPU pueden "compartir el tiempo"en las PCPU mediante un programador para determinar qué vCPU se está ejecutando en qué PCPU en un momento dado.
- **CPU virtuales invitadas**: las vCPU que se presentan a un sistema operativo invitado dentro de una máquina virtual.
- vCPU**Dom0: las vCPU**que están visibles para el dominio de control de XenServer (dom0).
- **Total de vCPU del host**: suma de vCPU dom0 y todas las vCPU invitadas del host.

Comportamiento general

La cantidad total de vCPU en un host es la cantidad de vCPU utilizadas por dom0 que se suma a la cantidad total de vCPU asignadas a todas las máquinas virtuales del host. A medida que aumenta la cantidad de vCPU en un host, puede experimentar los siguientes tipos de comportamiento:

- Cuando la cantidad total de vCPU en el host es *menor o igual a* la cantidad de CPU en el host, el host siempre proporciona la cantidad de CPU solicitada por las máquinas virtuales.
- Cuando la cantidad total de vCPU en el host es *mayor que* la cantidad de PCPU en el host, el host comparte el tiempo de las PCPU del host con las máquinas virtuales. Este comportamiento no suele afectar a las máquinas virtuales porque sus vCPU suelen estar inactivas durante parte del tiempo y, en la mayoría de los casos, el host no alcanza el 100% de uso de la CPU.
- Cuando la cantidad total de vCPU en el host es *mayor que* la cantidad de PCPU en el host y, en *ocasiones*, el host alcanza el 100% de uso de la CPU del host, las vCPU de las máquinas virtuales no reciben la cantidad de CPU que solicitan durante los picos. En cambio, durante estos picos, las máquinas virtuales se ralentizan para recibir una parte de la PCPU disponible en el host.
- Cuando la cantidad total de CPU virtuales en el host es *mayor que* la cantidad de PCPU en el host y el host *suele* alcanzar el 100% de uso de la CPU del host, las vCPU de las máquinas virtuales se ralentizan continuamente para recibir una parte de las CPU disponibles en el host. Si las máquinas virtuales tienen requisitos de tiempo real, esta situación no es ideal y puede solucionarla reduciendo la cantidad de vCPU en el host.

La cantidad óptima de vCPU en un host puede depender de la percepción de los usuarios de la máquina virtual sobre la velocidad de sus máquinas virtuales, especialmente cuando las máquinas virtuales tienen requisitos de tiempo real.

Obtener información sobre sus CPU

Para encontrar el número total de PCPU en su host, ejecute el siguiente comando:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe host-cpu-info --minimal
```

Para averiguar el número total de vCPU (guest y dom0) que hay actualmente en el host, ejecute el siguiente comando:

```
xl vcpu-list | grep -v VCPU | wc -l
```

Supervisión del uso de la CPU con métricas RRD

XenServer proporciona métricas de RRD que describen el rendimiento de las vCPU de las máquinas virtuales.

Cuando el uso de la CPU del host es del 100%

Cuando un host alcance el 100% del uso de la CPU del host, utilice estas métricas de VM para decidir si quiere mover la VM a otro host:

runstate_concurrency_hazard

- **runstate_concurrency_hazard > 0%** indica que, en ocasiones, al menos una vCPU está en ejecución mientras que al menos otra vCPU quiere ejecutarse, pero no puede obtener el tiempo de la CPU. Si las vCPU deben coordinarse, este comportamiento provoca problemas de rendimiento.
- El hecho de que**runstate_concurrency_hazard se acerque** al 100% es una situación que hay que evitar.

  > **Acciones sugeridas:**
  >
  > Si hay problemas de rendimiento, realice una de las siguientes acciones:
  >
  > - Reduzca la cantidad de vCPU en la máquina virtual.
  > - Mueva la máquina virtual a otro host.
  > - Reduzca la cantidad total de vCPU en el host migrando otras máquinas virtuales o disminuyendo su cantidad de vCPU.

runstate_partial_contention

- **runstate_partial_contention > 0%** indica que al menos una vCPU quiere ejecutarse pero no puede obtener el tiempo de la CPU, y también que al menos otra vCPU está bloqueada (ya sea porque no hay nada que hacer o porque está esperando a que se complete la E/S).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- El hecho de que**runstate_concurrency_hazard se acerque** al 100% es una situación que hay que evitar.

  > **Acción sugerida:**
  >
  > Compruebe si los servidores de almacenamiento de E/S de back-end están sobrecargados consultando las métricas de back-end proporcionadas por su proveedor de almacenamiento. Si los servidores de almacenamiento no están sobrecargados y hay problemas de rendimiento, lleve a cabo una de las siguientes acciones:
  >
  > - Reduzca la cantidad de vCPU en la máquina virtual.
  > - Mueva la máquina virtual a otro host.
  > - Reduzca la cantidad total de vCPU en el host migrando otras máquinas virtuales o disminuyendo su cantidad de vCPU.

runstate_full_contention

- **runstate_full_contention > 0%** indica que, a veces, las vCPU quieren ejecutarse todas al mismo tiempo, pero ninguna puede obtener el tiempo de la CPU.
- El hecho de que**runstate_full_contention se acerque al 100%** es una situación que debe evitarse.

  > **Acciones sugeridas:**
  >
  > Si hay problemas de rendimiento, realice una de las siguientes acciones:
  >
  > - Reduzca la cantidad de vCPU en la máquina virtual.
  > - Mueva la máquina virtual a otro host.
  > - Reduzca la cantidad total de vCPU en el host migrando otras máquinas virtuales o disminuyendo su cantidad de vCPU.

Cuando el uso de la PCPu del host es inferior al 100 %

Si un host no alcanza el 100% del uso de la CPU del host, utilice estas métricas de VM para decidir si una VM tiene la cantidad correcta de vCPU:

runstate_fullrun

- **runstate_fullrun = 0%** indica que las vCPU nunca se utilizan todas al mismo tiempo.

  > **Acción sugerida:**
  >
  > Reduzca la cantidad de vCPU en esta máquina virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **0% < runstate_fullrun < 100%** indica que las vCPU a veces se utilizan todas al mismo tiempo.
- **runstate_fullrun = 100%** indica que las vCPU se utilizan siempre al mismo tiempo.

  > **Acción sugerida:**
  >
  > Puede aumentar la cantidad de vCPU en esta máquina virtual hasta que runstate_fullrun sea inferior al 100%. No aumente aún más la cantidad de vCPU; de lo contrario, puede aumentar la probabilidad de peligro de concurrencia si el host alcanza el 100% del uso de la CPU.

runstate_partial_run

- **runstate_partial_run = 0%** indica que siempre se usan todas las vCPU (ejecución completa = 100%) o no se usa ninguna vCPU (inactiva = 100%).
- **0% < runstate_partial_run < 100%** indica que, en ocasiones, al menos una vCPU está bloqueada, ya sea porque no tiene nada que hacer o porque está esperando a que se complete la E/S.
- **runstate_partial_run= 100%** indica que siempre hay al menos una vCPU bloqueada.

  > **Acción sugerida**:
  >
  > Compruebe si los servidores de almacenamiento de E/S de back-end están sobrecargados. Si no lo están, es probable que la máquina virtual tenga demasiadas vCPU y usted pueda reducir la cantidad de vCPU en esta máquina virtual. Tener demasiadas vCPU en una VM puede aumentar el riesgo de que la VM entre en estado de peligro de concurrencia cuando el uso de la CPU del host alcance el 100%.

---

layout: doc
description: Create virtual machines (VMs) from templates, by cloning, or by importing existing VMs.
—

Administrar máquinas virtuales

En esta sección se proporciona una descripción general de cómo crear máquinas virtuales (VM) mediante plantillas. También explica otros métodos de preparación, como la clonación de plantillas y la importación de máquinas virtuales exportadas anteriormente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Qué es una máquina virtual?

Una máquina virtual (VM) es un equipo de software que, al igual que un equipo físico, ejecuta un sistema operativo y aplicaciones. La VM comprende un conjunto de archivos de especificación y configuración respaldados por los recursos físicos de un host. Cada VM tiene dispositivos virtuales que proporcionan las mismas funciones que el hardware físico. Las VM pueden ofrecer las ventajas de ser más portátiles, administrables y seguras. Además, puede adaptar el comportamiento de arranque de cada VM a sus requisitos específicos. Para obtener más información, consulte Comportamiento de arranque de VM.

XenServer admite invitados con cualquier combinación de direcciones configuradas IPv4 o IPv6.

En XenServer, las máquinas virtuales pueden funcionar en modo totalmente virtualizado. Las funciones específicas del procesador se utilizan para "atrapar"las instrucciones privilegiadas que lleva a cabo la máquina virtual. Esta capacidad le permite usar un sistema operativo sin modificaciones. Para el acceso a la red y al almacenamiento, los dispositivos emulados se presentan a la máquina virtual. Alternativamente, los controladores fotovoltaicos se pueden usar por razones de rendimiento y fiabilidad.

Creación de máquinas virtuales

Usar plantillas de VM

Las VM se preparan a partir de plantillas. Una plantilla es una *imagen dorada* que contiene todos los ajustes de configuración para crear una instancia de una VM específica. XenServer incluye un conjunto básico de plantillas, que son máquinas virtuales *sin procesar*, en las que puede instalar un sistema operativo. Los diferentes sistemas operativos requieren configuraciones diferentes para funcionar de la mejor manera. Las plantillas de XenServer se ajustan para maximizar el rendimiento del sistema operativo.

Hay dos métodos básicos mediante los cuales puede crear máquinas virtuales a partir de plantillas:

- Uso de una plantilla completa preconfigurada.
- Instalar un sistema operativo desde un CD, una imagen ISO o un repositorio de red en la plantilla proporcionada apropiada.

Lasmáquinas virtuales de Windows describen cómo instalar sistemas operativos Windows en las máquinas virtuales.

Las máquinas virtuales Linux describen cómo instalar sistemas operativos Linux en las máquinas virtuales.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Las plantillas creadas por versiones anteriores de XenServer se pueden usar en las versiones más recientes de XenServer. Sin embargo, las plantillas creadas en las versiones más recientes de XenServer no son compatibles con las versiones anteriores de XenServer. Si creó una plantilla de VM mediante Citrix Hypervisor 8.2, para usarla con una versión anterior, exporte los VDI por separado y vuelva a crear la VM.

Otros métodos de creación de VM

Además de crear máquinas virtuales a partir de las plantillas proporcionadas, puede utilizar los siguientes métodos para crear máquinas virtuales.

Clonar una VM existente Puede hacer una copia de una VM existente *clonando* desde una plantilla. Las plantillas son máquinas virtuales normales que están diseñadas para usarse como copias originales para crear instancias de máquinas virtuales. Una VM se puede personalizar y convertir en una plantilla. Asegúrese de seguir el procedimiento de preparación adecuado para la VM. Para obtener más información, consulte Preparación para clonar una máquina virtual Windows mediante Sysprep y Preparación para clonar una máquina virtual Linux.

> **Nota:**
>
> Las plantillas no se pueden usar como máquinas virtuales normales.

XenServer tiene dos mecanismos para clonar máquinas virtuales:

- Una copia completa
- Copia en escritura

  El modo de copia en escritura más rápido solo escribe los bloques *modificados* en el disco. La función de copia en escritura está diseñada para ahorrar espacio en disco y permitir clones rápidos, pero reduce ligeramente el rendimiento normal del disco. Una plantilla se puede clonar rápidamente varias veces sin ralentización.

  > **Nota:**
  >
  > Si clonas una plantilla en una VM y, a continuación, conviertes el clon en una plantilla, el rendimiento del disco puede disminuir. La cantidad de disminución tiene una relación lineal con el número de veces que ha ocurrido este proceso. En este caso, el comando `vm-copy` de la CLI se puede usar para realizar una copia completa de los discos y restaurar los niveles esperados de rendimiento del disco.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Notas para los grupos de recursos Si crea una plantilla a partir de discos virtuales de máquina virtual en un SR compartido, la operación de clonación de la plantilla se reenvía a cualquier host del grupo que pueda acceder a los SR compartidos. Sin embargo, si crea la plantilla a partir de un disco virtual de máquina virtual que solo tiene un SR local, la operación de clonación de la plantilla solo se puede ejecutar en el host que puede acceder a ese SR.

Importar una VM exportada Puede crear una VM *importando* una VM exportada existente. Al igual que clonar, exportar e importar una VM es una forma rápida de crear más VM de una configuración determinada. El uso de este método le permite aumentar la velocidad de su implementación. Por ejemplo, puede tener una configuración de host de propósito especial que utilice muchas veces. Después de configurar una VM según sea necesario, expórtela e impórtela más tarde para crear otra copia de la VM configurada especialmente. También puede utilizar la exportación y la importación para mover una máquina virtual al host de XenServer que se encuentra en otro grupo de recursos.

Para obtener detalles y procedimientos sobre la importación y exportación de máquinas virtuales, consulte Importación y exportación de máquinas virtuales.

Herramientas de máquinas virtuales de XenServer

Las herramientas de máquinas virtuales de XenServer proporcionan servicios de E/S de alto rendimiento sin la sobrecarga de la emulación de dispositivos tradicional.

Herramientas de máquinas virtuales de XenServer para Windows

XenServer VM Tools para Windows consta de controladores de E/S (también conocidos como controladores paravirtualizados o controladores PV) y el agente de administración.

Los controladores de E/S contienen controladores de red y almacenamiento e interfaces de administración de bajo nivel. Estos controladores sustituyen a los dispositivos emulados y proporcionan un transporte de alta velocidad entre Windows y el software de la familia de productos XenServer. Al instalar un sistema operativo Windows, XenServer utiliza la emulación de dispositivos tradicional para presentar un controlador IDE estándar y una tarjeta de red estándar a la máquina virtual. Esta emulación permite que la instalación de Windows utilice controladores integrados, pero con un rendimiento reducido debido a la sobrecarga inherente a la emulación de los controladores del controlador.

El agente de administración, también conocido como agente invitado, es responsable de las funciones de administración de máquinas virtuales de alto nivel y proporciona un conjunto completo de funciones a XenCenter.

Instale XenServer VM Tools para Windows en cada máquina virtual de Windows para que esa máquina virtual tenga una configuración totalmente compatible y pueda usar la CLI xe o XenCenter. Una

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

máquina virtual funciona sin las herramientas de máquina virtual de XenServer para Windows, pero el rendimiento se ve afectado cuando los controladores de E/S (controladores PV) no están instalados. Debe instalar XenServer VM Tools para Windows en las máquinas virtuales de Windows para poder realizar las siguientes operaciones:

- Apagar, reiniciar o suspender una VM de forma limpia
- Ver los datos de rendimiento de las VM en XenCenter
- Migrar una VM en ejecución (mediante migración en vivo o migración en vivo de almacenamiento)
- Crear instantáneas con memoria (puntos de control) o volver a instantáneas

Para obtener más información, consulte Instalar XenServer VM Tools para Windows.

Herramientas de máquinas virtuales de XenServer para Linux

Las herramientas de máquinas virtuales de XenServer para Linux contienen un agente invitado que proporciona información adicional sobre la máquina virtual al host.

Debe instalar XenServer VM Tools para Linux en las máquinas virtuales Linux para poder realizar las siguientes operaciones:

- Ver los datos de rendimiento de las VM en XenCenter
- Ajustar la cantidad de vCPU en una VM Linux en ejecución
- Habilitar el control de memoria dinámica

> **Nota:**
>
> No puede usar la función de control dinámico de memoria (DMC) en las máquinas virtuales Red Hat Enterprise Linux 8, Red Hat Enterprise Linux 9, Rocky Linux 8, Rocky Linux 9 o CentOS Stream 9, ya que estos sistemas operativos no admiten la expansión de memoria con el hipervisor Xen.

Para obtener más información, consulte Instalar XenServer VM Tools para Linux.

Descubra el estado de virtualización de una VM

XenCenter informa del estado de virtualización de una VM en la ficha **General** de la VM. Puede averiguar si XenServer VM Tools está instalado o no. Esta ficha también muestra si la VM puede instalar y recibir actualizaciones de Windows Update. En la siguiente sección se enumeran los mensajes que se muestran en XenCenter:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

E/S optimizadas (no optimizadas): este campo muestra si los controladores de E/S están instalados o no en la máquina virtual.

Agente de administración instalado (no instalado): este campo muestra si el agente de administración está instalado o no en la máquina virtual.

Capaz de (no puede) recibir actualizaciones de Windows Update: especifica si la máquina virtual puede recibir controladores de E/S de Windows Update.

> **Nota:**
>
> Windows Server Core 2016 no admite el uso de Windows Update para instalar o actualizar los controladores de E/S. En su lugar, utilice el instalador de XenServer VM Tools para Windows que se proporciona en la página de descargas de XenServer.

Instalar controladores de E/S y agente de administración: Este mensaje se muestra cuando la máquina virtual no tiene los controladores de E/S ni el agente de administración instalados.

Arranque UEFI invitado y arranque seguro

XenServer permite que los siguientes sistemas operativos invitados se inicien en modo UEFI:

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 9 (versión preliminar)
- Ubuntu 20.04
- Ubuntu 22.04

El arranque UEFI proporciona una interfaz más completa para que los sistemas operativos invitados interactúen con el hardware, lo que puede reducir significativamente los tiempos de arranque de las máquinas virtuales. Si XenServer admite el arranque UEFI para el sistema operativo invitado, le recomendamos que elija este modo de arranque en lugar de BIOS.

Para estos sistemas operativos, XenServer también admite Secure Boot. El arranque seguro evita que se ejecuten binarios sin firmar, firmados incorrectamente o modificados durante el arranque. En una máquina virtual habilitada para UEFI que aplica el arranque seguro, todos los controladores deben estar firmados. Este requisito puede limitar el rango de usos de la VM, pero proporciona la seguridad de bloquear los controladores no firmados/modificados. Si usa un controlador sin firmar, se produce un error en el arranque seguro y se muestra una alerta en XenCenter. El arranque seguro también

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

reduce el riesgo de que el malware en el huésped pueda manipular los archivos de arranque o ejecutarse durante el proceso de arranque.

Debe especificar el modo de arranque al crear una VM. No es posible cambiar el modo de arranque de una VM entre BIOS y UEFI (o arranque seguro UEFI) después de arrancar la VM por primera vez. Sin embargo, puede cambiar el modo de arranque entre UEFI y UEFI Secure Boot después de usar la máquina virtual para solucionar posibles problemas de arranque seguro. Para obtener más información, consulte Solucionar problemas.

Tenga en cuenta lo siguiente al habilitar el arranque UEFI en máquinas virtuales:

- Asegúrese de que una máquina virtual Windows compatible con UEFI tenga al menos dos vCPU. Las máquinas virtuales Linux compatibles con UEFI no tienen esta restricción.
- Puede importar o exportar una máquina virtual habilitada para UEFI creada en XenServer como un archivo OVA, OVF o XVA. No se admite la importación de una máquina virtual habilitada para UEFI desde paquetes OVA u OVF creados en otros hipervisores.
- Para usar PVS-Accelerator con máquinas virtuales habilitadas para UEFI, asegúrese de usar Citrix Provisioning 1906 o posterior.
- En el caso de las máquinas virtuales de Windows, utilice el menú de configuración de UEFI para cambiar la resolución de pantalla de la consola XenCenter. Para obtener instrucciones detalladas, consulte Solución de problemas.

> **Nota**
>
> Las VM habilitadas para UEFI usan NVME y E1000 para dispositivos emulados. La información de emulación no muestra estos valores hasta después de instalar XenServer VM Tools para Windows en la máquina virtual.
> Las máquinas virtuales habilitadas para UEFI también muestran que solo tienen 2 NIC hasta después de instalar XenServer VM Tools para Windows.

Habilitar el arranque UEFI o el arranque seguro UEFI

Puede usar XenCenter o la CLI de xe para habilitar el arranque UEFI o el arranque seguro UEFI para su máquina virtual.

Para obtener información sobre la creación de una máquina virtual compatible con UEFI en XenCenter, consulte Crear una máquina virtual Windows mediante XenCenter o Crear una máquina virtual Linux mediante XenCenter.

Uso de la CLI de xe para habilitar el arranque UEFI o el arranque seguro UEFI Cuando cree una VM, ejecute el siguiente comando antes de arrancarla por primera vez:

```
1     xe vm-param-set uuid=<UUID> HVM-boot-params:firmware=<MODE>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    xe vm-param-set uuid=<UUID> platform:device-model=qemu-upstream-
       uefi
    xe vm-param-set uuid=<UUID> platform:secureboot=<OPTION>
<!--NeedCopy-->
```

Donde UUID es el UUID de la VM, MODE es BIOS o uefi, y OPTION es "true"o "false". Si no especifica el modo, se establece de forma predeterminada en uefi si esa opción es compatible con el sistema operativo de la máquina virtual. De lo contrario, el modo se establece de forma predeterminada BIOS. Si no especifica la opción secureboot, el valor predeterminado es "automático". Para las máquinas virtuales habilitadas para UEFI, el comportamiento "automático"consiste en habilitar el arranque seguro para la máquina virtual.

Para crear una máquina virtual habilitada para UEFI a partir de una plantilla suministrada con XenServer, ejecute el siguiente comando:

```
    UUID=$(xe vm-clone name-label='Windows 10 (64-bit)' new-name-label=
       'Windows 10 (64-bit)(UEFI)')
    xe template-param-set uuid=<UUID> HVM-boot-params:firmware=<MODE>
       platform:secureboot=<OPTION>
<!--NeedCopy-->
```

No ejecute este comando para plantillas que tengan algo instalado o plantillas que haya creado a partir de una instantánea. El modo de arranque de estas instantáneas no se puede cambiar y, si intenta cambiar el modo de arranque, la VM no arranca.

Cuando arranca la máquina virtual habilitada para UEFI, la primera vez que se le pide en la consola de la máquina virtual que presione cualquier tecla para iniciar la instalación. Si no inicia la instalación del sistema operativo, la consola de la máquina virtual cambia al shell UEFI.

Para reiniciar el proceso de instalación, en la consola UEFI, escriba los siguientes comandos.

```
EFI:
EFI\BOOT\BOOTX64
```

Cuando se reinicie el proceso de instalación, observe la consola de la VM para ver el mensaje de instalación. Cuando aparezca el mensaje, presiona cualquier tecla.

Desactivación del arranque seguro

Es posible que quiera desactivar el arranque seguro en ocasiones. Por ejemplo, algunos tipos de depuración no se pueden habilitar en una máquina virtual que esté en modo de usuario de arranque seguro. Para inhabilitar el arranque seguro, cambie la VM al modo de configuración de arranque seguro. En el host de XenServer, ejecute el siguiente comando:

```
varstore-sb-state <VM_UUID> setup
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Teclas

Para máquinas virtuales Windows:

Las máquinas virtuales Windows compatibles con UEFI se aprovisionan con una PK a partir de una clave privada efímera, la KEK de Microsoft, la PCA de producción de Microsoft Windows y las claves de terceros de Microsoft. Las VM también reciben una lista de revocaciones actualizada del foro de la UEFI. Esta configuración permite que las máquinas virtuales de Windows se inicien con el arranque seguro activado y reciban actualizaciones automáticas de las claves y la lista de revocaciones de Microsoft.

Para máquinas virtuales Linux:

Para instalar controladores de terceros en una máquina virtual Linux que tenga habilitado el arranque seguro, debe crear una clave de firma, agregarla a la máquina virtual como clave de propietario de la máquina (MOK) y usar esa clave para firmar el controlador. Para obtener más información, consulte Instalar controladores de terceros en su máquina virtual Linux de arranque seguro.

Solución de problemas de las máquinas virtuales de arranque seguro UEFI y UEFI

Para obtener información sobre la solución de problemas de las máquinas virtuales de arranque seguro UEFI o UEFI, consulte Solucionar problemas de arranque seguro y UEFI.

Invitados apoyados y asignación de recursos

Para obtener una lista de los sistemas operativos invitados compatibles, consulte Invitados compatibles, memoria virtual y límites de tamaño de disco

En esta sección se describen las diferencias en el soporte de dispositivos virtuales para los miembros de la familia de productos XenServer.

Compatibilidad con dispositivos virtuales de la familia de productos XenServer

La versión actual de la familia de productos XenServer tiene algunas limitaciones generales en los dispositivos virtuales para máquinas virtuales. Los sistemas operativos invitados específicos pueden tener límites más bajos para ciertas funciones. En la sección de instalación de invitados individuales se indican las limitaciones. Para obtener información detallada sobre los límites de configuración, consulte Límites de configuración.

Factores como el hardware y el entorno pueden afectar las limitaciones. Para obtener información sobre el hardware compatible, consulte la Lista de compatibilidad de hardwarede XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Dispositivos de bloques de VM XenServer emula un bus IDE en forma de dispositivo. hd* Al usar Windows, al instalar XenServer VM Tools, se instala un controlador de E/S especial que funciona de forma similar a Linux, excepto en un entorno totalmente virtualizado.

Funciones de la CPU

El conjunto de funciones de CPU de un grupo puede cambiar mientras se ejecuta una máquina virtual, por ejemplo, cuando se agrega un nuevo host a un grupo existente o cuando la máquina virtual se migra a un host de otro grupo. Cuando el conjunto de funciones de la CPU de un grupo cambia, la máquina virtual sigue utilizando el conjunto de funciones que se aplicó cuando se inició. Para actualizar la máquina virtual para usar el nuevo conjunto de funciones del grupo, debe reiniciar la máquina virtual.

VM de Windows

April 10, 2024

La instalación de máquinas virtuales de Windows en el host de XenServer requiere soporte de virtualización de hardware (Intel VT o AMD-V).

> **Nota:**
>
> La virtualización anidada no es compatible con las máquinas virtuales de Windows alojadas en XenServer.

Procedimiento básico para crear una VM Windows

El proceso de instalación de Windows en una máquina virtual consiste en los siguientes pasos:

1. Selección de la plantilla de Windows apropiada
2. Elección del modo de arranque apropiado
3. Instalación del sistema operativo Windows
4. Instalación de XenServer VM Tools para Windows (*controladores de E/S* y el *agente de administración*)

> **Advertencia:**
>
> Las máquinas virtuales de Windows solo se admiten cuando las máquinas virtuales tienen instaladas las herramientas de máquinas virtuales de XenServer para Windows.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Plantillas de VM de Windows

Los sistemas operativos Windows se instalan en las máquinas virtuales mediante la clonación de una plantilla adecuada mediante XenCenter o la CLI de xe y, a continuación, la instalación del sistema operativo. Las plantillas para huéspedes individuales tienen establecidos indicadores de plataforma predefinidos que definen la configuración del hardware virtual. Por ejemplo, todas las máquinas virtuales de Windows se instalan con el modo Capa de abstracción de hardware (HAL) de ACPI habilitado. Si posteriormente cambia una de estas máquinas virtuales para que tenga varias CPU virtuales, Windows cambia automáticamente la HAL al modo multiprocesador.

Las plantillas de Windows disponibles se enumeran en la siguiente tabla:

Nombre de plantilla	Modos de arranque compatibles	Descripción
Windows 10 (64 bits)	Arranque seguro de BIOS, UEFI, UEFI	Se utiliza para instalar Windows 10 (64 bits)
Windows 11 (64 bits)	UEFI, arranque seguro de UEFI	Se usa para instalar Windows 11 (64 bits)
Windows Server 2016 (64 bits)	Arranque seguro de BIOS, UEFI, UEFI	Se utiliza para instalar Windows Server 2016 o Windows Server Core 2016 (64 bits)
Windows Server 2019 (64 bits)	Arranque seguro de BIOS, UEFI, UEFI	Se utiliza para instalar Windows Server 2019 o Windows Server Core 2019 (64 bits)
Windows Server 2022 (64 bits)	Arranque seguro de BIOS, UEFI, UEFI	Se utiliza para instalar Windows Server 2022 o Windows Server Core 2022 (64 bits)

XenServer admite todos los SKU (ediciones) de las versiones de Windows enumeradas.

Adjuntar una biblioteca de imágenes ISO

El sistema operativo Windows se puede instalar desde un CD de instalación en una unidad de CD-ROM física en el host XenServer o desde una imagen ISO. Consulte Crear imágenes ISO para obtener información sobre cómo crear una imagen ISO desde un CD de instalación de Windows y ponerla a disposición para su uso.

Crear una VM mediante XenCenter

Para crear una VM Windows:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. En la barra de herramientas de XenCenter, haga clic en el botón **Nueva máquina virtual** para abrir el asistente para nueva máquina virtual.

   El asistente para nueva VM le permite configurar la nueva VM, ajustando varios parámetros para la CPU, el almacenamiento y los recursos de red.

2. Seleccione una plantilla de VM y haga clic en **Siguiente**.

   Cada plantilla contiene la información de configuración necesaria para crear una VM con un sistema operativo (SO) invitado específico y con un almacenamiento óptimo. Esta lista refleja las plantillas que XenServer admite actualmente.

   > **Nota:**
   >
   > Si el sistema operativo que va a instalar en su máquina virtual solo es compatible con el hardware original, marque la casilla **Copiar cadenas de BIOS del host a la máquina virtual**. Por ejemplo, puede usar esta opción para un CD de instalación de SO que se empaquetó con un equipo específico.
   >
   > Después de iniciar una VM por primera vez, no puede cambiar sus cadenas de BIOS. Asegúrese de que las cadenas del BIOS sean correctas antes de iniciar la VM por primera vez.

   Para copiar cadenas de BIOS mediante la CLI, consulte Instalación de máquinas virtuales desde un soporte del kit de opciones del distribuidor (bloqueado por BIOS).

   Los usuarios avanzados pueden configurar cadenas de BIOS definidas por el usuario. Para obtener más información, consulte Cadenas de BIOS definidas por el usuario.

3. Introduzca un nombre y una descripción opcional para la nueva VM.

4. Elija el origen del medio del sistema operativo que quiere instalar en la nueva máquina virtual.

   La instalación desde un CD/DVD es la opción más sencilla para empezar.

   a) Elija la opción de fuente de instalación predeterminada (unidad de DVD)
   b) Inserte el disco en la unidad de DVD del host XenServer

   XenServer también le permite extraer los medios de instalación del sistema operativo de una variedad de fuentes, incluida una biblioteca ISO preexistente. Una imagen ISO es un archivo que contiene toda la información que contendría un disco óptico (CD, DVD, etc.). En este caso, una imagen ISO contendría los mismos datos del sistema operativo que un CD de instalación de Windows.

   Para adjuntar una biblioteca ISO preexistente, haga clic en **Nueva biblioteca ISO** e indique la ubicación y el tipo de la biblioteca ISO. A continuación, puede elegir el medio ISO del sistema operativo específico de la lista.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. En la ficha **Medios de instalación**, puede elegir un modo de arranque para la máquina virtual. De forma predeterminada, XenCenter selecciona el modo de arranque más seguro disponible para la versión del sistema operativo de la máquina virtual.

   > **Notas:**
   >
   > - Las opciones de **arranqueUEFI y arranque seguro** UEFI aparecen atenuadas si la plantilla de VM que ha elegido no admite el arranque UEFI.
   > - No puede cambiar el modo de arranque después de arrancar la VM por primera vez.
   >
   > Para obtener más información, consulte Arranque UEFI invitado y Arranque seguro.

6. Si es necesario, cambie la opción **Crear y adjuntar un nuevo vTPM**.

   - Para los sistemas operativos de máquinas virtuales que requieren un vTPM, la opción está seleccionada y no se puede anular la selección.
   - Para los sistemas operativos de máquinas virtuales que no admiten un vTPM, la opción aparece atenuada y no se puede seleccionar.
   - Para los sistemas operativos de máquinas virtuales que admiten vTPM, pero no lo requieren, elija si desea conectar un vTPM a la máquina virtual.

   Para obtener más información, consulte vTPM.

7. Seleccione un servidor doméstico para la VM.

   Un servidor doméstico es el host que proporciona los recursos para una máquina virtual en un grupo. Al designar un servidor doméstico para una máquina virtual, XenServer intenta iniciar la máquina virtual en ese host. Si esta acción no es posible, se selecciona automáticamente un anfitrión alternativo dentro del mismo grupo. Para elegir un servidor doméstico, haga clic en **Colocar la máquina virtual en este servidor** y seleccione un host de la lista.

   > **Notas:**
   >
   > - En los grupos habilitados para WLB, el servidor doméstico designado no se usa para iniciar, reiniciar, reanudar o migrar la VM. En cambio, Workload Balancing designa el mejor host para la máquina virtual mediante el análisis de las métricas del grupo de recursos de XenServer y la recomendación de optimizaciones.
   > - Si una VM tiene una o más GPU virtuales asignadas, la nominación de servidor doméstico no se aplica. En cambio, la nominación del anfitrión se basa en la directiva de ubicación de la GPU virtual establecida por el usuario.
   > - Durante la actualización progresiva del pool, no se tiene en cuenta el servidor doméstico al migrar la máquina virtual. En su lugar, la máquina virtual se migra de nuevo al host en el que estaba antes de la actualización.

   Si no quiere designar un servidor doméstico, haga clic en **No asignar un servidor doméstico a**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

esta máquina virtual. La máquina virtual se inicia en cualquier host con los recursos necesarios.

Haga clic en **Next** para continuar.

8. Asigne recursos de memoria y procesador para la VM. Para una máquina virtual Windows 10 (64 bits), los valores predeterminados son 2 CPU virtuales y 4 GB de RAM. También puede optar por modificar los valores predeterminados. Haga clic en **Next** para continuar.

9. Asigna una GPU virtual. El asistente para nueva VM le pide que asigne una GPU dedicada o una o más GPU virtuales a la VM. Esta opción permite que la VM utilice la potencia de procesamiento de la GPU. Con esta función, tiene un mejor soporte para aplicaciones de gráficos profesionales en 3D de alta gama, como CAD/CAM, GIS y aplicaciones de imágenes médicas.

10. Asigne y configure el almacenamiento para la nueva VM.

    Haga clic en **Siguiente** para seleccionar la asignación predeterminada (32 GB) y la configuración, o puede que quiera realizar la siguiente configuración adicional:

    - Cambie el nombre, la descripción o el tamaño del disco virtual haciendo clic en **Modificar**.
    - Para agregar un disco virtual nuevo, seleccione **Agregar**.

11. Configure las redes en la nueva VM.

    Haga clic en **Siguiente** para seleccionar la NIC y las configuraciones predeterminadas, incluida una dirección MAC única creada automáticamente para cada NIC. Como alternativa, es posible que quiera realizar la siguiente configuración adicional:

    - Cambie la red física, la dirección MAC o la prioridad de calidad de servicio (QoS) del disco virtual haciendo clic en **Modificar**.
    - Agregue una nueva NIC virtual seleccionando **Agregar**.

12. (Opcional) Si esta máquina virtual se va a usar como plantilla con Citrix Provisioning o con el indicador `reset-on-boot` establecido, asegúrese de que no esté seleccionada la opción **Iniciar la nueva máquina virtual automáticamente**. Esto le permite realizar algunas de las configuraciones necesarias antes de instalar Windows.

13. Revise la configuración y, a continuación, haga clic en **Crear ahora** para crear la VM y volver a la ficha **Buscar**.

    Aparece un icono para la nueva VM debajo del host en el panel **Recursos**.

14. (Opcional) Si esta máquina virtual está pensada para usarse como plantilla en Citrix Provisioning o tiene el indicador `reset-on-boot` establecido, configúrela antes de instalar Windows.

    En la consola host, escriba el siguiente comando:

    ```
    1 xe vm-param-set uuid=<uuid> has-vendor-device=false
    ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El indicador `has-vendor-device=false` garantiza que Windows Update no intente instalar ni actualizar los controladores de E/S incluidos en XenServer VM Tools. Para obtener más información, consulte Configuración de los destinos de Citrix Provisioning o de las máquinas que se restablecen al arrancar.

15. En el panel **Recursos**, seleccione la VM y, a continuación, haga clic en la ficha **Consola** para ver la consola de VM.
16. (Opcional) Si desea poder clonar la máquina virtual, le recomendamos que no ejecute la configuración inicial de Windows, conocida como Out-Out-Box-Experience (OOBE). En su lugar, cuando el OOBE comience en la página que solicita información sobre la región, pulse **Ctrl + Shift + F3** para entrar en el modo de auditoría.

    A continuación, puede usar Sysprep para generalizar la máquina virtual. Para obtener más información, consulte Preparar la clonación de una máquina virtual de Windows mediante Sysprep.

    Si no tiene intención de clonar la máquina virtual, continúe con los pasos siguientes de este procedimiento.
17. Siga la pantalla de instalación del sistema operativo y haga sus selecciones.
18. Una vez finalizada la instalación del sistema operativo y la máquina virtual se reinicie, instale XenServer VM Tools para Windows.

Crear una VM Windows mediante la CLI

Para crear una máquina virtual Windows a partir de un repositorio ISO mediante la CLI de xe:

> **Nota:**
>
> Para las máquinas virtuales con Windows 10 y Windows 11, la plantilla especifica el requisito de un vTPM. No es necesario agregar nada a los comandos de la CLI xe para configurar el vTPM.

1. Crea una VM a partir de una plantilla:

```
xe vm-install new-name-label=<vm_name> template=<template_name>
<!--NeedCopy-->
```

    Este comando devuelve el UUID de la nueva VM.

2. (Opcional) Cambie el modo de arranque de la máquina virtual.

```
xe vm-param-set uuid=<uuid> HVM-boot-params:firmware=<mode>
xe vm-param-set uuid=<uuid> platform:secureboot=<option>
<!--NeedCopy-->
```

    El valor de `mode` puede ser `BIOS` o `uefi` y el valor predeterminado es `uefi` si esa opción es compatible con el sistema operativo de su máquina virtual. De lo contrario, el modo se es-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

tablece de forma predeterminada `BIOS`. El valor de `option` se puede establecer en **`true`** o **`false`**. Si no especifica la opción Arranque seguro, el valor predeterminado es. `auto`

Para obtener más información, consulte Arranque UEFI de invitado y Arranque seguro.

3. (Opcional) Si esta máquina virtual está pensada para usarse como plantilla en Citrix Provisioning o tiene el indicador `reset-on-boot` establecido, configúrela antes de instalar Windows.

```
xe vm-param-set uuid=<uuid> has-vendor-device=false
<!--NeedCopy-->
```

El indicador `has-vendor-device=false` garantiza que Windows Update no intente instalar ni actualizar los controladores de E/S incluidos en XenServer VM Tools. Para obtener más información, consulte Configuración de los destinos de Citrix Provisioning o de las máquinas que se restablecen al arrancar.

4. Cree un repositorio de almacenamiento ISO:

```
xe-mount-iso-sr <path_to_iso_sr>
<!--NeedCopy-->
```

5. Enumera todas las ISO disponibles:

```
xe cd-list
<!--NeedCopy-->
```

6. Inserte la ISO especificada en la unidad de CD virtual de la VM especificada:

```
xe vm-cd-add vm=<vm_name> cd-name=<iso_name> device=3
<!--NeedCopy-->
```

7. Inicie la VM e instale el sistema operativo:

```
xe vm-start vm=<vm_name>
<!--NeedCopy-->
```

En este punto, la consola de VM está visible en XenCenter.

8. En el panel **Recursos** de XenCenter, seleccione la máquina virtual y, a continuación, haga clic en la ficha **Consola** para ver la consola de máquina virtual.

9. (Opcional) Si desea poder clonar la máquina virtual, le recomendamos que no ejecute la configuración inicial de Windows, conocida como Out-Out-Box-Experience (OOBE). En su lugar, cuando el OOBE comience en la página que solicita información sobre la región, pulse **Ctrl + Shift + F3** para entrar en el modo de auditoría.

A continuación, puede usar Sysprep para generalizar la máquina virtual. Para obtener más información, consulte Preparar la clonación de una máquina virtual de Windows mediante Sysprep.

Si no tiene intención de clonar la máquina virtual, continúe con los pasos siguientes de este procedimiento.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

10. Siga la pantalla de instalación del sistema operativo y haga sus selecciones.
11. Una vez completada la instalación del sistema operativo y reiniciada la máquina virtual, instale XenServer VM Tools para Windows.

Para obtener más información sobre el uso de la CLI, consulte Interfaz de línea de comandos.

Instalación de XenServer VM Tools para Windows

Las herramientas de máquinas virtuales de XenServer para Windows proporcionan servicios de E/S de alto rendimiento sin la sobrecarga de la emulación de dispositivos tradicional. Para obtener más información sobre XenServer VM Tools para Windows y su uso avanzado, consulte XenServer VMTools para Windows.

> **Nota:**
>
> Para instalar XenServer VM Tools para Windows en una máquina virtual Windows, la máquina virtual debe ejecutar Microsoft.NET Framework versión 4.0 o posterior.

Antes de instalar XenServer VM Tools para Windows, asegúrese de que su máquina virtual esté configurada para recibir los controladores de E/S de Windows Update. Windows Update es la forma recomendada de recibir actualizaciones de los controladores de E/S. Sin embargo, si Windows Update no es una opción disponible para su máquina virtual, también puede recibir actualizaciones de los controladores de E/S por otros medios. Para obtener más información, consulte XenServer VM Tools para Windows.

Para instalar XenServer VM Tools para Windows:

1. Se recomienda realizar una instantánea de la máquina virtual antes de instalar o actualizar XenServer VM Tools.
2. Descargue el archivo XenServer VM Tools para Windows desde la página de descargas de XenServer.
3. Verifique su descarga con el valor SHA256 proporcionado.
4. Copie el archivo en su máquina virtual de Windows o en una unidad compartida a la que pueda acceder la máquina virtual de Windows.
5. Ejecute el `managementagentxXX.msi` archivo para iniciar la instalación de XenServer VM Tools.

   ```
   1 Msiexec.exe /package managementagentxXX.msi
   ```

6. Siga las instrucciones del instalador.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a) Siga las instrucciones del asistente para aceptar el acuerdo de licencia y elegir una carpeta de destino.

b) El asistente muestra la configuración recomendada en la página **Configuración de instalación y actualizaciones**. Para obtener información sobre cómo personalizar estos ajustes, consulte XenServer VM Tools para Windows.

c) Haga clic en **Siguiente** y, a continuación, en **Instalar** para iniciar el proceso de instalación de XenServer VM Tools para Windows.

7. Reinicie la VM cuando se le pida que complete el proceso de instalación.

vTPM

XenServer le permite crear un módulo de plataforma segura (vTPM) virtual y conectarlo a su máquina virtual Windows 10 o Windows 11.

Las máquinas virtuales de Windows 11 requieren la presencia de un vTPM vinculado. Este vTPM se crea automáticamente cuando se crea la máquina virtual de Windows 11 a partir de la plantilla proporcionada. Para las máquinas virtuales de Windows 10, el vTPM es opcional.

Una máquina virtual tiene una relación de uno a uno con su vTPM vinculado. Una máquina virtual solo puede tener un vTPM y un vTPM solo puede estar asociado a una sola máquina virtual. Los usuarios con las funciones de administrador de máquina virtual y superiores pueden crear y destruir instancias de vTPM.

Las aplicaciones que se ejecutan en la máquina virtual pueden acceder al vTPM a través de la API compatible con TPM 2.0. No se admite TPM 1.2. Los usuarios con las funciones de operador de máquina virtual y superiores pueden acceder al vTPM a través de la máquina virtual.

Para comprobar si la máquina virtual tiene un vTPM vinculado, en XenCenter, vaya a la ficha **General** y consulte la sección **Seguridad del dispositivo**.

Limitaciones

Las siguientes restricciones se aplican actualmente a las máquinas virtuales creadas con un vTPM adjunto:

- Si bien puede exportar sus máquinas virtuales al formato OVF/OVA, todos los datos de su vTPM se pierden como parte de este proceso. Esta pérdida de datos puede provocar que la máquina virtual muestre comportamientos inesperados o impedir que se inicie. Si utiliza alguna función de vTPM en la máquina virtual, no exporte las máquinas virtuales con este formato.
- Actualmente, BitLocker no es compatible con las máquinas virtuales con un vTPM conectado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Actualmente, la alta disponibilidad no es compatible con máquinas virtuales con un vTPM adjunto.
- No puede realizar una instantánea ni poner en punto de control una máquina virtual suspendida con un vTPM conectado.

Problemas conocidos

- Si tiene muchas máquinas virtuales con un vTPM, puede experimentar los siguientes comportamientos:
  - La base de datos XAPI se hace grande y consume mucha memoria.
  - Las escrituras de máquinas virtuales en el vTPM pueden provocar un cuello de botella en la pila de herramientas.
- Las operaciones de vTPM realizadas por el usuario o por Windows en segundo plano pueden fallar en las siguientes situaciones:
  - Si la pila de herramientas o el host de XenServer se bloquean antes de que la operación se sincronice con el disco. Se ignoran los errores al escribir en el disco.

  En el caso de este tipo de error, el vTPM devuelve un error al sistema operativo. Windows registra estos errores en el registro de eventos del sistema.

Adjuntar un vTPM a una máquina virtual de Windows

Para las nuevas máquinas virtuales de Windows 11 y Windows 10, el vTPM se puede agregar durante la creación de la máquina virtual. Para obtener más información, consulte la documentación del método de creación de máquinas virtuales que prefiera.

Si tiene una máquina virtual Windows 10 de arranque seguro UEFI o UEFI existente a la que desea agregar un vTPM, puede hacerlo mediante XenCenter o mediante la CLI xe. Si desea actualizar el sistema operativo de la máquina virtual a uno que requiera un vTPM, debe conectar el vTPM a la máquina virtual *antes* de actualizar el sistema operativo de la máquina virtual.

Mediante XenCenter

1. Apague la máquina virtual de Windows 10.
2. Agregue un vTPM a la máquina virtual.
   a) Haga clic con el botón derecho en la máquina virtual y seleccione **Administrar vTPM**. O bien, en la barra de menú principal, vaya a **VM > Administrar vTPM**. Se abre el cuadro de diálogo **TPM Manager** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

b) En el cuadro de diálogo **Administrador de TPM**, agregue un vTPM.

3. Para comprobar que la máquina virtual tiene un vTPM vinculado, seleccione la máquina virtual, vaya a la ficha **General** y consulte la sección **Seguridad del dispositivo** .
4. Inicie la máquina virtual de Windows 10.

Mediante la CLI xe

1. Apague la máquina virtual:

```
xe vm-shutdown uuid=<vm_uuid>
<!--NeedCopy-->
```

2. Cree un vTPM y adjúntelo a la máquina virtual:

```
xe vtpm-create vm-uuid=<vm_uuid>
<!--NeedCopy-->
```

3. Inicie la máquina virtual:

```
xe vm-start uuid=<vm_uuid>
<!--NeedCopy-->
```

Actualice el sistema operativo Windows en su máquina virtual

Por lo general, se requieren actualizaciones a máquinas virtuales cuando se cambia a una versión más reciente de XenServer.

Antes de actualizar su máquina virtual Windows

1. Si va a actualizar el sistema operativo a una versión de Windows que requiere un vTPM (como Windows 11), debe conectar un vTPM a la máquina virtual antes de actualizar su sistema operativo. Para obtener más información, consulte Adjuntar un vTPM a una máquina virtual Windows.
2. Actualice XenServer VM Tools para Windows a la versión más reciente de la máquina virtual. Para obtener más información, consulte XenServer VM Tools para Windows.

   Le recomendamos que no elimine las herramientas de máquina virtual de XenServer de la máquina virtual de Windows antes de actualizar automáticamente la versión de Windows en la máquina virtual.

Actualizar el sistema operativo Windows

Puede actualizar las máquinas virtuales de Windows de una de las siguientes maneras:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Use Windows Update para actualizar la versión del sistema operativo Windows en las máquinas virtuales de Windows. Si usa Windows Update para actualizar las herramientas de máquina virtual de XenServer, le recomendamos que utilice este método.
- Utilice la ISO de instalación de Windows para las versiones más recientes. Los discos de instalación de Windows suelen ofrecer una opción de actualización si los arranca en un servidor que ya tiene instalada una versión anterior de Windows.

En la consola de VM de Windows, siga las instrucciones de actualización proporcionadas por Windows.

Prepararse para clonar una VM Windows mediante Sysprep

La única forma admitida de clonar una VM de Windows es mediante la utilidad de Windows `sysprep` para preparar la VM.

La utilidad `sysprep` cambia el SID del equipo local para que sea único para cada equipo. Los binarios `sysprep` están en la carpeta `C:\Windows\System32\Sysprep`.

Para obtener más información sobre el uso de Sysprep, consulte Sysprep (generalizar) una instalación de Windows.

Para ejecutar sysprep en una máquina virtual de Windows:

> **Nota:**
>
> En Windows 10 y 11, la configuración inicial de Windows o la configuración rápida (OOBE) instala aplicaciones (como AppX) que pueden interferir en el proceso `sysprep`. Debido a este comportamiento, al crear una máquina virtual clonable, recomendamos omitir la configuración inicial e iniciar Windows en modo de auditoría.

1. Cree una máquina virtual de Windows.
2. Instala Windows.
3. (Opcional) Cuando comience la experiencia predeterminada (OOBE) en la página que solicita información sobre la región, pulse **Ctrl**+ Shift + F3. Windows se inicia en modo auditoría. Para obtener más información, consulte Arrancar Windows en modo Auditoría u OOBE.

   Si bien no es obligatorio, le recomendamos que salgas de OOBE para evitar crear una cuenta de usuario innecesaria en la imagen y evitar problemas de compatibilidad con aplicaciones de terceros. Si continúa con OOBE, es posible que algunas aplicaciones o actualizaciones de Windows que se instalen durante OOBE impidan que Sysprep funcione correctamente.
4. Instale la versión más reciente de XenServer VM Tools para Windows.
5. Instale cualquier aplicación y realice cualquier otra configuración necesaria.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Ejecute `sysprep` para generalizar la máquina virtual. Esta utilidad apaga la VM cuando se completa.

> **Nota:**
>
> No vuelva a reiniciar la máquina virtual original y generalizada (la máquina virtual "de origen") después de la etapa `sysprep`. Conviértalo inmediatamente en una plantilla para evitar que se reinicie. Si se reinicia la máquina virtual de origen, `sysprep` debe ejecutarse de nuevo en ella antes de que se pueda usar de forma segura para hacer más clones.

Para clonar una máquina virtual de Windows generalizada:

1. Mediante XenCenter, convierta la máquina virtual en una plantilla.
2. Clonar la plantilla recién creada en máquinas virtuales nuevas según sea necesario.
3. Cuando se inicia la VM clonada, completa las siguientes acciones antes de estar disponible para su uso:
    - Obtiene un nuevo SID y un nombre
    - Ejecuta una configuración para solicitar valores de configuración según sea necesario.
    - Por último, se reinicia

Notas de la versión de VM Windows

Hay muchas versiones y variaciones de Windows con diferentes niveles de asistencia para las funciones que proporciona XenServer. En esta sección se enumeran notas y erratas para las diferencias conocidas.

Problemas generales de Windows

- Al instalar máquinas virtuales de Windows, comience con no más de tres discos vDisk. Después de instalar la máquina virtual y las herramientas de máquina virtual de XenServer para Windows, puede agregar discos virtuales adicionales. Asegúrese de que el dispositivo de arranque sea siempre uno de los discos iniciales para que la máquina virtual pueda arrancar correctamente sin las herramientas de máquina virtual de XenServer para Windows.
- Cuando el modo de arranque de una máquina virtual de Windows es arranque por BIOS, Windows formatea el disco principal con un registro de arranque maestro (MBR). El MBR limita el espacio de almacenamiento direccionable máximo de un disco a 2 TiB. Para usar un disco de más de 2 TiB con una máquina virtual de Windows, realice una de las siguientes acciones:
    - Si el arranque UEFI es compatible con la versión de Windows, asegúrese de usar UEFI como modo de arranque para la máquina virtual de Windows.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Cree el disco grande como disco secundario para la VM y seleccione el formato de tabla de particiones GUID (GPT).

- Varias CPU virtuales se exponen como zócalos de CPU a los invitados de Windows y están sujetas a las limitaciones de licencia presentes en la VM. La cantidad de CPU presentes en el huésped se puede confirmar consultando el Administrador de dispositivos. La cantidad de CPU que utiliza Windows se puede ver en el Administrador de tareas.
- El orden de enumeración de discos en un invitado de Windows puede diferir del orden en que se agregaron inicialmente. Este comportamiento se debe a la interacción entre los controladores de E/S y el subsistema Plug-and-Play de Windows. Por ejemplo, el primer disco puede aparecer como `Disk 1`, el siguiente disco conectado en caliente como `Disk 0`, un disco posterior como `Disk 2` y, a continuación, hacia arriba de la manera esperada.
- Un error en el back-end de DirectX del reproductor VLC reemplaza el amarillo con el azul durante la reproducción de vídeo cuando las propiedades de pantalla de Windows se configuran en color de 24 bits. VLC mediante OpenGL como back-end funciona correctamente, y cualquier otro reproductor de vídeo basado en DirectX u OpenGL funciona también. No es un problema si el invitado está configurado para usar colores de 16 bits en lugar de 24.
- El adaptador PV Ethernet informa de una velocidad de 100 Gbps en las VM de Windows. Esta velocidad es un valor codificado artificial y no es relevante en un entorno virtual porque la NIC virtual está conectada a un conmutador virtual. La VM de Windows usa la velocidad máxima disponible, pero es posible que la red no sea capaz de alcanzar los 100 Gbps completos.
- Si intenta realizar una conexión RDP insegura a una máquina virtual de Windows, esta acción puede fallar y mostrar el siguiente mensaje de error: "Esto podría deberse a la corrección de Oracle de cifrado de CredSSP. "Este error se produce cuando la actualización del protocolo de proveedor de soporte de seguridad de credenciales (CredSSP) se aplica solo a uno de los clientes y servidores de la conexión RDP. Para obtener más información, consulte https://support.microsoft.com/en-gb/help/4295591/credssp-encryption-oracle-remediation-error-when-to-rdp-to-azure-vm.

Herramientas de máquinas virtuales de XenServer para Windows

April 10, 2024

XenServer VM Tools (anteriormente Citrix VM Tools o XenServer PV Tools) para Windows proporciona servicios de E/S de alto rendimiento sin la sobrecarga de la emulación de dispositivos tradicional. XenServer VM Tools para Windows consta de controladores de E/S (también conocidos como controladores paravirtualizados o controladores PV) y el agente de administración.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Las herramientas de máquina virtual de XenServer para Windows deben estar instaladas en cada máquina virtual de Windows para que la máquina virtual tenga una configuración totalmente compatible. Una máquina virtual funciona sin ellas, pero el rendimiento se ve obstaculizado.

La versión de XenServer VM Tools para Windows se actualiza de forma independiente de la versión de XenServer. Asegúrese de que las herramientas de máquinas virtuales de XenServer para Windows se actualicen periódicamente a la última versión, tanto en las máquinas virtuales como en las plantillas que utilice para crear las máquinas virtuales. Para obtener más información sobre la versión más reciente de las herramientas, consulte Novedades.

Instalación de XenServer VM Tools

> **Nota:**
>
> Para instalar XenServer VM Tools para Windows en una máquina virtual Windows, la máquina virtual debe ejecutar Microsoft.NET Framework versión 4.0 o posterior.

Las herramientas de máquina virtual de XenServer para Windows se instalan de forma predeterminada en el `C:\Program Files\XenServer\XenTools` directorio de la máquina virtual.

Para instalar XenServer VM Tools para Windows:

1. Se recomienda realizar una instantánea de la máquina virtual antes de instalar o actualizar XenServer VM Tools.
2. Descargue el archivo XenServer VM Tools para Windows desde la página de descargas de XenServer.
3. Verifique su descarga con el valor SHA256 proporcionado.
4. Copie el archivo en su máquina virtual de Windows o en una unidad compartida a la que pueda acceder la máquina virtual de Windows.
5. Ejecute el `managementagentx64.msi` archivo para iniciar la instalación de XenServer VM Tools.

   ```
   1 Msiexec.exe /package managementagentx64.msi
   ```

6. Siga las instrucciones del instalador.

   - Siga las instrucciones del asistente para aceptar el acuerdo de licencia y elegir una carpeta de destino.
   - Personalice la configuración en la página **Configuración de instalación y actualizaciones**.

     De forma predeterminada, el asistente muestra la siguiente configuración recomendada:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Instale los controladores de E/S ahora
  - Si la máquina virtual tiene configurado `has-vendor-device=true`, esta opción no está seleccionada porque Windows Update ya ha instalado los controladores de E/S.
  - SI la máquina virtual tiene configurado `has-vendor-device=false`, se selecciona esta opción.
- Permitir las actualizaciones automáticas del agente de administración
- No permitir que el agente de administración actualice automáticamente los controladores de E/S
- Enviar información de uso anónima a Cloud Software Group, Inc.

En algunos casos de uso, se recomiendan parámetros de actualización diferentes. Para obtener más información, consulte Actualizar XenServer VM Tools.

Para configurar los parámetros de actualización, puede realizar los siguientes cambios:

- Si no quiere permitir la actualización automática del agente de administración, seleccione **No permitir actualizaciones automáticas del agente de administración** en la lista.
- Si quiere permitir que el agente de administración actualice automáticamente los controladores de E/S, seleccione **Permitir actualizaciones automáticas de controladores de E/S por parte del agente de administración**. Sin embargo, se recomienda utilizar Windows Update para actualizar los controladores de E/S, no el agente de administración. Si ha elegido recibir actualizaciones de controladores de E/S a través del mecanismo de Windows Update, no permita que el agente de administración actualice los controladores de E/S automáticamente.
- Si no quieres compartir información de uso anónima con nosotros, desmarca la casilla **Enviar información de uso anónima a Cloud Software Group, Inc.** La información transmitida a Cloud Software Group contiene los cuatro primeros caracteres del UUID de la máquina virtual que solicita la actualización. No se recopila ni transmite ninguna otra información relacionada con la máquina virtual.

- Haga clic en **Siguiente** y, a continuación, en **Instalar** para iniciar el proceso de instalación de XenServer VM Tools para Windows.

7. Reinicie la VM cuando se le pida que complete el proceso de instalación.

   Es posible que los clientes que instalen XenServer VM Tools para Windows o el agente de administración a través de RDP no vean la solicitud de reinicio, ya que solo aparece en la sesión de la consola de Windows. Para asegurarse de reiniciar la VM (si es necesario) y para que la VM alcance un estado optimizado, especifique la opción forzar reinicio en RDP. La opción forzar reinicio reinicia la VM solo si es necesario para que la VM alcance un esta do optimizado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Advertencia:**
>
> La instalación o actualización de XenServer VM Tools para Windows puede provocar que cambien el nombre descriptivo y el identificador de algunos adaptadores de red. Es posible que cualquier software que esté configurado para usar un adaptador en particular deba reconfigurarse después de la instalación o actualización de XenServer VM Tools para Windows.

Instalación silenciosa

Para instalar XenServer VM Tools para Windows de forma silenciosa e impedir que el sistema se reinicie, ejecute uno de los siguientes comandos:

```
Msiexec.exe /package managementagentx64.msi /quiet /norestart
<!--NeedCopy-->
```

O bien

```
Setup.exe /quiet /norestart
<!--NeedCopy-->
```

Se puede obtener una instalación no interactiva, pero no silenciosa ejecutando:

```
Msiexec.exe managementagentx64.msi /passive
<!--NeedCopy-->
```

O bien

```
Setup.exe /passive
<!--NeedCopy-->
```

> **Notas:**
>
> - El parámetro `/quiet` solo se aplica a los cuadros de diálogo de instalación, pero no a la instalación del controlador del dispositivo. Cuando se especifica el parámetro `/quiet`, la instalación del controlador del dispositivo solicita permiso para reiniciarse si es necesario.
>   - Cuando `/quiet /norestart` se especifica, el sistema no se reinicia una vez que se completa la instalación de las herramientas. Este comportamiento es independiente de lo que el usuario especifique en el cuadro de diálogo de reinicio.
>   - Cuando se especifica `/quiet /forcerestart`, el proceso de actualización o instalación puede provocar varios reinicios. Este comportamiento es independiente de lo que el usuario especifique en el cuadro de diálogo de reinicio.
>   - Cuando la instalación del controlador del dispositivo solicita permiso para reiniciar, la instalación de herramientas con el parámetro `quiet` especificado aún puede estar en curso. Use el Administrador de tareas para confirmar si el instalador sigue ejecután-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> dose.

Para personalizar la configuración de la instalación, utilice los siguientes parámetros con los comandos de instalación silenciosa:

Parámetro	Valores permitidos	Valor predeterminado	Descripción
ALLOWAUTOUPDATE	SÍ o NO	SÍ	Permitir las actualizaciones automáticas del agente de administración
ALLOWDRIVERINSTALL	SÍ o NO	SÍ	Instale los controladores de E/S ahora
ALLOWDRIVERUPDATE	SÍ o NO	NO	Permitir que las actualizaciones automáticas del agente de administración instalen controladores actualizados
IDENTIFICAR ACTUALIZACIÓN AUTOMÁTICA	SÍ o NO	SÍ	Envíenos información de uso anónima

Por ejemplo, para realizar una instalación silenciosa de las herramientas que no permita futuras actualizaciones automáticas del agente de administración y no envíe información anónima a Cloud Software Group, Inc., ejecute uno de los siguientes comandos:

```
1 Msiexec.exe /package managementagentx64.msi ALLOWAUTOUPDATE=NO
     IDENTIFYAUTOUPDATE=NO /quiet /norestart
2 <!--NeedCopy-->
```

En el caso de las instalaciones interactivas, silenciosas y pasivas, tras el siguiente reinicio del sistema, es posible que se produzcan varios reinicios automáticos antes de que las herramientas de máquina virtual de XenServer para Windows estén completamente instaladas. Este comportamiento también es el caso de las instalaciones con el indicador `/norestart` especificado. Sin embargo, para las instalaciones en las que se proporciona el indicador `/norestart`, el reinicio inicial puede iniciarse manualmente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Actualizar XenServer VM Tools

Asegúrese de que las herramientas de máquinas virtuales de XenServer para Windows se actualicen periódicamente a la última versión, tanto en las máquinas virtuales como en las plantillas que utilice para crear las máquinas virtuales. Le recomendamos que haga una instantánea de la máquina virtual antes de actualizar XenServer VM Tools. Para obtener más información sobre la versión más reciente de las herramientas, consulte Novedades.

> **Importante:**
>
> Asegúrese de que todos los reinicios de VM solicitados se completen como parte de la actualización. Es posible que se requieran varios reinicios. Si no se completan todos los reinicios solicitados, es posible que la máquina virtual muestre un comportamiento inesperado.

XenServer proporciona mecanismos de actualización automática para cada uno de sus componentes:

- El agente de administración puede actualizarse automáticamente
- Los controladores de E/S se pueden actualizar mediante el agente de administración o mediante Windows Update.

Como alternativa, puede actualizar uno o ambos componentes manualmente.

El método de actualización que se elija para cada componente de las herramientas puede depender del entorno.

Parámetros de actualización recomendados

En la mayoría de los casos de uso, recomendamos usar los siguientes parámetros para actualizar los diferentes componentes de XenServer VM Tools para Windows:

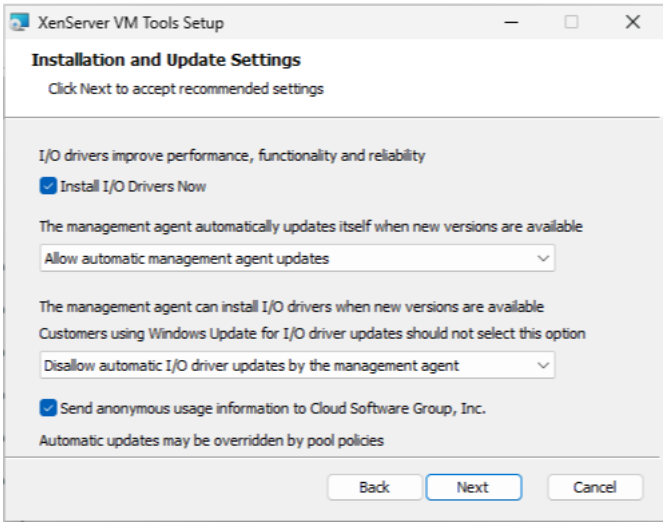
1. Habilite las actualizaciones del agente de administración.
2. Impida que el agente de administración actualice los controladores de E/S.
3. Establezca el valor de la siguiente clave de registro en un valor REG_DWORD de '3': `HLKM\System\CurrentControlSet\services\xenbus_monitor\Parameters\Autoreboot`.

   Para obtener más información, consulte ### Reinicios automáticos.
4. Configure los controladores de E/S para que se actualicen mediante Windows Update.

Durante la instalación:

Las dos primeras configuraciones son las predeterminadas al ejecutar el instalador:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Parámetros de los destinos de Citrix Provisioning o de las máquinas que se restablecen al arrancar

Si tiene la intención de usar su máquina virtual de Windows como destino de Citrix Provisioning o con el indicador de restablecimiento al arrancar establecido, no puede usar ninguno de los mecanismos de actualización automática. Le recomendamos que establezca la siguiente configuración en la plantilla maestra que utiliza para crear estas máquinas virtuales:

1. Durante la creación de la máquina virtual, asegúrese de que el indicador `has-vendor-device` esté establecido en **`false`**.

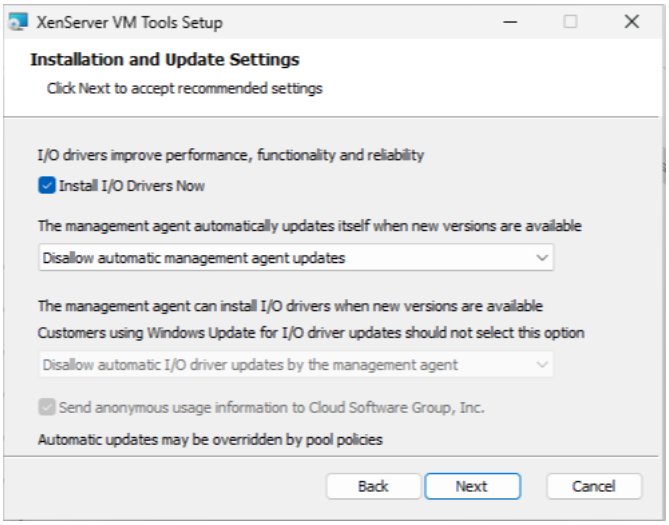
   Para obtener más información, consulte Crear una máquina virtual Windows mediante la CLI.

2. Inhabilite las actualizaciones del agente de administración.

Durante la instalación:

Especifique esta configuración al instalar por primera vez XenServer VM Tools:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Configuración para actualizaciones automáticas únicamente por parte del agente de administración

Puede configurar el agente de administración para que se actualice tanto a sí mismo como a los controladores de E/S. Si usa esta configuración, impida que las máquinas virtuales actualicen los controladores de E/S a través de Windows Update. Si ambos mecanismos intentan actualizar los controladores de E/S, puede provocar actualizaciones innecesarias.

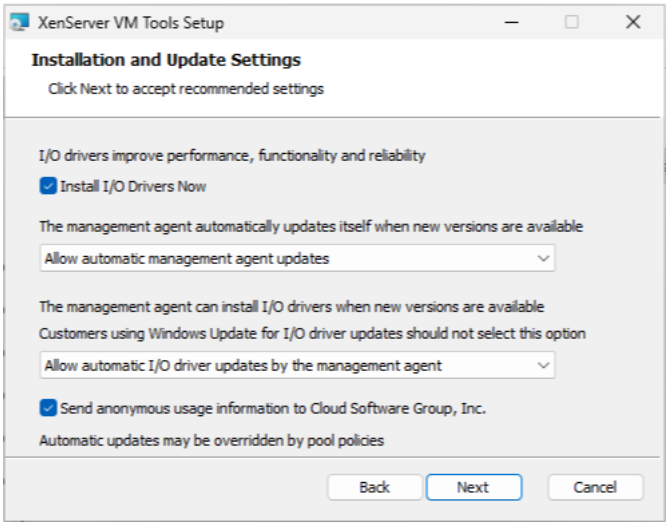
Elija este enfoque si su organización requiere que revise las actualizaciones antes de aplicarlas a las máquinas virtuales Windows. Si este es el caso, también debe redirigir el agente de administración para que obtenga sus actualizaciones de un servidor interno.

1. Inhabilite la actualización de los controladores de E/S a través de Windows Update.
2. Configure el agente de administración para actualizar los controladores de E/S.
3. (Opcional) Redirija las actualizaciones del agente de administración.

Durante la instalación:

Especifique esta configuración al instalar por primera vez XenServer VM Tools:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Actualizar el agente de administración

XenServer le permite actualizar el agente de administración automáticamente en las máquinas virtuales Windows nuevas y existentes. De forma predeterminada, XenServer permite la actualización automática del agente de administración. Sin embargo, no permite que el agente de administración actualice los controladores de E/S automáticamente. Puede personalizar la configuración de actualización del agente de administración durante la instalación de XenServer VM Tools para Windows. La actualización automática del agente de administración se produce sin problemas y no reinicia la VM. En situaciones en las que se requiere reiniciar una VM, aparece un mensaje en la ficha Consola de la VM que notifica a los usuarios sobre la acción requerida.

Puede obtener las actualizaciones del agente de administración automáticamente, siempre que la máquina virtual de Windows tenga acceso a Internet.

Administrar actualizaciones automáticas mediante la CLI XenServer le permite usar la línea de comandos para administrar la actualización automática de los controladores de E/S y del agente de administración. Puede ejecutar `msiexec.exe` con los argumentos enumerados en la siguiente tabla para especificar si los controladores de E/S y el agente de administración se actualizan automáticamente. Para obtener información sobre cómo instalar XenServer VM Tools para Windows mediante el uso `msiexec.exe`, consulte Instalación silenciosa.

> **Nota:**
>
> Para las máquinas virtuales administradas mediante PVS o MCS, las actualizaciones automatizadas se desactivan automáticamente cuando el VDA de Citrix Virtual Desktops está presente e informa de que la máquina no es persistente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Argumento	Valores	Descripción
ALLOWAUTOUPDATE	SÍ/NO	Permitir/no permitir la actualización automática del agente de administración
ALLOWDRIVERINSTALL	SÍ/NO	Permitir o impedir que el instalador de XenServer VM Tools para Windows instale controladores de E/S
ALLOWDRIVERUPDATE	SÍ/NO	Permitir/no permitir que el agente de administración actualice los controladores de E/S automáticamente
IDENTIFICAR ACTUALIZACIÓN AUTOMÁTICA	SÍ/NO	Permitir o no permitir que el mecanismo de actualización automática nos envíe información de uso anónima

Por ejemplo:

```
setup.exe  /passive /forcerestart ALLOWAUTOUPDATE=YES
    ALLOWDRIVERINSTALL=NO \
      ALLOWDRIVERUPDATE=NO IDENTIFYAUTOUPDATE=YES
<!--NeedCopy-->
```

Habilitar las actualizaciones del agente de administración Para habilitar la actualización automática del agente de administración por máquina virtual:

1. En la máquina virtual, abra un símbolo del sistema como administrador.
2. Ejecute este comando:

   ```
   reg.exe ADD HKLM\SOFTWARE\XenServer\XenTools\AutoUpdate /t
       REG_DWORD /v DisableAutoUpdate /d 0
   <!--NeedCopy-->
   ```

3. Asegúrese de que su grupo permita las actualizaciones del agente de administración. En la consola host, ejecute el siguiente comando:

   ```
   xe pool-param-set uuid=pooluuid guest-agent-config:
       auto_update_enabled=true
   <!--NeedCopy-->
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Inhabilitar las actualizaciones del agente de administración Para inhabilitar la actualización automática del agente de administración por VM:

1. En la máquina virtual, abra un símbolo del sistema como administrador.
2. Ejecute este comando:

```
reg.exe ADD HKLM\SOFTWARE\XenServer\XenTools\AutoUpdate /t
   REG_DWORD /v DisableAutoUpdate /d 1
<!--NeedCopy-->
```

Para inhabilitar la actualización automática del agente de administración por grupo, ejecute el siguiente comando en la consola del host:

```
xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_enabled=
   false
<!--NeedCopy-->
```

Redirigir las actualizaciones del agente de administración XenServer permite a los clientes redirigir las actualizaciones del agente de administración a un servidor web interno antes de que se instalen. Esta redirección permite a los clientes revisar las actualizaciones antes de que se instalen automáticamente en la VM.

El agente de administración utiliza un archivo de actualizaciones para obtener información sobre las actualizaciones disponibles. El nombre de este archivo de actualizaciones depende de la versión del agente de administración que utilice:

- Para Management Agent 9.2.1.35 y versiones posteriores, utilice https://pvupdates.vmd.citrix.com/autoupdate.v1.json.
- Para Management Agent 9.0.0.0 a 9.2.0.27 https://pvupdates.vmd.citrix.com/updates.v9.json.

Complete los siguientes pasos para redirigir las actualizaciones del agente de administración:

1. Descargue el archivo de actualizaciones.
2. Descargue los archivos MSI de Management Agent referenciados en el archivo de actualizaciones.
3. Cargue los archivos MSI en un servidor web interno al que puedan acceder las máquinas virtuales.
4. Actualice el archivo de actualizaciones para que apunte a los archivos MSI en el servidor web interno.
5. Cargue el archivo de actualizaciones en el servidor web.

Las actualizaciones automáticas también se pueden redirigir por VM o por grupo. Para redirigir las actualizaciones por VM:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. En la máquina virtual, abra un símbolo del sistema como administrador.
2. Ejecute el comando

```
reg.exe ADD HKLM\SOFTWARE\XenServer\XenTools /t REG_SZ /v
   update_url /d \
    url of the update file on the web server
<!--NeedCopy-->
```

Para redirigir la actualización automática del agente de administración por grupo, ejecute el siguiente comando:

```
xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_url=url
   of the update file on the web server
<!--NeedCopy-->
```

Actualizar los controladores de E/S

Puede actualizar los controladores de E/S mediante Windows Update o mediante el agente de administración. También puede desactivar las actualizaciones automáticas y administrar las actualizaciones de los controladores de E/S de forma manual.

Cada uno de los controladores de E/S (xennet, xenvif, xenvbd, xeniface y xenbus) tiene su propia versión. Para obtener información sobre las versiones más recientes, consulte Novedades.

Configurar los controladores de E/S para que se actualicen mediante Windows Update Puede obtener actualizaciones de controladores de E/S automáticamente desde Microsoft Windows Update, siempre que:

- Windows Update está habilitado en la VM
- La VM tiene acceso a Internet o puede conectarse a un servidor proxy WSUS
- No está ejecutando la versión Core de Windows Server. Windows Server Core no admite el uso de Windows Update para instalar o actualizar los controladores de E/S.

La sección **Estado de virtualización** en la ficha **General** de una VM en XenCenter especifica si la VM puede recibir actualizaciones de Windows Update. El mecanismo para recibir actualizaciones de controladores de E/S de Windows Update está activado de forma predeterminada. Si no quiere recibir actualizaciones de controladores de E/S de Windows Update, inhabilite Windows Update en su máquina virtual o especifique una directiva de grupo.

Inhabilitar la actualización de los controladores de E/S a través de Windows Update La sección **Estado de virtualización** en la ficha **General** de una VM en XenCenter especifica si la VM puede recibir

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

actualizaciones de Windows Update. El mecanismo para recibir actualizaciones de controladores de E/S de Windows Update está activado de forma predeterminada.

En el caso de las máquinas virtuales Windows que ya existen, si no quiere recibir actualizaciones de controladores de E/S de Windows Update, especifique una directiva de grupo.

En el caso de las nuevas máquinas virtuales Windows, puede establecer un indicador en la máquina virtual durante la creación de la misma para evitar que Windows Update actualice los controladores de E/S. Para obtener más información, consulte Configuración de los destinos de Citrix Provisioning o de las máquinas que se restablecen al arrancar y Crear una máquina virtual Windows mediante la CLI.

Configurar el agente de administración para actualizar los controladores de E/S Durante la instalación de XenServer VM Tools para Windows, puede especificar que el agente de administración actualice los controladores de E/S automáticamente. Si prefiere actualizar esta configuración después de completar el proceso de instalación de XenServer VM Tools para Windows, lleve a cabo los siguientes pasos:

1. En la máquina virtual, abra un símbolo del sistema como administrador.
2. Ejecute este comando:

```
reg.exe ADD HKLM\SOFTWARE\XenServer\XenTools\AutoUpdate /t REG_SZ
   /v \
    InstallDrivers /d YES
<!--NeedCopy-->
```

Impedir que el agente de administración actualice los controladores de E/S Para evitar que el agente de administración actualice los controladores de E/S, lleve a cabo los siguientes pasos:

1. En la máquina virtual, abra un símbolo del sistema como administrador.
2. Ejecute este comando:

```
reg.exe ADD HKLM\SOFTWARE\XenServer\XenTools\AutoUpdate /t REG_SZ
   /v \
    InstallDrivers /d NO
<!--NeedCopy-->
```

Reinicios automáticos

Asegúrese de que todos los reinicios de VM solicitados se completen como parte de la actualización. Es posible que se requieran varios reinicios. Si no se completan todos los reinicios solicitados, es posible que veas un comportamiento inesperado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puede establecer una clave de registro que especifique el número máximo de reinicios automáticos que se realizan al instalar los controladores a través del Administrador de dispositivos o Windows Update. Tras instalar la versión 9.1.1.8 o posterior del controlador xenbus, XenServer VM Tools para Windows sigue las instrucciones que proporciona esta clave de registro.

Para utilizar esta función, le recomendamos que configure la siguiente clave de registro lo antes posible: `HLKM\System\CurrentControlSet\services\xenbus_monitor\Parameters\Autoreboot`. El valor de la clave de registro debe ser un número entero positivo. Le recomendamos que establezca el número de reinicios de la clave de registro en 3.

Cuando se establece esta clave de registro, las herramientas de máquina virtual de XenServer para Windows realizan tantos reinicios como sean necesarios para completar las actualizaciones o el número de reinicios especificado por la clave de registro, el valor que sea inferior.

Antes de cada reinicio, Windows puede mostrar una alerta durante 60 segundos que avisa del próximo reinicio. Puede descartar la alerta, pero esta acción no cancela el reinicio. Debido a esta demora entre los reinicios, espere unos minutos después del reinicio inicial para que se complete el ciclo de reinicio.

> **Notas:**
>
> Esta configuración es necesaria para los servidores headless con direcciones IP estáticas.
>
> Esta función de reinicio automático solo se aplica a las actualizaciones de los controladores de E/S de Windows a través del Administrador de dispositivos o Windows Update. Si utiliza el instalador del agente de administración para implementar los controladores, el instalador ignora esta clave de registro y administra los reinicios de la máquina virtual de acuerdo con su propia configuración.

Otras configuraciones y consultas

Encuentre la versión del controlador de E/S

Para averiguar la versión de los controladores de E/S instalados en la VM:

1. Vaya a `C:\Windows\System32\drivers`.
2. Busque al conductor en la lista.
3. Haga clic con el botón secundario en el controlador y seleccione **Propiedades** y luego **Detalles**.

   El campo **Versión del archivo** muestra la versión del controlador instalado en la máquina virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Busque la versión de Management Agent

Para averiguar la versión del agente de administración instalado en la máquina virtual:

1. Vaya a `C:\Program Files\XenServer\XenTools`.
2. Haga clic en `XenGuestAgent` con el botón secundario en la lista y haga clic en **Propiedades** y, luego, en **Detalles**.

   El campo **Versión del archivo** muestra la versión del agente de administración instalado en la máquina virtual.

Configurar la información de uso anónima

Durante la instalación de XenServer VM Tools para Windows, puede especificar si desea enviar información de uso anónima a Cloud Software Group, Inc. Si prefiere actualizar esta configuración después de completar el proceso de instalación de XenServer VM Tools para Windows, lleve a cabo los siguientes pasos:

1. En la máquina virtual, abra un símbolo del sistema como administrador.
2. Ejecute este comando:

```
reg.exe ADD HKLM\SOFTWARE\XenServer\XenTools\AutoUpdate REG_SZ /v
    \
    IDENTIFYAUTOUPDATE /d YES/NO
<!--NeedCopy-->
```

Desinstalar XenServer VM Tools

No recomendamos eliminar las herramientas de máquina virtual de XenServer de las máquinas virtuales de Windows. Estas herramientas son necesarias para que las máquinas virtuales de Windows sean totalmente compatibles. Quitarlos puede provocar un comportamiento inesperado. Desinstale manualmente las herramientas de VM de XenServer solo como último recurso.

Desinstalación estándar

Para realizar una desinstalación estándar de XenServer VM Tools, puede usar la función **Agregar o quitar programas** de Windows:

1. Cree una instantánea de la máquina virtual antes de empezar.
2. En la máquina virtual de Windows, vaya a **Agregar o quitar programas**.
3. Seleccione **XenServer VM Tools** y haga clic en **Desinstalar**.
4. Reinicie la máquina virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El `uninstall.exe` comando

Al desinstalar XenServer VM Tools mediante la función **Agregar o quitar programas de Windows**, se llama al archivo <`tools-install-directory`>\`uninstall.exe` para realizar las acciones de desinstalación. En su lugar, puede optar por llamar a este comando desde una terminal de PowerShell o desde una línea de comandos con privilegios de administrador.

1. Cree una instantánea de la máquina virtual antes de empezar.
2. Como administrador, abra una línea de comandos o un terminal de PowerShell.
3. Ejecute el comando <`tools-install-directory`>\`uninstall.exe`.
4. Reinicie la máquina virtual.

Opciones de comandos El `uninstall.exe` comando acepta los siguientes parámetros:

- `help` - Muestra la información de uso del comando.
- `log` - Genera un archivo de registro que indica lo que ha hecho el comando.
- `verbose` - Imprime en la consola lo que ha hecho el comando.
- `disable` - Desactiva los controladores instalados por el instalador MSI.
- `force-disable` - Desactiva a los conductores en todas las situaciones.
- `hidden` - Elimina los dispositivos ocultos. Estos dispositivos no se utilizan y han sido reemplazados, pero es posible que hayan dejado entradas de registro obsoletas.
- `cleanup` - Elimina los desinstaladores antiguos de **Agregar o quitar programas**. Estos desinstaladores pueden incluir entradas duplicadas de versiones anteriores de las herramientas.
- `purge` - (9.3.1 y versiones posteriores) Restablece la máquina virtual a un estado limpio como estaba antes de instalar cualquier parte de las herramientas de máquina virtual de XenServer. Para obtener más información, consulte Desinstalación completa de todos los componentes de XenServer VM Tools.
- `install` - (9.3.1 y versiones posteriores) Instala el conjunto actual de controladores de E/S y solicita el reinicio de la máquina virtual cuando sea necesario.
- `reboot`- Reinicia la máquina virtual después de que se hayan completado todas las demás operaciones de comando.

Desinstalación completa de todos los componentes de XenServer VM Tools

La versión más reciente de XenServer VM Tools para Windows (9.3.1 y versiones posteriores) incluye el comando. `uninstall.exe purge` La opción `purge` de la aplicación `uninstall.exe` restablece una máquina virtual al estado anterior a la instalación de cualquiera de los controladores de E/S. Si tiene problemas al actualizar sus herramientas a una versión más reciente o necesita un estado limpio para instalar un conjunto de herramientas posterior en su máquina virtual, utilice esta utilidad.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Cree una instantánea de la máquina virtual antes de empezar.
2. Como administrador, abra una línea de comandos o un terminal de PowerShell.
3. Ejecute el comando `<tools-install-directory>\uninstall.exe purge verbose`
4. Reinicie la máquina virtual.

Después de usar este comando, no necesita realizar ningún paso de limpieza manual como lo habría hecho con las versiones anteriores de XenServer VM Tools. Se han eliminado todos los cambios relacionados con las herramientas de máquina virtual de XenServer.

¿Qué elimina la `purge` opción? Si usa el comando `uninstall.exe purge`, todos los rastros de las herramientas de máquina virtual de XenServer se eliminan de la máquina virtual de Windows. La lista de acciones realizadas por este comando es la siguiente:

- Servicios:
  - Inhabilita todos los servicios de XenServer VM Tools, lo que impide que los controladores y servicios instalados se inicien al reiniciarse.
  - Detiene todos los servicios de XenServer VM Tools en ejecución.
- Controladores:
  - Desinstala los controladores de E/S de todos los nodos del dispositivo.
  - Desinstala los dispositivos ocultos. Esta acción es la misma que se realizó en la opción de línea de `hidden` comandos.
  - Desinstala los paquetes de controladores en caché, lo que los elimina del almacén de controladores. Como resultado, los controladores de E/S no se reinstalan automáticamente.
- Registro:
  - Elimina la información de registro obsoleta utilizada por las versiones no compatibles de los controladores.
  - Elimina las claves relacionadas con las herramientas de `HKLM\System\CurrentControlSet\Control\Class\...`
  - Elimina las claves relacionadas con las herramientas de `HKLM\System\CurrentControlSet\Services`.
  - Elimina las claves relacionadas con las herramientas de `HKLM\System\CurrentControlSet\Enum\...`
- Archivos:
  - Elimina cualquier archivo `C:\Windows\System32` de controlador de XenServer VM Tools de y. `C:\Windows\System32\drivers`
  - Elimina los archivos `INF` de XenServer VM Tools de `C:\Windows\INF`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Elimina de y los archivos obsoletos que hayan dejado las versiones no compatibles de las herramientas`C:\Program Files\Citrix\XenTools`C:\Program Files\XenServer\XenTools.

- Otros:

  - Elimina las entradas antiguas en **Agregar o quitar programas**. Esta acción es la misma que se realizó en la opción de línea de `cleanup` comandos.
  - Borra parte de la información de estado obsoleta del InstallAgent.
  - Se elimina `xenfilt.sys` de los filtros superiores. Este cambio `xenfilt.sys` impide que se cargue en ningún nodo del controlador.
  - Elimina las `unplug` claves, lo que hace que la máquina virtual vuelva a ser dispositivos emulados al reiniciarse.
  - Elimina StartOverride de StorNvme. Este cambio obliga a `stornvme.sys` a que se inicie durante el arranque y permite que los dispositivos de arranque NVMe (UEFI) emulados funcionen.

Novedades

La versión de XenServer VM Tools para Windows se actualiza de forma independiente de la versión de XenServer. Asegúrese de que las herramientas de máquinas virtuales de XenServer para Windows se actualicen periódicamente a la última versión, tanto en las máquinas virtuales como en las plantillas que utilice para crear las máquinas virtuales.

La versión más reciente de XenServer VM Tools para Windows está disponible en la página de descargas de XenServer.

Herramientas de máquina virtual de XenServer para Windows 9.3.2

Publicado el 27 de noviembre de 2023

Esta versión cambia el nombre de Citrix VM Tools a XenServer VM Tools.

Este conjunto de herramientas contiene las siguientes versiones de componentes:

- Instalador: 9.3.2
- Agente de administración: 9.2.2.435
- xenbus: 9.1.7.80
- Xeniface: 9.1.8.69
- xennet: 9.1.5.51
- xenvbd: 9.1.6.58
- xenvif: 9.1.10.83

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Mejoras en la versión 9.3.2 Esta versión también contiene las siguientes mejoras:

- Mejoras en el `uninstall.exe` comando.
- Cambios para permitir que algunas máquinas virtuales de Windows usen hasta 64 vCPU cuando su versión de XenServer y el sistema operativo Windows lo admitan.

Problemas resueltos en la versión 9.3.2 Esta versión incluye una solución para el siguiente problema:

- En ocasiones, al instalar XenServer VM Tools, un error no grave puede provocar un error en la instalación.

Versiones anteriores

9.3.1 Publicado el 25 de enero de 2023

Este conjunto de herramientas contiene las siguientes versiones de componentes:

- Instalador: 9.3.1
- Agente de administración: 9.2.1.35
- xenbus: 9.1.5.54
- xeniface: 9.1.5.42
- xennet: 9.1.3.34
- xenvbd: 9.1.4.37
- xenvif: 9.1.8.58

Esta versión incluye las siguientes mejoras:

- Mejoras en la utilidad `uninstall.exe`, incluido el parámetro `purge`. Para obtener más información, consulte Desinstalar XenServer VM Tools.
- Mejoras generales en el instalador de XenServer VM Tools.
- Mejoras generales en el manejo de cadenas de claves de registro.

Esta versión contiene correcciones para los siguientes problemas:

- A veces, cuando las herramientas de máquina virtual de XenServer se actualizan mediante Windows Update, se pierde la configuración de IP estática y la configuración de red cambia para usar DHCP.
- En las máquinas virtuales de Windows, las tablas de subvenciones pueden agotarse fácilmente. Cuando esto ocurre, las solicitudes de lectura y escritura pueden fallar o los VIF adicionales no se habilitan correctamente y no se inician.
- En raras ocasiones, al actualizar XenServer VM Tools para Windows, es posible que el agente de administración existente no se cierre e impida que la actualización se realice correctamente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- En una máquina virtual Windows, es posible que vea la versión anterior y la más reciente de las herramientas o el agente de administración en los programas instalados.

  - (ANTERIOR) Agente de administración de Windows de Citrix XenServer
  - (POSTERIOR) Citrix Hypervisor PV Tools.

  Tras actualizar a la versión más reciente de las herramientas, no aparece ninguno de estos nombres anteriores. Solo XenServer VM Tools aparece en los programas instalados.

9.3.0 Publicado el 26 de julio de 2022

Este conjunto de herramientas contiene las siguientes versiones de componentes:

- Instalador: 9.3.0
- Agente de administración: 9.2.0.27
- xenbus: 9.1.4.49
- xeniface: 9.1.4.34
- xennet: 9.1.3.34
- xenvbd: 9.1.3.33
- xenvif: 9.1.6.52

Esta versión incluye las siguientes mejoras:

- Mejoras generales en el instalador de XenServer VM Tools.

Esta versión contiene correcciones para los siguientes problemas:

- El software de seguridad impedía que los discos secundarios marcados como extraíbles quedaran expuestos al sistema operativo, como medida de prevención de la exfiltración de datos. Esta actualización permite marcar un VBD como no extraíble y exponerlo correctamente en el sistema operativo.
- En una VM Windows, a veces la dirección IP de una VIF de SR-IOV no está visible en XenCenter.

9.2.3 Publicado el 28 de abril de 2022

Este conjunto de herramientas contiene las siguientes versiones de componentes:

- Instalador: 9.2.3
- Agente de administración: 9.1.1.13
- xenbus: 9.1.3.30
- xeniface: 9.1.4.34
- xennet:

  - 9.1.1.8 (para Windows Server 2012 y Windows Server 2012 R2)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 9.1.2.23 (para todos los demás sistemas operativos Windows compatibles)

- xenvbd: 9.1.2.20
- xenvif: 9.1.5.48

Esta versión contiene correcciones para los siguientes problemas:

- En la versión 9.2.2 de XenServer VM Tools para Windows, las opciones de sincronización horaria no están disponibles.
- Una condición de carrera puede provocar que las máquinas virtuales de Windows muestren un error de pantalla azul tras la migración en vivo a la actualización acumulativa 1 de Citrix Hypervisor 8.2.
- Las máquinas virtuales de Windows que tienen instalada la versión 9.2.1 o 9.2.2 de XenServer VM Tools y que son destinos de PVS a veces pueden bloquearse con una pantalla negra. El mensaje "Guest Rx está estancado"aparece en los registros del núcleo dom0. Este problema ocurre con más frecuencia en los coordinadores del grupo que en otros miembros del grupo.
- En máquinas virtuales de Windows con más de 8 vCPU, es posible que Receive Side Scaling no funcione porque el controlador xenvif no puede configurar la tabla de indirecciones.

9.2.2 Publicado el 14 de enero de 2022

Este conjunto de herramientas contiene las siguientes versiones de componentes:

- Instalador: 9.2.2
- Agente de administración: 9.1.1.13
- xenbus: 9.1.3.30
- xeniface: 9.1.2.22
- xennet:
  - 9.1.1.8 (para Windows Server 2012 y Windows Server 2012 R2)
  - 9.1.2.23 (para todos los demás sistemas operativos Windows compatibles)
- xenvbd: 9.1.2.20
- xenvif: 9.1.3.31

Esta versión contiene correcciones para los siguientes problemas:

- Durante una actualización de las herramientas, el controlador xenbus puede solicitar un reinicio antes de que se complete la instalación del controlador. Aceptar el reinicio puede provocar un error de pantalla azul en la máquina virtual de Windows.
- Al comprimir la información de diagnóstico recopilada, la herramienta de diagnóstico xt-bugtool agota el tiempo de espera transcurridos 20 segundos. Este comportamiento puede provocar que el archivo zip de diagnóstico no se cree correctamente.
- El uso compartido del portapapeles de VNC no funciona.
- Las versiones anteriores de los controladores no se publicaron a través de Windows Update.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

9.2.1 Publicado el 24 de junio de 2021

Este conjunto de herramientas contiene las siguientes versiones de componentes:

- Instalador: 9.2.1
- Agente de administración: 9.1.0.10
- xenbus: 9.1.2.14
- xeniface: 9.1.1.11
- xennet: 9.1.1.8
- xenvbd: 9.1.1.8
- xenvif: 9.1.2.16

> **Nota:**
>
> Este conjunto de controladores no se proporcionó a través de Windows Update.

Esta versión contiene correcciones para los siguientes problemas:

- En algunos casos, no se puede cambiar el estado de Laptop/Slate de la máquina virtual.
- Después de reiniciar una máquina virtual, a veces puede empezar a enviar demasiados mensajes de registro al archivo daemon.log.
- Una condición de carrera en las dependencias de carga del controlador después de una actualización del sistema operativo puede impedir la actualización de XenServer VM Tools.
- Un error de almacenamiento puede provocar que las máquinas virtuales de Windows se bloqueen.
- A veces, la dirección IP de un VIF SR-IOV no está visible en XenCenter. Para solucionar el problema, reinicie el agente de administración desde VM Service Manager.
- Con una carga alta de red y sistema, y con pocos recursos, las máquinas virtuales pueden experimentar comprobaciones de errores tanto en los controladores de Citrix como en los de terceros, normalmente con el código IRQL_NOT_LESS_OR_EQUAL. Esta corrección mejora el almacenamiento en búfer de la red para evitar estas comprobaciones de errores.
- La actualización de los controladores de E/S de Windows puede provocar que las máquinas virtuales UEFI no se inicien y den como resultado "0xC000000E. El dispositivo necesario no está conectado o no se puede acceder al mismo".
- Al instalar XenServer VM Tools después de desinstalar una versión anterior de XenServer VM Tools, puede producirse un problema que devuelva el siguiente mensaje de error: "Este dispositivo no se puede iniciar (código 10) (la operación falló) La operación solicitada no se realizó correctamente".

---

layout: doc
description: Create a Linux VM from a template for the operating system you want to run on the VM. You can create the VM from either XenCenter or the CLI.—

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Máquinas virtuales Linux

Cuando quiera crear una máquina virtual de Linux, cree la máquina virtual con una plantilla para el sistema operativo que quiere ejecutar en la máquina virtual. Puede usar una plantilla que XenServer proporcione para su sistema operativo o una que haya creado anteriormente. Puede crear la VM desde XenCenter o desde la CLI. Esta sección se centra en el uso de la CLI.

> **Nota:**
>
> Para crear una máquina virtual de una actualización secundaria más reciente de una versión de RHEL que XenServer admite para su instalación, complete los siguientes pasos:
>
> - Instalar desde los medios compatibles más recientes
> - Use `yum update` para actualizar la VM
>
> Este proceso también se aplica a los derivados de RHEL, como CentOS y Oracle Linux.

Se recomienda instalar XenServer VM Tools para Linux inmediatamente después de instalar el sistema operativo. Para obtener más información, consulte Instalar XenServer VM Tools para Linux.

La descripción general para crear una VM Linux es la siguiente:

1. Cree la máquina virtual para el sistema operativo de destino mediante XenCenter o la CLI.
2. Instale el sistema operativo mediante los medios de instalación del proveedor.
3. Instale XenServer VM Tools para Linux (recomendado).
4. Configure la hora y la zona horaria correctas en la VM y la VNC como lo haría en un entorno no virtual normal.

XenServer admite la instalación de muchas distribuciones de Linux como máquinas virtuales.

> **Advertencia:**
>
> La plantilla **Otros medios de instalación** es para usuarios avanzados que desean intentar instalar máquinas virtuales que ejecuten sistemas operativos no compatibles. XenServer se ha probado ejecutando solo las distribuciones compatibles y las versiones específicas incluidas en las plantillas estándar suministradas. *No* se admiten las máquinas virtuales instaladas con la plantilla **Otros medios de instalación**.

Para obtener información sobre distribuciones de Linux específicas, consulte Notas de instalación para distribuciones de Linux.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Distribuciones compatibles de Linux

Para obtener una lista de las distribuciones de Linux compatibles, consulte Compatibilidad con sistemas operativos invitados.

No se admiten otras distribuciones de Linux. Sin embargo, las distribuciones que utilizan el mismo mecanismo de instalación que Red Hat Enterprise Linux (por ejemplo, Fedora Core) podrían instalarse correctamente mediante la misma plantilla.

Cree una VM Linux

Esta sección incluye procedimientos para crear una máquina virtual Linux mediante la instalación del sistema operativo desde un CD/DVD físico o desde una ISO accesible a la red.

Cree una máquina virtual de Linux mediante la CLI xe

En esta sección se muestra el procedimiento de la CLI para crear una máquina virtual Linux mediante la instalación del sistema operativo desde un CD/DVD físico o desde una ISO accesible en red.

1. Cree una VM a partir de la plantilla apropiada. Se devuelve el UUID de la VM:

```
xe vm-install template=template-name new-name-label=vm-name
<!--NeedCopy-->
```

2. (Opcional) Cambie el modo de arranque de la máquina virtual.

```
xe vm-param-set uuid=<uuid> HVM-boot-params:firmware=<mode>
xe vm-param-set uuid=<UUID> platform:device-model=qemu-upstream-
   uefi
xe vm-param-set uuid=<uuid> platform:secureboot=<option>
<!--NeedCopy-->
```

   El valor de `mode` puede ser `BIOS` o `uefi` y el valor predeterminado es `uefi` si esa opción es compatible con el sistema operativo de la máquina virtual. De lo contrario, el modo se establece de forma predeterminada `BIOS`. El valor de `option` se puede establecer en **`true`** o **`false`**. Si no especifica la opción Arranque seguro, el valor predeterminado es. `auto`

   Para obtener más información, consulte Arranque UEFI de invitado y Arranque seguro.

3. Agregue un CD-ROM virtual a la nueva VM:

   - Si realiza la instalación desde un CD o DVD, obtenga el nombre de la unidad de CD física del host de XenServer:

```
xe cd-list
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El resultado de este comando le da algo como SCSI 0:0:0:0 para el campo `name-label`.

Use este parámetro value como parámetro `cd-name`:

```
xe vm-cd-add vm=vm_name cd-name="host_cd_drive_name_label"
   device=3
<!--NeedCopy-->
```

- Si va a realizar la instalación desde una ISO accesible en red, utilice el nombre de la ISO de la etiqueta de biblioteca ISO como valor para el parámetro `cd-name`:

```
xe vm-cd-add vm=vm_name cd-name="iso_name.iso" device=3
<!--NeedCopy-->
```

4. Inserte el CD de instalación del sistema operativo en la unidad de CD del host XenServer.
5. Abra una consola en la VM con XenCenter o una terminal SSH y siga los pasos para realizar la instalación del sistema operativo.
6. Inicie la VM. Se inicia directamente en el instalador del sistema operativo:

```
xe vm-start uuid=UUID
<!--NeedCopy-->
```

7. Instale las utilidades para invitados y configure la pantalla gráfica. Para obtener más información, consulte Instalación de XenServer VM Tools para Linux.

Cree una máquina virtual de Linux mediante XenCenter

1. En la barra de herramientas de XenCenter, haga clic en el botón **Nueva máquina virtual** para abrir el asistente para nueva máquina virtual.

   El asistente para nueva VM le permite configurar la nueva VM, ajustando varios parámetros para la CPU, el almacenamiento y los recursos de red.

2. Seleccione una plantilla de VM y haga clic en **Siguiente**.

   Cada plantilla contiene la información de configuración necesaria para crear una VM con un sistema operativo (SO) invitado específico y con un almacenamiento óptimo. Esta lista refleja las plantillas que XenServer admite actualmente.

   > **Nota:**
   >
   > Si el sistema operativo que va a instalar en su máquina virtual solo es compatible con el hardware original, marque la casilla **Copiar cadenas de BIOS del host a la máquina virtual**. Por ejemplo, puede usar esta opción para un CD de instalación de SO que se empaquetó con un equipo específico.
   >
   > Después de iniciar una VM por primera vez, no puede cambiar sus cadenas de BIOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Asegúrese de que las cadenas del BIOS sean correctas antes de iniciar la VM por primera vez.

Para copiar cadenas de BIOS mediante la CLI, consulte Instalación de máquinas virtuales desde un soporte del kit de opciones del distribuidor (bloqueado por BIOS).

Los usuarios avanzados pueden configurar cadenas de BIOS definidas por el usuario. Para obtener más información, consulte Cadenas de BIOS definidas por el usuario.

3. Introduzca un nombre y una descripción opcional para la nueva VM.
4. Elija el origen del medio del sistema operativo que quiere instalar en la nueva máquina virtual.

   La instalación desde un CD/DVD es la opción más sencilla para empezar.

   a) Elija la opción de fuente de instalación predeterminada (unidad de DVD)
   b) Inserte el disco en la unidad de DVD del host XenServer

   XenServer también le permite extraer los medios de instalación del sistema operativo de una variedad de fuentes, incluida una biblioteca ISO preexistente.

   Para adjuntar una biblioteca ISO preexistente, haga clic en **Nueva biblioteca ISO** e indique la ubicación y el tipo de la biblioteca ISO. A continuación, puede elegir el medio ISO del sistema operativo específico de la lista.
5. En la ficha **Medios de instalación**, puede elegir un modo de arranque para la máquina virtual. De forma predeterminada, XenCenter selecciona el modo de arranque más seguro disponible para la versión del sistema operativo de la máquina virtual.

   > **Notas:**
   >
   > - Las opciones de **arranqueUEFI y arranque seguro** UEFI aparecen atenuadas si la plantilla de VM que ha elegido no admite el arranque UEFI.
   > - No puede cambiar el modo de arranque después de arrancar la VM por primera vez.
   >
   > Para obtener más información, consulte Arranque UEFI invitado y Arranque seguro.
6. Seleccione un servidor doméstico para la VM.

   Un servidor doméstico es el host que proporciona los recursos para una máquina virtual en un grupo. Al designar un servidor doméstico para una máquina virtual, XenServer intenta iniciar la máquina virtual en ese host. Si esta acción no es posible, se selecciona automáticamente un anfitrión alternativo dentro del mismo grupo. Para elegir un servidor doméstico, haga clic en **Colocar la máquina virtual en este servidor** y seleccione un host de la lista.

   > **Notas:**
   >
   > - En los grupos habilitados para WLB, el servidor doméstico designado no se usa para

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> iniciar, reiniciar, reanudar o migrar la VM. En cambio, Workload Balancing designa el mejor host para la máquina virtual mediante el análisis de las métricas del grupo de recursos de XenServer y la recomendación de optimizaciones.
> - Si una VM tiene una o más GPU virtuales asignadas, la nominación de servidor doméstico no se aplica. En cambio, la nominación del anfitrión se basa en la directiva de ubicación de la GPU virtual establecida por el usuario.
> - Durante la actualización progresiva del pool, no se tiene en cuenta el servidor doméstico al migrar la máquina virtual. En su lugar, la máquina virtual se migra de nuevo al host en el que estaba antes de la actualización.
>
> Si no desea designar un servidor doméstico, haga clic en **No asignar un servidor doméstico a esta máquina virtual**. La máquina virtual se inicia en cualquier host con los recursos necesarios.

Haga clic en **Next** para continuar.

7. Asigne recursos de memoria y procesador para la VM. Haga clic en **Next** para continuar.
8. Asigna una GPU virtual.

   Si se admite vGPU, el asistente para nuevas máquinas virtuales le pide que asigne una GPU dedicada o una o más GPU virtuales a la máquina virtual. Esta opción permite que la VM utilice la potencia de procesamiento de la GPU. Con esta función, tiene un mejor soporte para aplicaciones de gráficos profesionales en 3D de alta gama, como CAD/CAM, GIS y aplicaciones de imágenes médicas.
9. Asigne y configure el almacenamiento para la nueva VM.

   Haga clic en **Siguiente** para seleccionar la asignación predeterminada (24 GB) y la configuración, o puede que quiera realizar la siguiente configuración adicional:

   - Cambie el nombre, la descripción o el tamaño del disco virtual haciendo clic en **Modificar**.
   - Para agregar un disco virtual nuevo, seleccione **Agregar**.
10. Configure las redes en la nueva VM.

    Haga clic en **Siguiente** para seleccionar la NIC y las configuraciones predeterminadas, incluida una dirección MAC única creada automáticamente para cada NIC. Como alternativa, es posible que quiera realizar la siguiente configuración adicional:

    - Cambie la red física, la dirección MAC o la prioridad de calidad de servicio (QoS) del disco virtual haciendo clic en **Modificar**.
    - Agregue una nueva NIC virtual seleccionando **Agregar**.
11. Revise la configuración y, a continuación, haga clic en **Crear ahora** para crear la VM y volver a la ficha **Buscar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aparece un icono para la nueva VM debajo del host en el panel **Recursos**.

En el panel **Recursos**, seleccione la VM y, a continuación, haga clic en la ficha **Consola** para ver la consola de VM.

12. Siga las pantallas de instalación del sistema operativo y haga sus selecciones.
13. Una vez completada la instalación del sistema operativo y reiniciada la máquina virtual, instale XenServer VM Tools para Linux.

Crear una VM Linux mediante el arranque PXE

Puede usar el arranque PXE para instalar el sistema operativo de su VM Linux. Este enfoque puede resultar útil cuando tiene que crear muchas máquinas virtuales Linux.

Para instalar mediante arranque PXE, configure los siguientes requisitos previos en la red donde se encuentran las VM de Linux:

- Servidor DHCP configurado para dirigir cualquier solicitud de instalación de arranque PXE al servidor TFTP
- Servidor TFTP que aloja los archivos de instalación para el sistema operativo Linux

Al crear la máquina virtual Linux, ejecute los siguientes comandos:

1. Cree una VM a partir de la plantilla apropiada. Se devuelve el UUID de la VM:

```
xe vm-install template=template-name new-name-label=vm-name
<!--NeedCopy-->
```

2. Configure el orden de arranque para que arranque desde el disco y, a continuación, desde la red:

```
xe vm-param-set uuid=<UUID> HVM-boot-params:order=cn
<!--NeedCopy-->
```

3. Inicie la VM para iniciar la instalación de arranque PXE:

```
xe vm-start uuid=<UUID>
<!--NeedCopy-->
```

4. Instale las utilidades para invitados y configure la pantalla gráfica. Para obtener más información, consulte Instalación de XenServer VM Tools para Linux.

Para obtener más información sobre el uso del arranque PXE para instalar sistemas operativos Linux, consulte la documentación del sistema operativo:

- Debian: Instalar Debian mediante arranque en red
- RedHat: Iniciar una instalación Kickstart automáticamente con PXE

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- CentOS: configuración de PXE
- SLES: Preparación del entorno de arranque de red
- Ubuntu: Arranque desde la red del instalador del servidor en amd64

Instalación de XenServer VM Tools para Linux

Si bien todas las distribuciones de Linux compatibles están paravirtualizadas de forma nativa (y no necesitan controladores especiales para obtener un rendimiento completo), XenServer VM Tools para Linux proporciona un agente invitado. Este agente invitado proporciona información adicional sobre la máquina virtual al host. Instale el agente invitado en cada máquina virtual Linux para disfrutar de las siguientes funciones:

- Vea los datos de rendimiento de las máquinas virtuales en XenCenter.

  Por ejemplo, los siguientes valores de rendimiento de la memoria solo están visibles en XenCenter cuando están instaladas las herramientas de máquina virtual de XenServer: "Memoria usada", "Discos", "Red"y "Dirección".
- En XenCenter, consulte la información del sistema operativo invitado Linux.
- En la pestaña **Redes** de XenCenter, consulte la dirección IP de la máquina virtual.
- Inicie una consola SSH en la máquina virtual desde XenCenter.
- Ajustar la cantidad de vCPU en una VM Linux en ejecución.
- Habilite el control dinámico de memoria (DMC).

  > **Nota:**
  >
  > No puede usar la función de control dinámico de memoria (DMC) en las máquinas virtuales Red Hat Enterprise Linux 8, Red Hat Enterprise Linux 9, Rocky Linux 8, Rocky Linux 9 o CentOS Stream 9, ya que estos sistemas operativos no admiten la expansión de memoria con el hipervisor Xen.

Es importante mantener el agente invitado de Linux actualizado a medida que actualiza el host de XenServer. Para obtener más información, consulte Actualizar los kernels de Linux y las utilidades de invitado.

> **Nota:**
>
> Antes de instalar el agente invitado en un invitado de SUSE Linux Enterprise Desktop o Server 15, asegúrese de que `insserv-compat-0.1-2.15.noarch.rpm` esté instalado en el invitado.

Para instalar XenServer VM Tools para Linux:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Descargue el archivo de XenServer VM Tools para Linux desde la página de descargas de XenServer.
2. Copie el archivo `LinuxGuestTools-xxx.tar.gz` en su máquina virtual Linux o en una unidad compartida a la que pueda acceder la máquina virtual Linux.
3. Extraiga el contenido del archivo tar: `tar -xzf LinuxGuestTools-xxx.tar.gz`
4. Ejecute el script de instalación como usuario root:

```
/<extract-directory>/install.sh
<!--NeedCopy-->
```

5. Si el kernel se ha actualizado o la VM se actualizó desde una versión anterior, reinicie la VM ahora.

Desinstalar XenServer VM Tools para Linux

A partir de la versión 8.4.0-1, puede usar el script `install.sh` para desinstalar XenServer VM Tools para Linux. Para desinstalar las herramientas, ejecute el siguiente comando como usuario raíz:

```
/<extract-directory>/install.sh -u
<!--NeedCopy-->
```

Instale controladores de terceros en su máquina virtual Linux de arranque seguro

Para instalar controladores de terceros en una máquina virtual Linux que tenga habilitado el arranque seguro de UEFI, debe crear una clave de firma, agregarla a la máquina virtual como clave de propietario de la máquina (MOK) y usar esa clave para firmar el controlador. Por ejemplo, si usa las funciones gráficas de XenServer con su máquina virtual Linux, es posible que necesite instalar el controlador de gráficos NVIDIA en la máquina virtual.

Siga estos pasos para crear una clave y utilizarla para instalar un controlador de terceros:

1. Genere un par de claves públicas y privadas.
2. Inscriba la clave pública en MOK.
3. Configure las claves que creó como claves de firma del módulo para el controlador.

El siguiente ejemplo muestra este procedimiento en detalle para un controlador de gráficos NVIDIA en una máquina virtual Ubuntu con arranque seguro:

1. Descarga el controlador de NVIDIA en tu máquina virtual.
2. Cree un directorio (por ejemplo, `/root/module-signing`) para guardar las claves:

```
mkdir -p /root/module-signing
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Crea una clave pública y privada para usar para firmar al conductor:

```
openssl req -new -x509 -newkey rsa:2048 -keyout /root/module-
    signing/Nvidia.key -outform DER -out /root/module-signing/
    Nvidia.der -nodes -days 36500 -subj "/CN=Graphics Drivers"
```

4. Importe la clave pública a MOK mediante `mokutil`:

```
mokutil --import /root/module-signing/Nvidia.der
```

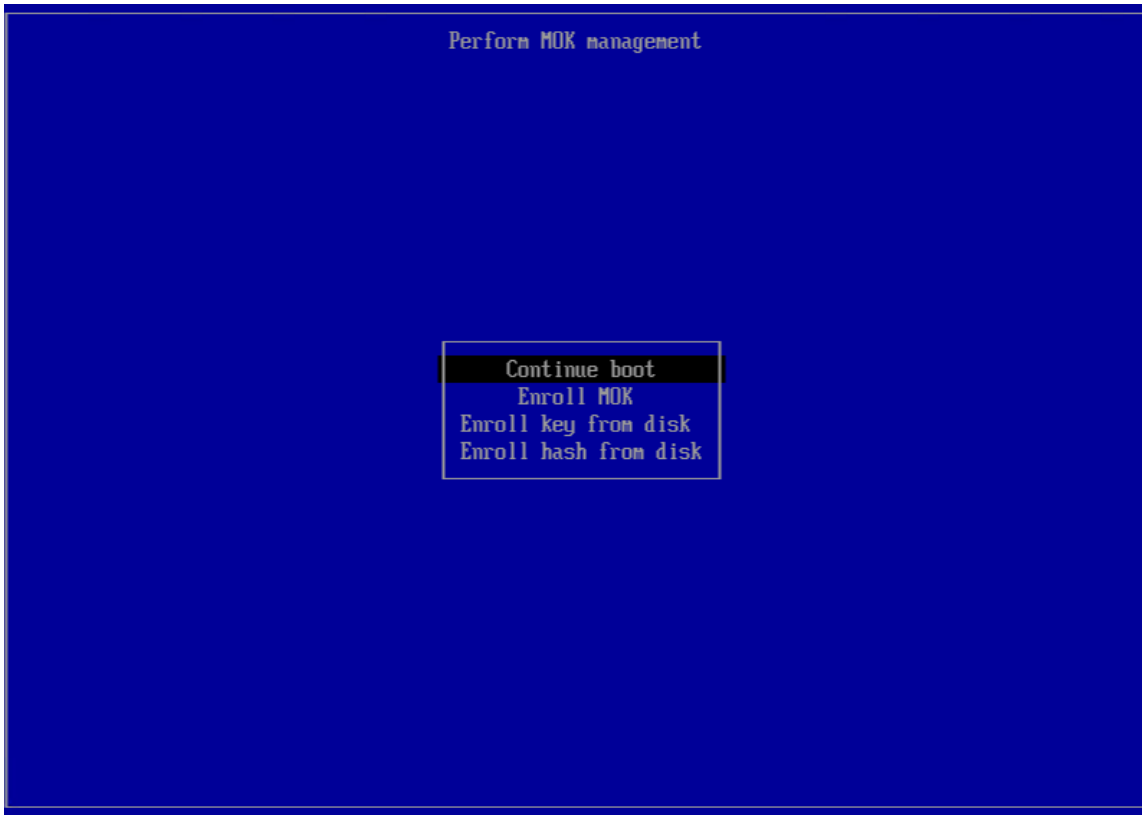
   Durante este paso, se le pedirá que cree una contraseña. La próxima vez que arranque, se le pedirá que introduzca la contraseña que creó aquí.

5. Asegúrese de que el destino de arranque de la máquina virtual esté configurado como gráfico:

```
systemctl set-default graphical.target
```

6. Reinicie la máquina virtual.

7. Durante el arranque, se muestra la GUI de **administración de Perform MOK** .



   En esta interfaz, complete los pasos siguientes:

   a) Seleccione **Inscribir MOK** > **Continuar**.
   b) Cuando se le pida si **inscribir las llaves**, seleccione **Sí**.
   c) Cuando se le solicite, introduzca la contraseña que creó al importar la clave pública (paso 4).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. Instale el paquete `libglvnd-dev`:

```
apt install pkg-config libglvnd-dev
```

9. Instale el controlador NVIDIA y especifique las claves que creó como claves de firma del módulo:

```
bash ./NVIDIA-Linux-x86_64-535.129.03-grid.run --module-signing-
    secret-key=/root/module-signing/Nvidia.key --module-signing-
    public-key=/root/module-signing/Nvidia.der
```

Notas de instalación para distribuciones de Linux

En esta sección se muestra la información de configuración específica del proveedor que se debe tener en cuenta antes de crear las máquinas virtuales Linux especificadas.

Para obtener notas de la versión más detalladas sobre todas las distribuciones, consulte Notas de la versión de VM de Linux.

Red Hat Enterprise Linux* 7 (32-64 bits)

La nueva plantilla para estos huéspedes especifica 2 GB de RAM. Esta cantidad de RAM es un requisito para una instalación correcta de v7.4 y versiones posteriores. Para v7.0 - v7.3, la plantilla especifica 2 GB de RAM, pero al igual que con las versiones anteriores de XenServer, 1 GB de RAM es suficiente.

> **Nota:**
>
> Esta información se aplica tanto a los derivados de Red Hat como de Red Hat.

Repositorios apt (Debian)

Para instalaciones poco frecuentes o puntuales, es razonable usar una réplica de Debian directamente. Sin embargo, si tiene la intención de realizar varias instalaciones de VM, le recomendamos que utilice un proxy de almacenamiento en caché o un espejo local. Se puede instalar cualquiera de las siguientes herramientas en una VM.

- `Apt-cacher`: implementación de un servidor proxy que mantiene una memoria caché local de paquetes
- `debmirror`: una herramienta que crea una réplica parcial o total de un repositorio de Debian

Prepararse para clonar una VM Linux

Por lo general, al clonar una máquina virtual o un equipo, a menos que generalice la imagen clonada, los atributos únicos de esa máquina se duplican en sus entornos. Algunos de los atributos únicos que

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

se duplican al clonar son la dirección IP, el SID o la dirección MAC.

Como resultado, XenServer cambia automáticamente algunos parámetros de hardware virtual cuando clona una VM Linux. Cuando copia la máquina virtual con XenCenter, XenCenter cambia automáticamente la dirección MAC y la dirección IP por usted. Si estas interfaces se configuran dinámicamente en su entorno, es posible que no necesite modificar la VM clonada. Sin embargo, si las interfaces están configuradas de forma estática, es posible que deba modificar sus configuraciones de red.

Es posible que la VM deba personalizarse para tener conocimiento de estos cambios. Para obtener instrucciones sobre distribuciones Linux compatibles específicas, consulte Notas de la versión de VM Linux.

Nombre de máquina

Una máquina virtual clonada es otro equipo y, como cualquier equipo nuevo en una red, debe tener un nombre único dentro del dominio de la red.

Dirección IP

Una máquina virtual clonada debe tener una dirección IP única dentro del dominio de red del que forma parte. En general, este requisito no es un problema cuando se usa DHCP para asignar direcciones. Cuando la máquina virtual se inicia, el servidor DHCP le asigna una dirección IP. Si la máquina virtual clonada tenía una dirección IP estática, se le debe dar al clon una dirección IP sin usar antes de iniciarse.

Dirección MAC

Hay dos situaciones en las que recomendamos inhabilitar las reglas de direcciones MAC antes de clonar:

1. En algunas distribuciones de Linux, la dirección MAC de la interfaz de red virtual de una máquina virtual clonada se registra en los archivos de configuración de red. Sin embargo, cuando clona una máquina virtual, XenCenter asigna a la nueva máquina virtual clonada una dirección MAC diferente. Como resultado, cuando se inicia la nueva VM por primera vez, la red reconoce la nueva VM y no se activa automáticamente.
2. Algunas distribuciones de Linux usan reglas udev para recordar la dirección MAC de cada interfaz de red y conservar un nombre para esa interfaz. Este comportamiento está diseñado para que la misma NIC física siempre se asigne a la misma interfaz `eth`*n*, lo que resulta útil con NIC

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

extraíbles (como portátiles). Sin embargo, este comportamiento es problemático en el contexto de las VM.

Por ejemplo, considere el comportamiento en el siguiente caso:

```
1.  Configure two virtual NICs when installing a VM
1.  Shut down the VM
1.  Remove the first NIC
```

Cuando la VM se reinicia, XenCenter muestra solo una NIC, pero la llama `eth0`. Mientras tanto, la VM está obligando deliberadamente a que esta NIC sea `eth1`. El resultado es que la creación de redes no funciona.

Para las máquinas virtuales que usan nombres persistentes, inhabilite estas reglas antes de clonar. Si no quieres desactivar los nombres persistentes, debes volver a configurar las redes dentro de la VM (de la forma habitual). Sin embargo, la información que se muestra en XenCenter no coincide con las direcciones reales de la red.

Actualización de kernels de Linux y utilidades invitadas

Las utilidades invitadas de Linux se pueden actualizar volviendo a ejecutar el `install.sh` script desde XenServer VM Tools para Linux (consulte Instalación de XenServerVM Tools para Linux).

Para distribuciones habilitadas para `yum`, CentOS y RHEL, `xe-guest-utilities` instala un archivo de configuración `yum` para permitir que las actualizaciones posteriores se realicen mediante `yum` de la manera estándar.

Para Debian, `/etc/apt/sources.list` se rellena para habilitar actualizaciones mediante apt de forma predeterminada.

Al actualizar, le recomendamos que vuelva a ejecutar siempre `install.sh`. Este script determina automáticamente si su máquina virtual necesita actualizaciones e instala si es necesario.

Notas de la versión de VM Linux

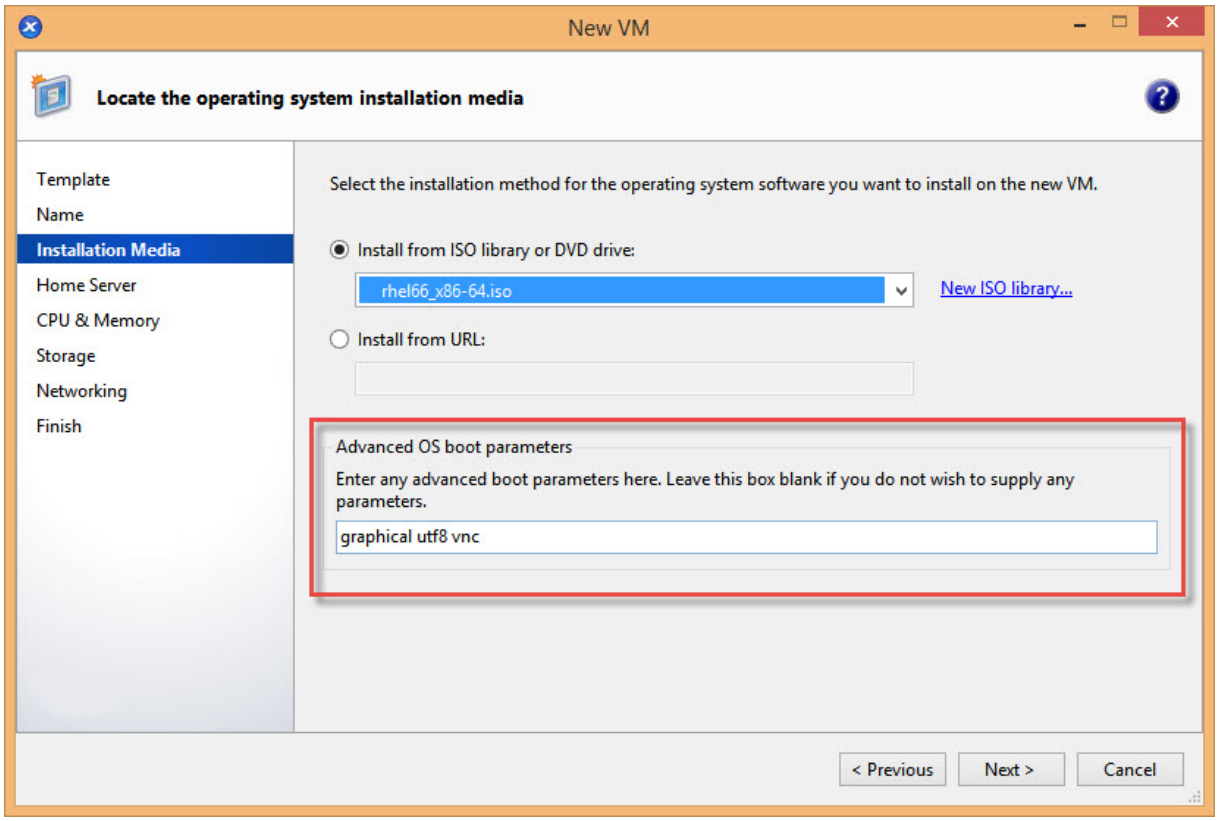
La mayoría de las distribuciones de Linux modernas admiten la paravirtualización de Xen directamente, pero tienen diferentes mecanismos de instalación y algunas limitaciones del núcleo.

Soporte de instalación gráfica de RHEL

Para usar el instalador gráfico, en XenCenter, recorra el asistente para **nuevas máquinas virtuales**. En la página **Medios de instalación**, en la sección **Parámetros de arranque avanzados del SO**, agregue `vnc` a la lista los parámetros:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
graphical utf8 vnc
<!--NeedCopy-->
```



Se le solicitará que proporcione una configuración de red para que la nueva VM habilite la comunicación de VNC. Repase el resto del asistente para nuevas máquinas virtuales. Cuando se complete el asistente, en la vista **Infraestructura**, seleccione la VM y haga clic en **Consola** para ver una sesión de consola de la VM. En este punto, utiliza el instalador estándar. La instalación de VM se inicia inicialmente en modo texto y puede solicitar la configuración de red. Una vez proporcionado, el botón **Cambiar a consola gráfica** se muestra en la esquina superior derecha de la ventana de XenCenter.

Red Hat Enterprise Linux 7

Después de migrar o suspender la VM, los invitados de RHEL 7 podrían congelarse durante la reanudación. Para obtener más información, consulte el número 1141249de Red Hat.

Red Hat Enterprise Linux 8

No puede usar la función de control dinámico de memoria (DMC) en las máquinas virtuales Red Hat Enterprise Linux 8, Red Hat Enterprise Linux 9, Rocky Linux 8, Rocky Linux 9 o CentOS Stream 9, ya que estos sistemas operativos no admiten la expansión de memoria con el hipervisor Xen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

CentOS 7

Para obtener la lista de notas de lanzamiento de CentOS 7, consulte Red Hat Enterprise Linux 7.

Oracle Linux 7

Para obtener la lista de notas de lanzamiento de Oracle Linux 7, consulte Red Hat Enterprise Linux 7.

Linux científico 7

Para obtener la lista de notas de lanzamiento de Scientific Linux 7, consulte Red Hat Enterprise Linux 7.

Debian 10

Si instala Debian 10 (Buster) mediante el arranque de red PXE, no agregue`console=tty0` los parámetros de arranque. Este parámetro puede provocar problemas con el proceso de instalación. Use solo `console=hvc0` en los parámetros de arranque.

Para obtener más información, consulte los números 944106 y 944125 de Debian.

SUSE Linux Enterprise 12

Preparar un huésped de SLES para la clonación

> **Nota:**
>
> Antes de preparar un invitado SLES para la clonación, asegúrese de borrar la configuración de udev para los dispositivos de red de la siguiente manera:

```
cat< /dev/null > /etc/udev/rules.d/30-net_persistent_names.rules
```

Para preparar a un huésped SLES para la clonación:

1. Abra el archivo `/etc/sysconfig/network/config`
2. Modifique la línea que dice:

```
FORCE_PERSISTENT_NAMES=yes
<!--NeedCopy-->
```

Para

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
FORCE_PERSISTENT_NAMES=no
<!--NeedCopy-->
```

3. Guarde los cambios y reinicie la VM.
   Para obtener más información, consulte Prepararse para clonar una máquina virtual Linux.

Ubuntu 18.04 (obsoleto)

Ubuntu 18.04 ofrece los siguientes tipos de kernel:

- El kernel de disponibilidad general (GA), que no se actualiza en las versiones puntuales
- El kernel Hardware Enablement (HWE), que se actualiza en las versiones puntuales

Algunas versiones menores de Ubuntu 18.04 (por ejemplo, 18.04.2 y 18.04.3) usan un kernel HWE de forma predeterminada que puede experimentar problemas al ejecutar la consola gráfica. Para evitar estos problemas, puede elegir ejecutar estas versiones secundarias de Ubuntu 18.04 con el kernel de GA o cambiar algunos de los ajustes gráficos. Para obtener más información, consulte CTX265663: Las máquinas virtuales de Ubuntu 18.04.2 puedenno arrancar en XenServer.

Memoria de VM

November 8, 2023

Cuando crea una VM, se asigna una cantidad fija de memoria a la VM. Puede usar el Control dinámico de memoria (DMC) para mejorar la utilización de la memoria física en el entorno de XenServer. DMC es una función de administración de memoria que permite la reasignación dinámica de memoria entre máquinas virtuales.

XenCenter proporciona una visualización gráfica del uso de memoria en su ficha **Memoria**. Para obtener más información, consulte la documentación de XenCenter.

El control dinámico de memoria (DMC) proporciona los siguientes beneficios:

- Puede agregar o eliminar memoria sin reiniciar las VM, lo que proporciona una experiencia perfecta para el usuario.
- Cuando los hosts están llenos, DMC le permite iniciar más máquinas virtuales en estos hosts, lo que reduce proporcionalmente la cantidad de memoria asignada a las máquinas virtuales en ejecución.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿Qué es el control dinámico de memoria (DMC)?

XenServer DMC funciona ajustando automáticamente la memoria de las máquinas virtuales en ejecución, manteniendo la cantidad de memoria asignada a cada máquina virtual entre los valores de memoria mínimos y máximos especificados, garantizando el rendimiento y permitiendo una mayor densidad de máquinas virtuales por host.

Sin DMC, cuando un host está lleno, se produce un error al iniciar más máquinas virtuales y se producen errores de "memoria insuficiente". Para reducir la asignación de memoria de VM existente y dejar espacio para más VM, modifique la asignación de memoria de cada VM y, a continuación, reinicie la VM. Al usar DMC, XenServer intenta recuperar memoria reduciendo automáticamente la asignación de memoria actual de las máquinas virtuales en ejecución dentro de los rangos de memoria definidos. XenServer intenta recuperar memoria incluso cuando el host está lleno.

> **Notas:**
>
> El control dinámico de memoria no se admite con máquinas virtuales que tienen una GPU virtual.

El concepto de rango dinámico

Para cada VM, el administrador puede establecer un rango de memoria dinámica. El rango de memoria dinámica es el rango dentro del cual se puede agregar/eliminar memoria de la VM sin necesidad de reiniciar. Cuando se ejecuta una máquina virtual, el administrador puede ajustar el rango dinámico. XenServer siempre garantiza mantener la cantidad de memoria asignada a la máquina virtual dentro del rango dinámico. Por lo tanto, si se ajusta mientras la máquina virtual está en ejecución, XenServer puede ajustar la cantidad de memoria asignada a la máquina virtual. El caso más extremo es cuando el administrador establece el valor mínimo/máximo dinámico, lo que obliga a XenServer a garantizar que esta cantidad de memoria se asigne a la máquina virtual. Si es necesario que las máquinas virtuales nuevas se inicien en hosts "completos", se "exprime"la memoria de las máquinas virtuales en ejecución para iniciar otras nuevas. La memoria adicional requerida se obtiene al comprimir proporcionalmente las VM en ejecución existentes dentro de sus rangos dinámicos predefinidos

DMC le permite configurar niveles de memoria mínimos y máximos dinámicos, creando un rango de memoria dinámica (DMR) en el que opera la VM.

- Memoria mínima dinámica: un límite de memoria inferior que se asigna a la máquina virtual.
- Límite superior dinámico: un límite superior de memoria que se asigna a la máquina virtual.

Por ejemplo, si la memoria mínima dinámica se estableció en 512 MB y la memoria máxima dinámica se estableció en 1024 MB, le da a la máquina virtual un rango de memoria dinámica (DMR) de 512 a 1024 MB, dentro del cual funciona. XenServer *garantiza* asignar siempre la memoria de cada máquina virtual dentro del DMR especificado cuando utilice DMC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El concepto de rango estático

Muchos sistemas operativos compatibles con XenServer no "entienden"completamente la noción de agregar o eliminar memoria de forma dinámica. Como resultado, XenServer debe declarar la cantidad máxima de memoria que se le pide a una máquina virtual que consuma en el momento en que se reinicia. La declaración de la cantidad máxima de memoria permite que el sistema operativo invitado ajuste el tamaño de sus tablas de páginas y otras estructuras de administración de memoria en consecuencia. Esto introduce el concepto de un rango de memoria estática en XenServer. El rango de memoria estática no se puede ajustar cuando la VM está en ejecución. Para un arranque en particular, el rango dinámico está restringido para que siempre esté contenido dentro de este rango estático. El mínimo estático (el límite inferior del rango estático) protege al administrador y se establece en la cantidad de memoria más baja que el sistema operativo puede ejecutar con XenServer.

> **Nota:**
>
> Le recomendamos que no cambie el nivel mínimo estático, ya que el nivel mínimo estático se establece en el nivel admitido por sistema operativo. Consulte la tabla de restricciones de memoria para obtener más información.
>
> Establecer un nivel máximo estático más alto que un máximo dinámico le permite asignar más memoria a una VM en el futuro sin reiniciar la VM.

Comportamiento DMC

Exprimido automático de máquinas virtuales

- Si DMC no está habilitado, cuando los hosts están llenos, la nueva máquina virtual comienza a fallar con errores de "memoria insuficiente".
- Cuando DMC está habilitado, incluso cuando los hosts están llenos, XenServer intenta recuperar memoria reduciendo la asignación de memoria de las máquinas virtuales en ejecución dentro de sus rangos dinámicos definidos. De esta manera, las VM en ejecución se comprimen proporcionalmente a la misma distancia entre el mínimo dinámico y el máximo dinámico para todas las VM en el host

Cuando DMC está habilitado

- Cuando la memoria del host es abundante: todas las máquinas virtuales en ejecución reciben su nivel de memoria máxima dinámica
- Cuando la memoria del host es escasa, todas las máquinas virtuales en ejecución reciben su nivel de memoria mínima dinámica.

Cuando configure DMC, recuerde que asignar solo una pequeña cantidad de memoria a una VM puede afectarla negativamente. Por ejemplo, asignar muy poca memoria:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- El uso de Dynamic Memory Control para reducir la cantidad de memoria física disponible para una VM puede provocar que se reinicie lentamente. Del mismo modo, si asigna muy poca memoria a una VM, puede iniciarse lentamente.
- Establecer un mínimo de memoria dinámica para una VM demasiado bajo puede provocar problemas de rendimiento o estabilidad deficientes cuando la VM se inicia.

¿Cómo funciona DMC?

Con DMC, es posible operar una máquina virtual invitada en uno de los dos modos siguientes:

1. **Modo de destino:** el administrador especifica un destino de memoria para el huésped. XenServer ajusta la asignación de memoria del huésped para cumplir con el objetivo. Especificar un destino es útil en entornos de servidores virtuales y en situaciones en las que sabe exactamente cuánta memoria quiere que utilice un huésped. XenServer ajusta la asignación de memoria del huésped para cumplir con el objetivo que especifique.
2. **Modo de rango dinámico:** el administrador especifica un rango de memoria dinámica para el huésped. XenServer selecciona un destino del rango y ajusta la asignación de memoria del huésped para cumplir con el objetivo. Especificar un rango dinámico resulta útil en entornos de escritorios virtuales y en cualquier situación en la que desee que XenServer reparticione la memoria del host de forma dinámica en respuesta a los cambios en el número de invitados o a los cambios en la presión de la memoria del host. XenServer selecciona un destino dentro del rango y ajusta la asignación de memoria del huésped para cumplir con el objetivo.

> **Nota:**
>
> Es posible cambiar entre el modo de destino y el modo de rango dinámico en cualquier momento para cualquier invitado en ejecución. Especifique un nuevo objetivo o un nuevo rango dinámico y XenServer se ocupará del resto.

Limitaciones de memoria

XenServer permite a los administradores utilizar todas las operaciones de control de memoria con cualquier sistema operativo huésped. Sin embargo, XenServer impone la siguiente restricción de orden de propiedades de memoria para todos los huéspedes:

```
0 < memory-static-min <= memory-dynamic-min <= memory-dynamic-max <= memory-static-max
```

XenServer permite a los administradores cambiar las propiedades de la memoria huésped a cualquier valor que cumpla con esta restricción, sujeto a comprobaciones de validación. Sin embargo, además de la restricción anterior, solo admitimos ciertas configuraciones de memoria de invitado para cada

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

sistema operativo compatible. La gama de configuraciones admitidas depende del sistema operativo invitado en uso. XenServer no impide que los administradores configuren los invitados para superar el límite admitido. Sin embargo, se recomienda a los clientes que mantengan las propiedades de la memoria dentro de los límites admitidos para evitar problemas de rendimiento o estabilidad. Para obtener pautas detalladas sobre los límites de memoria mínimo y máximo para cada sistema operativo compatible, consulte Compatibilidad con sistemas operativos invitados.

> **Advertencia:**
>
> Al configurar la memoria de invitado, le recomendamos NO exceder la cantidad máxima de memoria física direccionable por su sistema operativo. Establecer un máximo de memoria que sea mayor que el límite admitido por el sistema operativo puede provocar problemas de estabilidad en el huésped.
>
> El mínimo dinámico debe ser mayor o igual a un cuarto del máximo estático para todos los sistemas operativos compatibles. Reducir el límite inferior por debajo del mínimo dinámico también puede provocar problemas de estabilidad. Se anima a los administradores a calibrar cuidadosamente los tamaños de sus máquinas virtuales y garantizar que su conjunto de aplicaciones de trabajo funcione de manera fiable con un mínimo dinámico.
>
> El mínimo dinámico debe ser al menos el 75% del máximo estático. Un importe inferior puede provocar fallos en los huéspedes y no es compatible.

comandos de CLI xe

Mostrar las propiedades de memoria estática de una VM

1. Busque el UUID de la VM requerida:

```
xe vm-list
<!--NeedCopy-->
```

2. Anote el uuid y, a continuación, ejecute el comando `param-name=memory-static`

```
xe vm-param-get uuid=uuid param-name=memory-static-{
 min,max }

<!--NeedCopy-->
```

Por ejemplo, lo siguiente muestra las propiedades de memoria máxima estática para la máquina virtual con el UUID que comienza en ec77:

```
xe vm-param-get uuid= \
    ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \
    param-name=memory-static-max;
    268435456
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<!--NeedCopy-->
```

El ejemplo muestra que la memoria máxima estática para esta máquina virtual es de 268 435 456 bytes (256 MB).

Mostrar las propiedades de memoria dinámica de una VM

Para mostrar las propiedades de memoria dinámica, siga el procedimiento descrito anteriormente, pero use el comando `param-name=memory-dynamic`:

1. Busque el UUID de la VM requerida:

```
xe vm-list
<!--NeedCopy-->
```

2. Anote el uuid y, a continuación, ejecute el comando `param-name=memory-dynamic`:

```
xe vm-param-get uuid=uuid param-name=memory-dynamic-{
 min,max }

<!--NeedCopy-->
```

Por ejemplo, lo siguiente muestra las propiedades de memoria máxima dinámica para la máquina virtual con UUID que comienza con ec77

```
xe vm-param-get uuid= \
    ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \
    param-name=memory-dynamic-max;
    134217728
<!--NeedCopy-->
```

El ejemplo muestra que la memoria máxima dinámica para esta máquina virtual es de 134 217 728 bytes (128 MB).

Actualizar las propiedades de memoria

> **Advertencia:**
>
> Use el orden correcto al configurar los parámetros mínimo/máximo estáticos/dinámicos. Además, no debe invalidar la siguiente restricción:
>
> `0 < memory-static-min <= memory-dynamic-min <= memory-dynamic-max <= memory-static-max`

Actualice el rango de memoria estática de una máquina virtual:

```
xe vm-memory-static-range-set uuid=uuid min=value max=value
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Actualice el rango de memoria dinámica de una máquina virtual:

```
xe vm-memory-dynamic-range-set \
      uuid=uuid min=value \
      max=value
<!--NeedCopy-->
```

Especificar un destino es útil en entornos de servidores virtuales y en cualquier situación en la que sepa exactamente cuánta memoria quiere que utilice un huésped. XenServer ajusta la asignación de memoria del huésped para cumplir con el objetivo que especifique. Por ejemplo:

```
xe vm-memory-target-set target=value vm=vm-name
<!--NeedCopy-->
```

Actualice todos los límites de memoria (estáticos y dinámicos) de una máquina virtual:

```
xe vm-memory-limits-set \
      uuid=uuid \
      static-min=value \
      dynamic-min=value \
      dynamic-max=value static-max=value
<!--NeedCopy-->
```

> **Notas:**
>
> - Para asignar una cantidad específica de memoria a una máquina virtual que no cambie, establezca el máximo dinámico y el mínimo dinámico en el mismo valor.
> - No puede aumentar la memoria dinámica de una VM más allá del máximo estático.
> - Para modificar el máximo estático de una VM, debe apagarla.

Actualizar las propiedades de memoria individuales

> **Advertencia:**
>
> No cambie el nivel mínimo estático, ya que se establece en el nivel admitido por sistema operativo. Para obtener más información, consulte Restricciones de memoria.

Actualice las propiedades de memoria dinámica de una VM.

1. Busque el UUID de la VM requerida:

   ```
   xe vm-list
   <!--NeedCopy-->
   ```

2. Anote el uuid y, a continuación, utilice el comando `memory-dynamic-{ min,max } = value`

   ```
   xe vm-param-set uuid=uuid memory-dynamic-{
    min,max }
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  =value
<!--NeedCopy-->
```

En el siguiente ejemplo, se cambia el máximo dinámico a 128 MB:

```
xe vm-param-set uuid=ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 memory-
   dynamic-max=128MiB
<!--NeedCopy-->
```

Migrar máquinas virtuales

April 10, 2024

Puede migrar una máquina virtual en ejecución mediante la migración en vivo o la migración en vivo del almacenamiento para mover la imagen de disco virtual (VDI) de una máquina virtual sin ningún tiempo de inactividad de la máquina virtual.

Migración en vivo y migración en vivo

Las siguientes secciones describen los requisitos de compatibilidad y las limitaciones de la migración en vivo y la migración en vivo del almacenamiento.

Migración en vivo

La migración en vivo está disponible en todas las versiones de XenServer. Esta función le permite mover una máquina virtual en ejecución de un host a otro, cuando los discos de la máquina virtual (VDI) están en un almacenamiento compartido por ambos hosts. Las funciones de mantenimiento de grupos, como la alta disponibilidad y la actualización gradual de grupos (RPU), pueden mover automáticamente las máquinas virtuales mediante la migración en vivo. Estas funciones permiten la nivelación de la carga de trabajo, la resiliencia de la infraestructura y la actualización del software del servidor, sin ningún tiempo de inactividad de la VM.

Durante la migración en vivo de una máquina virtual, su memoria se transfiere como un flujo de datos entre dos hosts que utilizan la red. La función de compresión del flujo de migración comprime este flujo de datos, lo que acelera la transferencia de memoria en redes lentas. Esta función está inhabilitada de forma predeterminada, pero se puede cambiar mediante XenCenter o la CLI xe. Para obtener más información, consulte Propiedades de la agrupación: Opciones avanzadas y Parámetros de la agrupación. Como alternativa, puede habilitar la compresión al migrar una máquina virtual mediante la línea de comandos. Para obtener más información, consulte el comando `vm-migrate` en Comandos de máquina virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La función de evacuación de hosts en paralelo acelera el tiempo de evacuación del host (durante las actualizaciones del host) al mover las máquinas virtuales de un host en paralelo en lugar de secuencialmente. De forma predeterminada, esta función está habilitada y las máquinas virtuales se migran en lotes de 10 en paralelo. Puede cambiar el tamaño de lote predeterminado en el `/etc/xapi.conf` archivo.

> **Nota:**
>
> El almacenamiento solo se puede compartir entre hosts del mismo grupo. Como resultado, las VM solo se pueden migrar a hosts del mismo grupo.
>
> Intel GVT-g no es compatible con la migración en vivo, la migración en vivo de almacenamiento ni la suspensión de VM. Para obtener información, consulte Gráficos.

Migración en vivo de

> **Notas:**
>
> - No utilice la migración de almacenamiento en vivo en implementaciones de Citrix Virtual Desktops.
> - La migración en vivo de almacenamiento no se puede usar en máquinas virtuales que tengan habilitado el seguimiento de bloques modificado. Inhabilite el seguimiento de bloques modificados antes de intentar la migración en vivo del almacenamiento.
> - La migración en vivo del almacenamiento no se puede usar en máquinas virtuales cuyos VDI estén en una SR GFS2.

La migración de almacenamiento en vivo permite mover una máquina virtual de un host a otro cuando los discos de la máquina virtual no están en el almacenamiento compartido entre los dos hosts. Como resultado, las VM almacenadas en el almacenamiento local se pueden migrar sin tiempo de inactividad y las VM se pueden mover de un grupo a otro. Esta función permite a los administradores del sistema:

- Reequilibre las máquinas virtuales entre los grupos de XenServer (por ejemplo, de un entorno de desarrollo a un entorno de producción).
- Actualice y actualice los hosts independientes de XenServer sin tiempo de inactividad de las máquinas virtuales.
- Actualice el hardware del servidor XenServer.

> **Nota:**
>
> - La migración de una máquina virtual de un host a otro conserva el *estado*de la máquina virtual. La información de estado incluye información que define e identifica la VM y las

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

métricas de rendimiento históricas, como el uso de la CPU y la red.

- Para mejorar la seguridad, puede cerrar el puerto TCP 80 en la interfaz de administración de los hosts de XenServer. Sin embargo, no puede migrar una máquina virtual de un grupo CU1 de Citrix Hypervisor 8.2 sin la revisión XS82ECU1033 instalada a un grupo de XenServer con el puerto 80 cerrado. Para ello, instale XS82ECU1033 en el grupo CU1 de Citrix Hypervisor 8.2 o abra temporalmente el puerto 80 en el grupo de XenServer. Para obtener más información acerca de cómo cerrar el puerto 80, consulte Restringir el uso del puerto 80.

Requisitos de compatibilidad

Al migrar una VM con migración en vivo o migración en vivo de almacenamiento, la nueva VM y el servidor deben cumplir los siguientes requisitos de compatibilidad:

- El host de destino debe tener instalada la misma versión de XenServer o una más reciente como host de origen.
- Las herramientas de máquinas virtuales de XenServer para Windows deben estar instaladas en cada máquina virtual de Windows que quiera migrar.
- Si las CPU del host de origen y de destino son diferentes, el host de destino debe tener al menos la misma capacidad que el host de origen. Por lo general, esto significa que el destino tiene la misma CPU o una más nueva.
  - Si está migrando dentro del mismo grupo, el grupo intenta automáticamente hacer que una máquina virtual sea compatible.
  - Si va a migrar de un grupo a otro, debe asegurarse de que la máquina virtual sea compatible con el conjunto de funciones del grupo de destino.
- No puede migrar en vivo una máquina virtual entre procesadores AMD e Intel.
- No puede migrar simultáneamente más de 3 máquinas virtuales que tengan su ubicación de origen en el mismo grupo.
- El host de destino debe tener suficiente capacidad de memoria de reserva o poder liberar suficiente capacidad mediante el control de memoria dinámica. Si no hay suficiente memoria, la migración no se completa.
- Migración de almacenamiento únicamente: un host del grupo de origen debe tener suficiente capacidad de memoria libre para ejecutar una máquina virtual detenida que se esté migrando. Este requisito permite iniciar la máquina virtual detenida en cualquier momento del proceso de migración.
- Solo migración en vivo de almacenamiento: el almacenamiento de destino debe tener suficiente espacio libre en disco disponible para las máquinas virtuales entrantes. El espacio libre

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

requerido puede ser tres veces el tamaño de la VDI (sin instantáneas). Si no hay suficiente espacio, la migración no se completa.

- No puede usar la migración en vivo de almacenamiento para migrar máquinas virtuales que hayan habilitado el seguimiento de bloques modificado. Inhabilite el seguimiento de bloques modificados antes de intentar la migración en vivo del almacenamiento. Para obtener más información, consulte Seguimiento de bloques modificados.

Limitaciones y advertencias

La migración en vivo y la migración en vivo del almacenamiento están sujetas a las siguientes limitaciones y advertencias:

- La migración en vivo de almacenamiento no se puede usar con máquinas virtuales creadas por Machine Creation Services.
- Las máquinas virtuales que utilizan dispositivos de transferencia PCI no se pueden migrar (excepto en el caso de las GPU NVIDIA SR-IOV). Para obtener más información, consulte Usar NIC habilitadas para SR-IOV.
- Las máquinas virtuales con VUSB conectados no se pueden migrar.
- Las máquinas virtuales con el `no-migrate` conjunto de parámetros no se pueden migrar.
- Intel GVT-g no es compatible con la migración en vivo y la migración en vivo de almacenamiento. Para obtener más información, consulte Descripción general de los gráficos.
- Las máquinas virtuales que tienen la opción `on-boot` establecida en `reset` no se pueden migrar. Para obtener más información, consulte Intellicache.
- Si utiliza la función de alta disponibilidad y la máquina virtual que se está migrando está marcada como protegida, es posible que reciba una advertencia durante la migración en vivo si la operación hace que no se cumplan las restricciones de alta disponibilidad.
- El rendimiento de la VM se reduce durante la migración.
- El tiempo hasta la finalización de la migración de VM depende del consumo de memoria de la VM y de su actividad. Además, el tamaño de la VDI y la actividad de almacenamiento de la VDI pueden afectar a las VM que se migran con la migración de almacenamiento en vivo. Las máquinas virtuales con vGPU conectadas migran todo el estado de la vGPU mientras la máquina virtual está en pausa. Se recomienda utilizar una tarjeta de red rápida en la red de administración para reducir el tiempo de inactividad, especialmente con las vGPU que tienen grandes cantidades de memoria.
- Si la migración en vivo falla, por ejemplo, en el caso de un error de red, la máquina virtual del host de origen puede pasar al instante a un estado detenido.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Migrar una VM mediante XenCenter

1. En el panel Recursos, seleccione la VM y lleve a cabo una de las siguientes acciones:

   - Para migrar una VM en ejecución o suspendida mediante migración en vivo o migración en vivo de almacenamiento, en el menú **VM**, haga clic en **Migrar al servidor y, a** continuación, en **Asistente para migrar VM** Esta acción abre el asistente **Migrar VM**.
   - Para mover una VM detenida: en el menú **VM**, seleccione **Mover VM**. Esta acción abre el asistente **Mover VM**.

2. En la lista de **destinos**, seleccione un host independiente o un grupo.
3. En la lista de **servidores domésticos**, seleccione un host para asignarlo como servidor doméstico para la máquina virtual y haga clic en **Siguiente**.
4. En la ficha **Almacenamiento**, especifique el repositorio de almacenamiento donde quiere colocar los discos vDisk de la VM migrada y, a continuación, haga clic en **Siguiente**.

   - El botón de **opción Colocar todos los discos vDisk migrados en el mismo SR** está seleccionado de forma predeterminada y muestra la SR compartida predeterminada en el grupo de destino.
   - Haga clic en **Colocar discos virtuales migrados en los SR especificados** para especificar un SR de la lista **Repositorio de almacenamiento**. Esta opción le permite seleccionar SR diferente para cada disco vDisk en la VM migrada.

5. En la lista **Red de almacenamiento**, seleccione una red en el grupo de destino que se utilice para la migración en vivo de los discos virtuales de la máquina virtual. Haga clic en **Siguiente**.

   > **Nota:**
   >
   > Por motivos de rendimiento, se recomienda que no utilice su red de administración para la migración en vivo.

6. Revise los valores de configuración y haga clic en **Finalizar** para iniciar la migración de la VM.

Si va a actualizar de 7,1 CU2 a 8,2 CU1, es posible que tenga que apagar y arrancar todas las máquinas virtuales después de migrarlas para asegurarse de que se incorporan las nuevas funciones de virtualización.

Migración de VDI en vivo

La migración de VDI en vivo permite al administrador reubicar la imagen de disco vDisk (VDI) de VM sin apagar la VM. Esta función permite realizar operaciones administrativas tales como:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Trasladar una VM desde un almacenamiento local barato a un almacenamiento rápido, resistente y respaldado por matrices.
- Mover una VM de un entorno de desarrollo a un entorno de producción.
- Moverse entre niveles de almacenamiento cuando una VM está limitada por la capacidad de almacenamiento.
- Realizar actualizaciones de arreglos de almacenamiento.

Limitaciones y advertencias

La migración de VDI en vivo está sujeta a las siguientes limitaciones y advertencias:

- No utilice la migración de almacenamiento en vivo en implementaciones de Citrix Virtual Desktops.
- Las máquinas virtuales Linux IPv6 requieren un kernel de Linux superior a 3.0.
- Si realiza una migración de VDI en vivo en una máquina virtual que tiene una vGPU, se utiliza la migración en vivo de vGPU. El host debe tener suficiente espacio de vGPU para hacer una copia de la instancia de vGPU en el host. Si las PGPU se emplean por completo, es posible que la migración de VDI no sea posible.
- Cuando realiza una migración en vivo de VDI para una VM que permanece en el mismo host, esa VM requiere temporalmente el doble de RAM.

Para mover discos virtuales

1. En el panel **Recursos**, seleccione la SR en la que está almacenado el disco virtual y, a continuación, haga clic en la ficha **Almacenamiento**.
2. En la lista **Discos virtuales**, seleccione el disco virtual que quiere mover y, a continuación, haga clic en **Mover**.
3. En el cuadro de diálogo **Mover disco vDisk**, seleccione el SR de destino al que quiere mover el VDI.

   > **Nota:**
   >
   > Asegúrese de que la SR tenga espacio suficiente para otro disco virtual: el espacio disponible se muestra en la lista de SR disponibles.

4. Haga clic en **Mover** para mover el disco vDisk.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Importación y exportación de máquinas virtuales

February 23, 2024

XenServer le permite importar máquinas virtuales y exportarlas a varios formatos diferentes. Con el asistente de importación de XenCenter, puede importar máquinas virtuales desde imágenes de disco (VHD y VMDK), formato de virtualización abierta (OVF y OVA) y formato XVA de XenServer. Incluso puede importar máquinas virtuales que se hayan creado en otras plataformas de virtualización, como las que ofrecen VMware y Microsoft.

> **Nota:**
>
> Al importar máquinas virtuales que se hayan creado con otras plataformas de virtualización, configure o *arregle* el sistema operativo invitado para asegurarse de que arranque en XenServer. La función de reparación del sistema operativo de XenCenter tiene como objetivo proporcionar este nivel básico de interoperabilidad. Para obtener más información, consulte Reparación del sistema operativo.

Con el asistente de exportación de **XenCenter**, puede exportar las máquinas virtuales al formato Open Virtualization Format (OVF y OVA) y al formato XVA de XenServer.

También puede usar la CLI xe para importar máquinas virtuales y exportarlas al formato XVA de XenServer.

Formatos de archivo admitidos

Formato	Descripción
Formato de virtualización abierta (OVF y OVA)	OVF es un estándar abierto para empaquetar y distribuir un dispositivo virtual que consta de una o más máquinas virtuales.
Formatos de imagen de disco (VHD y VMDK)	Los archivos de imagen de disco en formato de disco duro virtual (VHD) y disco de máquina virtual (VMDK) se pueden importar mediante el asistente de importación. La importación de una imagen de disco puede ser apropiada cuando hay una imagen de disco vDisk disponible, sin metadatos OVF asociados.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Formato	Descripción
Formato XVA de XenServer	XVA es un formato específico de hipervisores basados en Xen para empaquetar una VM individual como un archivo único, incluyendo un descriptor e imágenes de disco. Su extensión de nombre de archivo es `.xva`.

¿Qué formato usar?

Considere usar el formato OVF/OVA para:

- Compartir vApps y máquinas virtuales de XenServer con otras plataformas de virtualización que admitan OVF
- Ahorre más de una VM
- Proteja una vApp o VM de la corrupción y la manipulación
- Incluir un acuerdo de licencia
- Simplifique la distribución de vApp almacenando un paquete OVF en un archivo OVA

Considere usar el formato XVA para:

- Importación y exportación de máquinas virtuales desde un script con una CLI

Formato de virtualización abierto (OVF y OVA)

OVF es un estándar abierto, especificado por el Grupo de trabajo de administración distribuida, para empaquetar y distribuir un dispositivo virtual que consta de una o más máquinas virtuales. Para obtener más información sobre los formatos OVF y OVA, consulte la siguiente información:

- Artículo CTX121652 de Knowledge Base: Descripción general del formato de virtualización abierta
- Especificación de formato de virtualización abierta

> **Nota:**
>
> Para importar o exportar paquetes de OVF u OVA, debe iniciar sesión como root o tener la función de control de acceso basado en funciones (RBAC) de administrador de grupos asociada a su cuenta de usuario.

Un **paquete OVF** es el conjunto de archivos que comprende el dispositivo virtual. Siempre incluye un archivo descriptor y cualquier otro archivo que represente los siguientes atributos del paquete:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

atributos **Descriptor (`.ovf`):** El descriptor siempre especifica los requisitos de hardware virtual del paquete. También puede especificar otra información, que incluye:

- Descripciones de los discos virtuales, el paquete en sí y los sistemas operativos invitados
- Un acuerdo de licencia
- Instrucciones para iniciar y detener máquinas virtuales en el dispositivo
- Instrucciones para instalar el paquete

Firma (`.cert`): La firma es la firma digital utilizada por un certificado de clave pública en el formato X.509 para autenticar al autor del paquete.

Manifest (`.mf`): El manifiesto le permite verificar la integridad del contenido del paquete. Contiene los resúmenes SHA-1 de cada archivo del paquete.

Discos virtuales: OVF no especifica un formato de imagen de disco. Un paquete OVF incluye archivos que comprenden discos vDisk en el formato definido por el producto de virtualización que exportó los discos vDisk. XenServer produce paquetes OVF con imágenes de disco en formato VHD dinámico; los productos VMware y Virtual Box producen paquetes OVF con discos virtuales en formato VMDK optimizado para streaming.

Los paquetes de OVF también admiten otras capacidades no relacionadas con metadatos, como compresión, archivado, datos adjuntos de CLUF y anotaciones.

> **Nota:**
>
> Al importar un paquete de OVF que se ha comprimido o contiene archivos comprimidos, es posible que necesite liberar espacio adicional en el disco del host de XenServer para importarlo correctamente.

Un **paquete Open Virtual Appliance (OVA)** es un archivo de almacenamiento único, en formato de archivo en cinta (.tar), que contiene los archivos que componen un paquete OVF.

Seleccione el formato OVF u OVA Los paquetes OVF contienen una serie de archivos sin comprimir, lo que facilita el acceso a imágenes de disco individuales en el archivo. Un paquete OVA contiene un archivo grande y, aunque puede comprimirlo, no le brinda la flexibilidad de una serie de archivos.

El uso del formato OVA es útil para aplicaciones específicas para las que es beneficioso tener un solo archivo, como la creación de paquetes para descargas web. Considere usar OVA solo como una opción para que el paquete sea más fácil de manejar. El uso de este formato alarga los procesos de exportación e importación.

Formatos de imagen de disco (VHD y VMDK)

Con XenCenter, puede importar imágenes de disco en los formatos de disco duro virtual (VHD) y disco de máquina virtual (VMDK). No se admite la exportación de imágenes de disco independientes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Para importar imágenes de disco, asegúrese de haber iniciado sesión como root o de tener la función RBAC de administrador de grupos asociada a su cuenta de usuario.

Puede importar una imagen de disco cuando esté disponible una imagen de disco vDisk sin metadatos OVF asociados. Esta opción puede producirse en las siguientes situaciones:

- Es posible importar una imagen de disco, pero los metadatos de OVF asociados no se pueden leer
- Un disco virtual no está definido en un paquete OVF
- Está pasando de una plataforma que no le permite crear un paquete OVF (por ejemplo, plataformas o imágenes más antiguas)
- Desea importar un dispositivo VMware anterior que no tenga ninguna información de OVF
- Quiere importar una máquina virtual independiente que no tenga información OVF

Cuando estén disponibles, recomendamos importar paquetes de dispositivos que contengan metadatos de OVF en lugar de una imagen de disco individual. Los datos de OVF proporcionan información que el asistente de importación requiere para recrear una máquina virtual a partir de su imagen de disco. Esta información incluye la cantidad de imágenes de disco asociadas a la máquina virtual, el procesador, el almacenamiento, la red, los requisitos de memoria, etc. Sin esta información, puede ser mucho más complejo y propenso a errores recrear la VM.

Formato XVA

XVA es un formato de dispositivo virtual específico de XenServer, que empaqueta una sola máquina virtual como un conjunto único de archivos, incluidos un descriptor e imágenes de disco. La extensión del nombre de archivo es `.xva`.

El descriptor (extensión de nombre de archivo `ova.xml`) especifica el hardware virtual de una sola VM.

El formato de imagen de disco es un directorio de archivos. El nombre del directorio corresponde a un nombre de referencia en el descriptor y contiene dos archivos para cada bloque de 1 MB de la imagen de disco. El nombre base de cada archivo es el número de bloque en decimal. El primer archivo contiene un bloque de la imagen de disco en formato binario sin procesar y no tiene extensión. El segundo archivo es una suma de comprobación del primer archivo. Si la máquina virtual se exportó desde Citrix Hypervisor 8.0 o anterior, este archivo tiene la extensión `.checksum`. Si la máquina virtual se exportó desde Citrix Hypervisor 8.1 o posterior, este archivo tiene la extensión `.xxhash`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Importante:**
>
> Si se exporta una máquina virtual desde el host de XenServer y, a continuación, se importa a otro host de XenServer con un tipo de CPU diferente, es posible que no se ejecute correctamente. Por ejemplo, una VM Windows exportada desde un host con una CPU habilitada para Intel® VT podría no ejecutarse cuando se importa a un host con una CPU AMD-VTM.

Corrección del sistema operativo

Al importar un dispositivo virtual o una imagen de disco creada y exportada desde una plataforma de virtualización distinta de XenServer, es posible que tenga que configurar la máquina virtual antes de que se inicie correctamente en el host de XenServer.

XenCenter incluye una función avanzada de interoperabilidad de hipervisores, Operating System Fixup, que tiene como objetivo garantizar un nivel básico de interoperabilidad para las máquinas virtuales que se importan a XenServer. Utilice la corrección del sistema operativo al importar máquinas virtuales de paquetes OVF/OVA e imágenes de disco creadas en otras plataformas de virtualización.

El proceso de reparación del sistema operativo aborda los problemas de controladores y dispositivos del sistema operativo inherentes al pasar de un hipervisor a otro. El proceso intenta reparar los problemas relacionados con el dispositivo de arranque con la máquina virtual importada que podrían impedir que el sistema operativo interno se inicie en el entorno de XenServer. Esta función no está diseñada para realizar conversiones de una plataforma a otra.

> **Nota:**
>
> Esta función requiere un repositorio de almacenamiento ISO con 40 MB de espacio libre y 256 MB de memoria virtual.

La reparación del sistema operativo se suministra como una imagen ISO de arranque automático que se conecta a la unidad de DVD de la máquina virtual importada. Realiza las operaciones de reparación necesarias cuando la VM se inicia por primera vez y, a continuación, la apaga. La próxima vez que se inicie la nueva VM, se restablecerá el dispositivo de arranque y la VM se iniciará normalmente.

Para usar la corrección del sistema operativo en imágenes de disco o paquetes OVF/OVA importados, habilite la función en la página Opciones avanzadas del asistente de importación de XenCenter. Especifique una ubicación en la que se copie la ISO de Fixup para que XenServer pueda usarla.

¿Qué le hace la reparación del sistema operativo a la VM?

La opción de reparación del sistema operativo está diseñada para realizar los cambios mínimos posibles para permitir que un sistema virtual se inicie. Según el sistema operativo invitado y el hipervisor

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

del host original, es posible que se requieran más acciones después de usar la reparación del sistema operativo. Estas acciones pueden incluir cambios de configuración e instalación de controladores.

Durante el proceso de reparación, una ISO se copia en una ISO SR. La ISO está conectada a una VM. El orden de arranque se establece para que arranque desde la unidad de DVD virtual y la VM se inicia en la ISO. El entorno dentro de la ISO luego verifica cada disco de la VM para determinar si se trata de un sistema Linux o Windows.

Si se detecta un sistema Linux, se determina la ubicación del archivo de configuración de GRUB. Los punteros a los dispositivos de arranque de disco SCSI se modifican para que apunten a los discos IDE. Por ejemplo, si GRUB contiene una entrada `/dev/sda1` que representa el primer disco en la primera controladora SCSI, esta entrada se cambia a `/dev/hda1` para representar el primer disco en la primera controladora IDE.

Si se detecta un sistema Windows, se extrae un controlador de dispositivo de arranque crítico genérico de la base de datos de controladores del sistema operativo instalado y se registra con el sistema operativo. Este proceso es especialmente importante para los sistemas operativos Windows más antiguos cuando el dispositivo de arranque se cambia entre una interfaz SCSI e IDE.

Si se detectan ciertos conjuntos de herramientas de virtualización en la VM, se inhabilitan para evitar problemas de rendimiento y mensajes de eventos innecesarios.

Importación de máquinas virtuales

Al importar una máquina virtual, se crea una máquina virtual de manera eficaz, siguiendo muchos de los mismos pasos necesarios para aprovisionar una nueva máquina virtual. Estos pasos incluyen la designación de un host y la configuración del almacenamiento y las redes.

Puede importar archivos OVF/OVA, imagen de disco, XVA y XVA versión 1 mediante el asistente de importación de XenCenter. También puede importar archivos XVA a través de la CLI xe.

Importación de máquinas virtuales de OVF/OVA

> **Nota:**
>
> Para importar paquetes OVF u OVA, debe iniciar sesión como raíz o tener la función de control de acceso basado en funciones (RBAC) de administrador de grupos asociada a su cuenta de usuario.

El asistente de importación de XenCenter le permite importar máquinas virtuales que se hayan guardado como archivos OVF/OVA. El asistente de importación le guiará por los pasos habituales para crear una máquina virtual en XenCenter: Designar un host y, a continuación, configurar el almacenamiento y las redes para la nueva máquina virtual. Al importar archivos OVF y OVA, es posible que se requieran pasos adicionales, tales como:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Al importar máquinas virtuales que se han creado con otras plataformas de virtualización, ejecute la función de reparación del sistema operativo para garantizar un nivel básico de interoperabilidad para la máquina virtual. Para obtener más información, consulte Reparación del sistema operativo.

> **Consejo:**
>
> Asegúrese de que el host de destino tenga suficiente RAM para admitir las máquinas virtuales que se van a importar. La falta de RAM disponible provoca un error en la importación. Para obtener más información sobre cómo resolver este problema, consulte CTX125120: El asistente de importación de dispositivos falla por falta de memoria.

Los paquetes OVF importados aparecen como vApp cuando se importan con XenCenter. Cuando se completa la importación, las nuevas VM aparecen en el panel **Recursos** de XenCenter y la nueva vApp aparece en el cuadro de diálogo **Administrar vApps**.

Para importar máquinas virtuales desde OVF/OVA mediante XenCenter:

1. Abra el asistente de importación mediante una de las siguientes acciones:
   - En el panel **Recursos**, haga clic con el botón derecho y, a continuación, seleccione **Importar** en el menú contextual.
   - En el menú **Archivo**, seleccione **Importar**.
2. En la primera página del asistente, busque el archivo que desea importar y, a continuación, haga clic en **Siguiente** para continuar.
3. Revise y acepte los EULA, si procede.

   Si el paquete que va a importar incluye algún CLUF, acéptelo y haga clic en **Siguiente** para continuar. Cuando no se incluyen CLUF en el paquete, el asistente omite este paso y avanza directamente a la página siguiente.
4. Especifique el grupo o el host al que desea importar las máquinas virtuales y, a continuación, asigne las máquinas virtuales a un servidor doméstico.

   Para seleccionar un host o un grupo, elija en la lista **Importar máquinas virtuales** a.

   Para asignar a cada máquina virtual un servidor doméstico, seleccione un host de la lista del **servidor doméstico**. Si no desea asignar un servidor doméstico, seleccione **No asignar un servidor doméstico**.

   Haga clic en **Next** para continuar.
5. Configure el almacenamiento para las máquinas virtuales importadas: elija uno o más repositorios de almacenamiento en los que colocar los discos virtuales importados y, a continuación, haga clic en **Siguiente** para continuar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para colocar todos los discos vDisk importados en el mismo SR, seleccione **Colocar todas las VM importadas en este SR de destino**. Seleccione un SR de la lista.

Para colocar los discos virtuales de las máquinas virtuales entrantes en diferentes SR, seleccione **Colocar máquinas virtuales importadas en los SR de destino especificados**. Para cada VM, seleccione el SR de destino en la lista de la columna SR.

6. Configure las redes para las máquinas virtuales importadas: asigne las interfaces de red virtual de las máquinas virtuales que va a importar a las redes de destino del grupo de destino. La dirección de red y MAC que se muestran en la lista de máquinas virtuales entrantes se almacenan como parte de la definición de la máquina virtual original (exportada) en el archivo de exportación. Para asignar una interfaz de red virtual entrante a una red de destino, seleccione una red de la lista en la columna Red de destino. Haga clic en **Next** para continuar.

7. Especificar la configuración de seguridad: si el paquete OVF/OVA seleccionado está configurado con funciones de seguridad, como certificados o un manifiesto, especifique la información necesaria y, a continuación, haga clic en **Siguiente** para continuar.

   En la página Seguridad aparecen diferentes opciones en función de las funciones de seguridad que se hayan configurado en el dispositivo OVF:

   - Si el dispositivo está firmado, aparece la casilla **Verificar firma digital**, que se selecciona automáticamente. Haga clic en **Ver certificado** para mostrar el certificado utilizado para firmar el paquete. Si el certificado parece que no es de confianza, es probable que el certificado raíz o la autoridad emisora de certificados no sean de confianza en el equipo local. Desmarque la casilla de verificación **Verificar firma digital** si no desea verificar la firma.
   - Si el dispositivo incluye un manifiesto, aparece la casilla de verificación **Verificar el contenido del manifiesto**. Seleccione esta casilla de verificación para que el asistente verifique la lista de archivos del paquete.

   Cuando los paquetes se firman digitalmente, el manifiesto asociado se verifica automáticamente, por lo que la casilla de verificación **Verificar el contenido del manifiesto** no aparece en la página Seguridad.

   > **Nota:**
   >
   > Los archivos OVF de VMware Workstation 7.1.x no se importan cuando decide verificar el manifiesto. Este error se produce porque VMware Workstation 7.1.x produce un archivo OVF con un manifiesto que tiene valores hash SHA-1 no válidos. Si decide no verificar el manifiesto, la importación se ha realizado correctamente.

8. Habilitar la reparación del sistema operativo: si las máquinas virtuales del paquete que va a importar se crearon en una plataforma de virtualización distinta de XenServer, active la casilla **Usar reparación del sistema operativo** . Seleccione una ISO SR donde se pueda copiar la ISO

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de Fixup para que XenServer pueda acceder a ella. Para obtener más información sobre esta función, consulte Corrección del sistema operativo.

Haga clic en **Next** para continuar.

9. Revise la configuración de importación y, a continuación, haga clic en **Finalizar** para iniciar el proceso de importación y cerrar el asistente.

> **Nota:**
>
> La importación de una VM puede llevar algún tiempo, según el tamaño de la VM y la velocidad y el ancho de banda de la conexión de red.

El progreso de la importación se muestra en la barra de estado en la parte inferior de la ventana de XenCenter y en la ficha **Registros**. Cuando la máquina virtual recién importada está disponible, aparece en el panel **Recursos** y la nueva vApp aparece en el cuadro de diálogo **Administrar vApps**.

> **Nota:**
>
> Después de utilizar XenCenter para importar un paquete OVF que contenga sistemas operativos Windows, debe establecer el parámetro `platform`.
>
> 1. Establezca el parámetro `platform` en `device_id=0002`. Por ejemplo:
>
> ```
> 1 xe vm-param-set uuid=VM uuid platform:device_id=0002
> ```
>
> 2. Establezca el parámetro `platform` en `viridian=true`. Por ejemplo:
>
> ```
> 1 xe vm-param-set uuid=VM uuid platform:viridian=true
> ```

Importar imágenes de disco

El asistente de importación de XenCenter le permite importar una imagen de disco en un grupo o host específico como una máquina virtual. El asistente de importación le guiará por los pasos habituales para crear una máquina virtual en XenCenter: Designar un host y, a continuación, configurar el almacenamiento y las redes para la nueva máquina virtual.

Requisitos

- Debe iniciar sesión como root o tener la función de control de acceso basado en funciones (RBAC) de administrador de grupos asociada a su cuenta de usuario.
- Asegúrese de que DHCP se ejecute en la red de administración que utiliza XenServer.
- El asistente de importación requiere almacenamiento local en el servidor en el que se ejecuta.

Para importar máquinas virtuales desde una imagen de disco mediante XenCenter:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Abra el asistente de importación mediante una de las siguientes acciones:

   - En el panel **Recursos**, haga clic con el botón derecho y, a continuación, seleccione **Importar** en el menú contextual.
   - En el menú **Archivo**, seleccione **Importar**.

2. En la primera página del asistente, busque el archivo que desea importar y, a continuación, haga clic en **Siguiente** para continuar.

3. Especifique el nombre de la VM y asigne los recursos de CPU y memoria.

   Introduzca un nombre para la nueva máquina virtual que se creará a partir de la imagen de disco importada y, a continuación, asigne la cantidad de CPU y la cantidad de memoria. Haga clic en **Next** para continuar.

4. Especifique el grupo o el host al que desea importar las máquinas virtuales y, a continuación, asigne las máquinas virtuales a un servidor doméstico.

   Para seleccionar un host o un grupo, elija en la lista **Importar máquinas virtuales** a.

   Para asignar a cada máquina virtual un servidor doméstico, seleccione un host de la lista del **servidor doméstico**. Si no desea asignar un servidor doméstico, seleccione **No asignar un servidor doméstico**.

   Haga clic en **Next** para continuar.

5. Configurar el almacenamiento de las máquinas virtuales importadas: seleccione uno o más repositorios de almacenamiento en los que colocar los discos virtuales importados y, a continuación, haga clic en **Siguiente** para continuar.

   Para colocar todos los discos vDisk importados en el mismo SR, seleccione **Colocar todas las VM importadas en este SR de destino**. Seleccione un SR de la lista.

   Para colocar los discos virtuales de las máquinas virtuales entrantes en diferentes SR, seleccione **Colocar máquinas virtuales importadas en los SR de destino especificados**. Para cada VM, seleccione el SR de destino en la lista de la columna SR.

6. Configure las redes para las máquinas virtuales importadas: asigne las interfaces de red virtual de las máquinas virtuales que va a importar a las redes de destino del grupo de destino. La dirección de red y MAC que se muestran en la lista de máquinas virtuales entrantes se almacenan como parte de la definición de la máquina virtual original (exportada) en el archivo de exportación. Para asignar una interfaz de red virtual entrante a una red de destino, seleccione una red de la lista en la columna Red de destino. Haga clic en **Next** para continuar.

7. Habilitar la reparación del sistema operativo: si las imágenes de disco que va a importar se crearon en una plataforma de virtualización distinta de XenServer, active la casilla Usar reparación del sistema operativo. Seleccione una ISO SR donde se pueda copiar la ISO de Fixup

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

para que XenServer pueda acceder a ella. Para obtener más información sobre esta función, consulte Corrección del sistema operativo.

Haga clic en **Next** para continuar.

8. Revise la configuración de importación y, a continuación, haga clic en **Finalizar** para iniciar el proceso de importación y cerrar el asistente.

> **Nota:**
>
> La importación de una VM puede llevar algún tiempo, según el tamaño de la VM y la velocidad y el ancho de banda de la conexión de red.

El progreso de la importación se muestra en la barra de estado en la parte inferior de la ventana de XenCenter y en la ficha **Registros**. Cuando la máquina virtual recién importada está disponible, aparece en el panel **Recursos**.

> **Nota:**
>
> Después de utilizar XenCenter para importar una imagen de disco que contenga sistemas operativos Windows, debe establecer el parámetro `platform`. El valor de este parámetro varía según la versión de Windows contenida en la imagen de disco:

- Para Windows Server 2016 y versiones posteriores, establezca el parámetro `platform` en `device_id=0002`. Por ejemplo:

```
xe vm-param-set uuid=VM uuid platform:device_id=0002
<!--NeedCopy-->
```

- Para todas las demás versiones de Windows, establezca el parámetro `platform` en `viridian=true`. Por ejemplo:

```
xe vm-param-set uuid=VM uuid platform:viridian=true
<!--NeedCopy-->
```

Importar máquinas virtuales desde XVA

Puede importar máquinas virtuales, plantillas e instantáneas que se hayan exportado y almacenado previamente de forma local en formato XVA (`.xva`). Para hacerlo, siga los pasos habituales para crear una VM: nominar un host y, a continuación, configurar el almacenamiento y las redes para la nueva VM.

> **Advertencia:**
>
> Es posible que no siempre sea posible ejecutar una máquina virtual importada que se exportó desde otro host con un tipo de CPU diferente. Por ejemplo, es posible que una máquina virtual de Windows exportada desde un host con una CPU compatible con Intel VT no se ejecute cuando

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> se importe a un host con una CPU AMD-VTM.

Para importar máquinas virtuales desde XVA mediante XenCenter:

1. Abra el asistente de importación mediante una de las siguientes acciones:
   - En el panel **Recursos**, haga clic con el botón derecho y, a continuación, seleccione **Importar** en el menú contextual.
   - En el menú **Archivo**, seleccione **Importar**.
2. En la primera página del asistente, busque el archivo que desea importar (`.xva` o `ova.xml`) y, a continuación, haga clic en **Siguiente** para continuar.

   Si introduce una ubicación de URL (`http`, `https`, `file` o `ftp`) en el cuadro **Nombre de archivo**. Haga clic en **Siguiente**, se abre un cuadro de diálogo Descargar paquete y debe especificar una carpeta en el host XenCenter donde se copia el archivo.
3. Seleccione un grupo o host para que se inicie la máquina virtual importada y, a continuación, haga clic en **Siguiente** para continuar.
4. Seleccione los repositorios de almacenamiento en los que desea colocar el disco virtual importado y, a continuación, haga clic en **Siguiente** para continuar.
5. Configure las redes para la máquina virtual importada: asigne la interfaz de red virtual en la máquina virtual que va a importar para apuntar a una red en el grupo de destino. La dirección de red y MAC que se muestran en la lista de máquinas virtuales entrantes se almacenan como parte de la definición de la máquina virtual original (exportada) en el archivo de exportación. Para asignar una interfaz de red virtual entrante a una red de destino, seleccione una red de la lista en la columna Red de destino. Haga clic en **Next** para continuar.
6. Revise la configuración de importación y, a continuación, haga clic en **Finalizar** para iniciar el proceso de importación y cerrar el asistente.

   > **Nota:**
   >
   > La importación de una VM puede llevar algún tiempo, según el tamaño de la VM y la velocidad y el ancho de banda de la conexión de red.

El progreso de la importación se muestra en la barra de estado en la parte inferior de la ventana de XenCenter y en la ficha **Registros**. Cuando la máquina virtual recién importada está disponible, aparece en el panel **Recursos**.

Para importar una VM desde XVA mediante la CLI xe:

Para importar la máquina virtual al SR predeterminado en el host de XenServer de destino, introduzca lo siguiente:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe vm-import -h hostname -u root -pw password \
    filename=pathname_of_export_file
<!--NeedCopy-->
```

Para importar la máquina virtual a un SR diferente en el host XenServer de destino, agregue el parámetro `sr-uuid` opcional:

```
xe vm-import -h hostname -u root -pw password \
    filename=pathname_of_export_file sr-uuid=uuid_of_target_sr
<!--NeedCopy-->
```

Si quiere conservar la dirección MAC de la máquina virtual original, agregue el parámetro `preserve` opcional y establezca en **`true`**:

```
xe vm-import -h hostname -u root -pw password \
    filename=pathname_of_export_file preserve=true
<!--NeedCopy-->
```

> **Nota:**
>
> La importación de una VM puede llevar algún tiempo, según el tamaño de la VM y la velocidad y el ancho de banda de la conexión de red.

Después de importar la máquina virtual, el símbolo del sistema devuelve el UUID de la máquina virtual recién importada.

Exportación de máquinas virtuales

Puede exportar archivos OVF/OVA y XVA mediante el asistente XenCenter Export; también puede exportar archivos XVA a través de la CLI xe.

Exportar máquinas virtuales como OVF/OVA

Con el asistente XenCenter Export, puede exportar una o más máquinas virtuales como un paquete OVF/OVA. Cuando exporta máquinas virtuales como un paquete OVF/OVA, los datos de configuración se exportan junto con los discos duros virtuales de cada máquina virtual.

> **Nota:**
>
> Para exportar paquetes OVF u OVA, debe iniciar sesión como raíz o tener la función de control de acceso basado en funciones (RBAC) de administrador de grupos asociada a su cuenta de usuario.

Para exportar máquinas virtuales como OVF/OVA mediante XenCenter:

1. Apague o suspenda las máquinas virtuales que quiera exportar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Abra el asistente de exportación: en el panel **Recursos**, haga clic con el botón derecho en el grupo o el host que contiene las máquinas virtuales que desea exportar y, a continuación, seleccione **Exportar**.
3. En la primera página del asistente:
   - Introduzca el nombre del archivo de exportación.
   - Especifique la carpeta en la que quiere que se guarden los archivos.
   - Seleccione **Paquete OVF/OVA (*.ovf, *.ova)** en la lista **Formato**.
   - Haga clic en **Siguiente** para continuar.
4. En la lista de máquinas virtuales disponibles, seleccione las máquinas virtuales que quiera incluir en el paquete OVF/OVA y, a continuación, haga clic en **Siguiente** para continuar.
5. Si es necesario, puede agregar al paquete un documento de acuerdo de licencia de usuario final (EULA) previamente preparado (.rtf, .txt).

   Para agregar un CLUF, haga clic en **Agregar** y busque el archivo que desea agregar. Una vez que haya agregado el archivo, puede ver el documento seleccionándolo en la lista de **archivos del CLUF** y, a continuación, haciendo clic en **Ver**.

   Los EULA pueden proporcionar los términos y condiciones legales para usar el dispositivo y las aplicaciones entregadas en el dispositivo.

   La capacidad de incluir uno o más EULA le permite proteger legalmente el software del dispositivo. Por ejemplo, si su dispositivo incluye un sistema operativo propietario en sus máquinas virtuales, es posible que quiera incluir el texto del CLUF de ese sistema operativo. Se muestra el texto y la persona que importa el dispositivo debe aceptarlo.

   > **Nota:**
   >
   > Intentar agregar archivos EULA que no están en formatos compatibles, incluidos archivos XML o binarios, puede provocar un error en la función de importación de CLUF.

   Selecciona **Siguiente** para continuar.
6. En la página **Opciones avanzadas**, especifique las opciones de manifiesto, firma y archivo de salida, o simplemente haga clic en **Siguiente** para continuar.

   a) Para crear un manifiesto para el paquete, seleccione la casilla de verificación **Crear un manifiesto**.

      El manifiesto proporciona un inventario o una lista de los demás archivos de un paquete. El manifiesto se usa para garantizar que los archivos incluidos originalmente cuando se creó el paquete sean los mismos archivos presentes cuando llega el paquete. Cuando se importan los archivos, se utiliza una suma de comprobación para verificar que los archivos no hayan cambiado desde que se creó el paquete.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

b) Para agregar una firma digital al paquete

i. Seleccione **Firmar el paquete de OVF**.

La firma digital (`.cert`) contiene la firma del archivo de manifiesto y el certificado utilizado para crear esa firma. Cuando se importa un paquete firmado, el usuario puede verificar la identidad del creador del paquete mediante la clave pública del certificado para validar la firma digital.

ii. Navegue para encontrar un certificado.

Use un certificado X.509 que ya haya creado a partir de una autoridad de confianza y que haya exportado como un archivo `.pfx`. Para certificados con exportación de resumen SHA-256 utilizando el "Proveedor criptográfico RSA y AES mejorado de Microsoft"como CSP.

iii. En **Contraseña de clave privada**, introduzca la contraseña de exportación (PFX) o, si no se proporcionó una contraseña de exportación, la clave privada asociada al certificado.

c) Para generar las máquinas virtuales seleccionadas como un único archivo (tar) en formato OVA, marque la casilla de verificación **Crear paquete OVA (archivo de exportación OVA único)**. Para obtener más información sobre los diferentes formatos de archivo, consulte Abrir formato de virtualización.

d) Para comprimir imágenes de disco duro virtual (archivos.VHD) incluidas en el paquete, seleccione la casilla Comprimir archivos OVF.

Cuando crea un paquete OVF, las imágenes de disco duro virtual se asignan, de forma predeterminada, a la misma cantidad de espacio que a la máquina virtual exportada. Por ejemplo, una máquina virtual a la que se le asignan 26 GB de espacio tiene una imagen de disco duro que consume 26 GB de espacio. La imagen del disco duro usa este espacio independientemente de si la VM lo requiere o no.

> **Nota:**
>
> La compresión de los archivos VHD hace que el proceso de exportación tarde más en completarse. La importación de un paquete que contiene archivos VHD comprimidos también lleva más tiempo, ya que el asistente de importación debe extraer todas las imágenes VHD a medida que las importa.

Si se seleccionan **Crear paquete OVA (archivo de exportación OVA único)** y **Comprimir archivos OVF**, el resultado es un archivo OVA comprimido con la extensión `.ova.gz`.

7. Revise la configuración de exportación.

Para que el asistente verifique el paquete exportado, marque la casilla **Verificar exportación al finalizar**. Haga clic en **Finalizar** para iniciar el proceso de exportación y cerrar el asistente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> La exportación de una VM puede llevar algún tiempo, según el tamaño de la VM y la velocidad y el ancho de banda de la conexión de red.

El progreso de la exportación se muestra en la barra de estado de la parte inferior de la ventana de XenCenter y en la ficha **Registros**. Para cancelar una exportación en curso, haga clic en la ficha **Registros**, busque la exportación en la lista de eventos y haga clic en el botón **Cancelar**.

Exportar máquinas virtuales como XVA Puede exportar una máquina virtual existente como un archivo XVA mediante el asistente XenCenter Export o la CLI xe. Recomendamos exportar una máquina virtual a una máquina que no sea el host de XenServer, en la que puede mantener una biblioteca de archivos de exportación. Por ejemplo, puede exportar la VM a la máquina que ejecuta XenCenter.

> **Advertencia:**
>
> Es posible que no siempre sea posible ejecutar una máquina virtual importada que se exportó desde otro host con un tipo de CPU diferente. Por ejemplo, es posible que una máquina virtual de Windows exportada desde un host con una CPU compatible con Intel VT no se ejecute cuando se importe a un host con una CPU AMD-VTM.

Para exportar máquinas virtuales como archivos XVA mediante XenCenter:

1. Apague o suspenda la VM que quiere exportar.
2. Abra el asistente de exportación: en el panel **Recursos**, haga clic con el botón derecho en la máquina virtual que desea exportar y, a continuación, seleccione **Exportar**.
3. En la primera página del asistente:
   - Introduzca el nombre del archivo de exportación.
   - Especifique la carpeta en la que quiere que se guarden los archivos.
   - Seleccione **Archivo XVA (*.xva)** en la lista **Formato**.
   - Haga clic en **Siguiente** para continuar.
4. En la lista de máquinas virtuales disponibles, seleccione la máquina virtual que desea exportar y, a continuación, haga clic en **Siguiente** para continuar.
5. Revise la configuración de exportación.

   Para que el asistente verifique el paquete exportado, marque la casilla **Verificar exportación al finalizar**. Haga clic en Finalizar para iniciar el proceso de exportación y cerrar el asistente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> La exportación de una VM puede llevar algún tiempo, según el tamaño de la VM y la velocidad y el ancho de banda de la conexión de red.

El progreso de la exportación se muestra en la barra de estado de la parte inferior de la ventana de XenCenter y en la ficha **Registros**. Para cancelar una exportación en curso, haga clic en la ficha **Registros**, busque la exportación en la lista de eventos y haga clic en el botón **Cancelar**.

Para exportar máquinas virtuales como archivos XVA mediante la CLI xe:

1. Apague la VM que quiere exportar.
2. Exporte la VM ejecutando lo siguiente:

```
xe vm-export -h hostname -u root -pw password vm=vm_name \
    filename=pathname_of_file
<!--NeedCopy-->
```

> **Nota:**
>
> Asegúrese de incluir la extensión `.xva` al especificar el nombre del archivo de exportación. Si la máquina virtual exportada no tiene esta extensión, es posible que XenCenter no reconozca el archivo como un archivo XVA válido cuando intente importarlo.

Eliminar máquinas virtuales

August 24, 2023

Puede eliminar máquinas virtuales mediante la CLI xe o XenCenter.

Al eliminar una máquina virtual (VM), se elimina su configuración y su sistema de archivos del host. Cuando elimina una VM, puede elegir eliminar o conservar cualquier disco virtual conectado a la VM, además de cualquier instantánea de la VM.

Eliminar una VM mediante la CLI xe

Para eliminar una VM:

1. Busque el UUID de VM:

```
xe vm-list
```

2. Apague la VM:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe vm-shutdown uuid=<uuid>
```

3. (Opcional) Puede elegir eliminar los discos virtuales conectados:

   a) Busque los UUID de disco virtual:

   ```
   xe vm-disk-list vm=<uuid>
   ```

   b) Elimine el disco virtual:

   ```
   xe vdi-destroy uuid=<uuid>
   ```

   > **Importante:**
   >
   > Se pierden todos los datos almacenados en las unidades de disco virtual de la VM.

4. (Opcional) Puede elegir eliminar las instantáneas asociadas a la VM:

   a) Busque los UUID de las instantáneas:

   ```
   xe snapshot-list snapshot-of=<uuid>
   ```

   b) Para eliminar cada instantánea, busque los UUID de los discos virtuales de esa instantánea:

   ```
   xe snapshot-disk-list snapshot-uuid=<uuid>
   ```

   c) Elimine cada disco de instantáneas:

   ```
   xe vdi-destroy uuid=<uuid>
   ```

   d) Elimine la instantánea:

   ```
   xe snapshot-destroy uuid=<uuid>
   ```

5. Elimine la VM:

```
xe vm-destroy uuid=<uuid>
```

Eliminar una VM mediante XenCenter

Para eliminar una VM:

1. Apague la VM.
2. Seleccione la VM detenida en el panel **Recursos**, haga clic con el botón secundario y seleccione **Eliminar** en el menú contextual. Alternativamente, en el menú **VM**, seleccione **Eliminar**.
3. Para eliminar un disco virtual conectado, seleccione su casilla de verificación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Importante:**
>
> Se pierden todos los datos almacenados en las unidades de disco virtual de la VM.

4. Para eliminar una instantánea de la VM, seleccione su casilla de verificación.
5. Haga clic en **Eliminar**.

   Cuando se completa la operación de eliminación, la VM se elimina del panel **Recursos**.

> **Nota:**
>
> Las instantáneas de VM cuya VM principal se ha eliminado (*instantáneas huérfanas*) aún se puede acceder desde el panel **Recursos**. Estas instantáneas se pueden exportar, eliminar o usar para crear máquinas virtuales y plantillas. Para ver instantáneas en el panel **Recursos**, seleccione **Objetos** en el panel de navegación y, a continuación, expanda el grupo **Instantáneas** en el panel Recursos.

vApps

August 24, 2023

Una vApp es un grupo lógico de una o más máquinas virtuales (VM) relacionadas que se pueden iniciar como una sola entidad. Cuando se inicia una vApp, las máquinas virtuales contenidas en la vApp se inician en un orden predefinido por el usuario. Esta función permite que las máquinas virtuales que dependen unas de otras se secuencien automáticamente. Un administrador ya no tiene que secuenciar manualmente el inicio de las VM dependientes cuando todo un servicio requiere el reinicio (por ejemplo, para una actualización de software). Las máquinas virtuales dentro de la vApp no tienen que residir en un host y se pueden distribuir dentro de un grupo mediante las reglas normales.

La función vApp es útil en la situación de recuperación ante desastres. Puede agrupar todas las VM que están en el mismo repositorio de almacenamiento o todas las VM que se relacionan con el mismo acuerdo de nivel de servicio (SLA).

> **Nota:**
>
> Los vApp se pueden crear y cambiar mediante XenCenter y Xe CLI. Para obtener información sobre cómo trabajar con vApps mediante la CLI, consulte Interfaz de línea de comandos.

Administrar vApps en XenCenter

El cuadro de diálogo **Administrar vApps** le permite crear, eliminar, cambiar, iniciar y cerrar vApps, e importar y exportar vApps dentro del grupo seleccionado. Si selecciona una vApp en la lista, las

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

máquinas virtuales que contiene se enumeran en el panel de detalles de la derecha.

Puede usar **Administrar vApps** para realizar las siguientes acciones:

- Para cambiar el nombre o la descripción de una vApp
- Para agregar o eliminar máquinas virtuales de la vApp
- Para cambiar la secuencia de inicio de las máquinas virtuales en la vApp

Para cambiar las vApps:

1. Seleccione el grupo y, en el menú **Grupo**, seleccione **Administrar vApps**.

   También puede hacer clic con el botón derecho en el panel **Recursos** y seleccionar **Administrar vApps** en el menú contextual.

2. Seleccione la vApp y elija **Propiedades** para abrir su cuadro de diálogo Propiedades.
3. Seleccione la ficha **General** para cambiar el nombre o la descripción de la vApp.
4. Seleccione la ficha **Máquinas virtuales** para agregar o eliminar máquinas virtuales de la vApp.
5. Seleccione la ficha **Secuencia de inicio de VM** para cambiar el orden de inicio y los valores del intervalo de demora de las VM individuales en la vApp.
6. Haga clic en **Aceptar** para guardar los cambios y cerrar **Propiedades**.

Crear vApps

Para agrupar las máquinas virtuales en una vApp, siga el procedimiento:

1. Elija el grupo y, en el menú **Agrupación**, seleccione **Administrar vApps**.
2. Escriba un nombre para la vApp y, si lo quiere, una descripción. Haga clic en **Siguiente**.

   Puede elegir el nombre que quieras, pero lo mejor es un nombre que describa la vApp. Si bien es recomendable evitar crear varias vApps que tengan el mismo nombre, no es un requisito. XenCenter no obliga a los nombres de vApp a ser únicos. No es necesario usar comillas para los nombres que incluyan espacios.

3. Elija qué máquinas virtuales desea incluir en la nueva vApp. Haga clic en **Siguiente**.

   Puede usar el campo de búsqueda para enumerar solo las máquinas virtuales que tengan nombres que incluyan la cadena de texto especificada.

4. Especifique la secuencia de inicio de las máquinas virtuales en la vApp. Haga clic en **Siguiente**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Valor	Descripción
Comenzar pedido	Especifica el orden en que se inician las VM individuales dentro de la vApp, lo que permite que ciertas VM se reinicien antes que otras. Las máquinas virtuales que tienen un valor de orden inicial de 0 (cero) se inician primero. Las máquinas virtuales que tienen un valor de orden inicial de 1 se inician a continuación. A continuación, se inician las máquinas virtuales que tienen un valor de orden inicial de 2, y así sucesivamente.
Intente iniciar la próxima máquina virtual después	Especifica cuánto tiempo se debe esperar después de iniciar la máquina virtual antes de intentar iniciar el siguiente grupo de máquinas virtuales en la secuencia de inicio. El siguiente grupo es el conjunto de máquinas virtuales que tienen un orden de inicio más bajo.

1. En la página final de **Administrar vApps**, puede revisar la configuración de vApp. Haga clic en **Anterior** para volver y cambiar cualquier configuración o en **Finalizar** para crear la vApp y cerrar **Administrar vApps**.

   > **Nota:**
   >
   > Una vApp puede abarcar varios hosts de un único grupo, pero no puede abarcar varios grupos.

Eliminar vApps

Para eliminar una vApp, siga el procedimiento:

1. Elija el grupo y, en el menú **Agrupación**, seleccione **Administrar vApps**.
2. Seleccione la vApp que quiera eliminar de la lista. Haga clic en **Eliminar**.

> **Nota:**
>
> Las máquinas virtuales de la vApp **no** se eliminan.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Iniciar y cerrar vApps mediante XenCenter

Para iniciar o cerrar una vApp, utilice **Administrar vApp, al**que se accede desde el menú **Agrupación**. Cuando inicia una vApp, todas las VM que contiene se inician automáticamente en secuencia. Los valores de orden de inicio e intervalo de demora especificados para cada máquina virtual individual controlan la secuencia de inicio. Estos valores se pueden establecer cuando se crea la vApp por primera vez. Cambie estos valores en cualquier momento desde el cuadro de diálogo Propiedades de vApp o el cuadro de diálogo Propiedades de VM individual.

Para iniciar una vApp:

1. Abra **Administrar vApps**: Elija el grupo donde se encuentran las VM de la vApp y, en el menú **Agrupación**, seleccione **Administrar vApps**. También puede hacer clic con el botón derecho en el panel **Recursos** y seleccionar **Administrar vApps** en el menú contextual.
2. Elija la vApp y haga clic en **Iniciar** para iniciar todas las máquinas virtuales que contiene.

Para cerrar una vApp:

1. Abra **Administrar vApps**: Elija el grupo donde se encuentran las VM de la vApp y, en el menú **Agrupación**, seleccione **Administrar vApps**. También puede hacer clic con el botón derecho en el panel **Recursos** y seleccionar **Administrar vApps** en el menú contextual.
2. Elija la vApp y haga clic en Apagar para **cerrar** todas las VM de la vApp.

   Se intenta un apagado suave en todas las VM. Si no es posible un apagado suave, se realiza un apagado forzado.

> **Nota:**
>
> Un apagado suave realiza un apagado correcto de la VM y todos los procesos en ejecución se detienen individualmente.
>
> Un apagado forzado realiza un apagado duro y equivale a desconectar un servidor físico. Es posible que no siempre cierre todos los procesos en ejecución. Si cierra una VM de esta manera, corre el riesgo de perder datos. Utilice un apagado forzado únicamente cuando no sea posible un apagado suave.

Importación y exportación de vApps

Las vApps se pueden importar y exportar como paquetes OVF/OVA. Para obtener más información, consulte Importación y exportación de máquinas virtuales.

Para exportar una vApp:

1. Abra **Gestionar vApps**: En el menú **Grupo**, seleccione **Administrar vApps**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Elija la vApp que quiera exportar de la lista. Haga clic en **Exportar**.
3. Siga el procedimiento descrito en Exportar máquinas virtuales como OVF/OVA.

La exportación de una vApp puede llevar algún tiempo.

Para importar una vApp:

1. Abra **Gestionar vApps**: En el menú **Grupo**, seleccione **Administrar vApps**.
2. Haga clic en **Importar** para abrir el cuadro de diálogo **Importar**.
3. Siga el procedimiento descrito en Importación de máquinas virtuales como OVF/OVA.

Una vez completada la importación, la nueva vApp aparece en la lista de vApps en **Administrar vApps**.

Notas avanzadas para máquinas virtuales

January 17, 2024

En esta sección se proporcionan algunas notas avanzadas para máquinas virtuales.

Comportamiento de arranque

Hay dos opciones para el comportamiento de la VDI de una máquina virtual cuando se inicia la VM:

> **Nota:**
>
> La VM debe apagarse antes de que pueda cambiar su configuración de comportamiento de arranque.

Persistir

> **Consejo:**
>
> Utilice este comportamiento de arranque si aloja escritorios virtuales Citrix que son máquinas estáticas o dedicadas.

Este comportamiento es el predeterminado en el arranque de VM. La VDI se deja en el estado en que se encontraba en el último cierre.

Seleccione esta opción si va a permitir que los usuarios realicen cambios permanentes en sus escritorios. Para seleccionar persistir, apague la VM y, a continuación, introduzca el siguiente comando:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe vdi-param-set uuid=vdi_uuid on-boot=persist
<!--NeedCopy-->
```

Restablecer

> **Consejo:**
>
> Utilice este comportamiento de arranque si aloja escritorios virtuales Citrix que son máquinas compartidas o asignadas de forma aleatoria.

En el arranque de la VM, la VDI se revierte al estado en el que se encontraba en el arranque anterior. Los cambios realizados mientras la VM está en ejecución se pierden la próxima vez que se inicia la VM.

Seleccione esta opción si planea entregar escritorios estandarizados que los usuarios no puedan cambiar permanentemente. Para seleccionar restablecer, apague la VM y, a continuación, introduzca el siguiente comando:

> **Advertencia:**
>
> Después de cambiar `on-boot=reset`, los datos guardados en la VDI se descartan después del siguiente apagado/inicio o reinicio.

Poner la biblioteca ISO a disposición de los hosts de XenServer

Para que una biblioteca ISO esté disponible para los hosts de XenServer, cree un directorio compartido NFS o SMB/CIFS externo. El servidor NFS o SMB/CIFS debe permitir el acceso raíz al recurso compartido. Para recursos compartidos NFS, permita el acceso estableciendo el indicador `no_root_squash` cuando cree la entrada de recurso compartido en `/etc/exports` en el servidor NFS.

A continuación, utilice XenCenter para adjuntar la biblioteca ISO o conéctese a la consola host y ejecute el comando:

```
xe-mount-iso-sr host:/volume
<!--NeedCopy-->
```

Para un uso avanzado, puede pasar argumentos adicionales al comando mount.

Para hacer que un recurso compartido SMB/CIFS de Windows esté disponible para el host, use XenCenter o conéctese a la consola del host y ejecute el siguiente comando:

```
xe-mount-iso-sr unc_path -t cifs -o username=myname/myworkgroup
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Reemplace las barras diagonales hacia atrás en el argumento `unc_path` con barras diagonales hacia adelante. Por ejemplo:

```
xe-mount-iso-sr //server1/myisos -t cifs -o username=johndoe/mydomain
<!--NeedCopy-->
```

Después de montar el recurso compartido, todas las ISO disponibles están disponibles en la lista **Instalar desde la biblioteca ISO o la unidad de DVD** de XenCenter. Estas ISO también están disponibles como imágenes de CD desde los comandos de la CLI.

Adjunte la ISO a una plantilla de Windows apropiada.

Conectarse a una VM de Windows mediante Escritorio remoto

Puede usar una de las siguientes formas de ver una consola de VM de Windows, las cuales admiten el uso completo del teclado y el mouse.

- Uso de XenCenter. Este método proporciona una consola gráfica estándar y utiliza la tecnología VNC integrada en XenServer para proporcionar acceso remoto a la consola de la máquina virtual.
- Conexión mediante Escritorio remoto de Windows. Este método utiliza la tecnología de Protocolo de escritorio remoto

En XenCenter, en la ficha **Consola**, hay un botón **Cambiar a escritorio remoto**. Este botón inhabilita la consola gráfica estándar de XenCenter y cambia al uso de Escritorio remoto.

Si no tiene habilitado Escritorio remoto en la máquina virtual, este botón está inhabilitado. Para habilitarlo, instale XenServer VM Tools para Windows. Siga el procedimiento que se indica a continuación para activarlo en cada máquina virtual que quiera conectar mediante Escritorio remoto.

Para habilitar el escritorio remoto en una máquina virtual de Windows:

1. Abra **Sistema** haciendo clic en el botón **Inicio**, haga clic con el botón secundario en **Equipo**y, a continuación, seleccione **Propiedades**.
2. Haga clic en **Configuración remota**. Si se le pide una contraseña de administrador, escriba la contraseña que creó durante la configuración de la VM.
3. En el área **Escritorio remoto**, haga clic en la casilla de verificación etiquetada **Permitir conexiones desde equipos que ejecutan cualquier versión de Escritorio remoto**.
4. Para seleccionar cualquier usuario que no sea administrador y que pueda conectarse a esta máquina virtual de Windows, haga clic en el botón **Seleccionar usuarios remotos** y proporcione los nombres de usuario. Los usuarios con privilegios de administrador en el dominio de Windows pueden conectarse de forma predeterminada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ahora puede conectarse a esta VM mediante Escritorio remoto. Para obtener más información, consulte el artículo de Microsoft Knowledge Base, Conectarse a otro equipo mediante Conexión a Escritorio remoto.

> **Nota:**
>
> No puede conectarse a una máquina virtual que esté inactiva o en hibernación. Establezca la configuración de suspensión e hibernación en el equipo remoto en **Nunca**.

Gestión del tiempo en máquinas virtuales de Windows

Para los invitados de Windows, inicialmente el reloj de dominio de control controla el tiempo. La hora se actualiza durante las operaciones del ciclo de vida de las máquinas virtuales, como suspender y reiniciar. Recomendamos ejecutar un servicio NTP fiable en el dominio de control y en todas las máquinas virtuales de Windows.

Si configuras manualmente una VM para que esté dos horas por delante del dominio de control, persiste. Puede adelantar la máquina virtual mediante un desplazamiento de zona horaria dentro de la máquina virtual. Si más tarde cambia la hora del dominio de control (ya sea manualmente o por NTP), la VM cambia en consecuencia, pero mantiene el desplazamiento de dos horas. Cambiar la zona horaria del dominio de control no afecta a las zonas horarias ni al desplazamiento de la VM. XenServer usa la configuración de reloj de hardware de la VM para sincronizarla. XenServer no usa la configuración del reloj del sistema de la VM.

Al realizar operaciones de suspensión y reanudación o al realizar una migración en vivo, asegúrese de tener instaladas las herramientas de máquina virtual de XenServer para Windows actualizadas. XenServer VM Tools para Windows notifica al kernel de Windows que se requiere una sincronización horaria después de reanudarla (posiblemente en un host físico diferente).

> **Nota:**
>
> Si ejecuta máquinas virtuales de Windows en un entorno de Citrix Virtual Desktops, debe asegurarse de que el reloj del host tenga el mismo origen que el dominio de Active Directory (AD). Si no se sincronizan los relojes, las máquinas virtuales pueden mostrar una hora incorrecta y provocar que los controladores de Windows PV se bloqueen.

Gestión del tiempo en máquinas virtuales Linux

Además del comportamiento definido por XenServer, la configuración y los comportamientos del sistema operativo pueden afectar el comportamiento de gestión del tiempo de las máquinas virtuales Linux. Algunos sistemas operativos Linux pueden sincronizar periódicamente el reloj del sistema y el reloj del hardware, o el sistema operativo puede usar su propio servicio NTP de forma predeter-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

minada. Para obtener más información, consulte la documentación del sistema operativo de su VM Linux.

> **Nota:**
>
> Al instalar una nueva VM de Linux, asegúrese de cambiar la zona horaria de la UTC predeterminada a su valor local. Para obtener instrucciones de distribución específicas, consulte Notas de la versión de Linux.

Los relojes de hardware de las máquinas virtuales de Linux **no** se sincronizan con el reloj que se ejecuta en el dominio de control y se pueden modificar. Cuando la VM se inicia por primera vez, la hora del dominio de control se usa para establecer la hora inicial del reloj de hardware y el reloj del sistema.

Si cambia la hora en el reloj de hardware, este cambio persiste cuando se reinicia la VM.

El comportamiento del reloj del sistema depende del sistema operativo de la VM. Para obtener más información, consulte la documentación del sistema operativo de su VM.

No puede cambiar este comportamiento de gestión del tiempo de XenServer.

Instalar máquinas virtuales desde medios del kit de opciones de revendedor (bloqueado por BIOS)

Hay dos tipos de VM: BIOS genéricas y BIOS personalizadas. Para habilitar la instalación de versiones OEM de Windows del Reseller Option Kit (bloqueado por BIOS) en una máquina virtual, copie las cadenas de BIOS de la máquina virtual desde el host con el que se suministró el medio. Como alternativa, los usuarios avanzados pueden establecer valores definidos por el usuario en las cadenas del BIOS.

BIOS genérico

La máquina virtual tiene cadenas de BIOS de XenServer genéricas.

> **Nota:**
>
> Si una máquina virtual no tiene cadenas de BIOS configuradas cuando se inicia, se insertan en ella las cadenas de BIOS estándar de XenServer y la máquina virtual pasa a ser genérica para BIOS.

BIOS personalizado

Puede personalizar la BIOS de dos maneras: cadenas de BIOS Copy-Host y cadenas de BIOS definidas por el usuario.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Después de iniciar una VM por primera vez, no puede cambiar sus cadenas de BIOS. Asegúrese de que las cadenas del BIOS sean correctas antes de iniciar la VM por primera vez.

Cadenas de BIOS Copy-Host La máquina virtual tiene una copia de las cadenas de BIOS de un host concreto del grupo. Para instalar los medios bloqueados con BIOS que vienen con el host, siga los procedimientos que se indican a continuación.

Con XenCenter:

1. Haga clic en la casilla de verificación **Copiar cadenas de BIOS del host a la VM** en el Asistente para nuevas VM.

Mediante la interfaz de línea de comandos:

1. Ejecute el comando `vm-install copy-bios-strings-from`. Especifique `host-uuid` como host desde el que se copian las cadenas (es decir, el host con el que se suministró el medio):

```
xe vm-install copy-bios-strings-from=host uuid \
    template=template name sr-name-label=name of sr \
    new-name-label=name for new VM
<!--NeedCopy-->
```

   Este comando devuelve el UUID de la máquina virtual recién creada.

   Por ejemplo:

```
xe vm-install copy-bios-strings-from=46dd2d13-5aee-40b8-ae2c-95786
   ef4 \
    template="win7sp1" sr-name-label=Local\ storage  \
    new-name-label=newcentos
    7cd98710-bf56-2045-48b7-e4ae219799db
<!--NeedCopy-->
```

2. Si las cadenas de BIOS relevantes del host se han copiado correctamente en la VM, el comando `vm-is-bios-customized` confirma este éxito:

```
xe vm-is-bios-customized uuid=VM uuid
<!--NeedCopy-->
```

   Por ejemplo:

```
xe vm-is-bios-customized uuid=7cd98710-bf56-2045-48b7-e4ae219799db
    This VM is BIOS-customized.
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Cuando inicia la VM, se inicia en el host físico desde el que copió las cadenas de BIOS.

> **Advertencia:**
>
> Es su responsabilidad cumplir con cualquier EULA que rija el uso de cualquier sistema operativo bloqueado por BIOS que instale.

Cadenas BIOS definidas por el usuario El usuario tiene la opción de establecer valores personalizados en cadenas de BIOS seleccionadas mediante CLI/API. Para instalar el medio en una máquina virtual con BIOS personalizada, siga el procedimiento que se indica a continuación.

Mediante la interfaz de línea de comandos:

1. Ejecute el comando `vm-install` (sin `copy-bios-strings-from`):

```
xe vm-install template=template name sr-name-label=name of sr \
      new-name-label=name for new VM
<!--NeedCopy-->
```

   Este comando devuelve el UUID de la máquina virtual recién creada.

   Por ejemplo:

```
xe vm-install template="win7sp1" sr-name-label=Local\ storage  \
      new-name-label=newcentos
    7cd98710-bf56-2045-48b7-e4ae219799db
<!--NeedCopy-->
```

2. Para establecer cadenas de BIOS definidas por el usuario, ejecute el siguiente comando antes de iniciar la VM por primera vez:

```
xe vm-param-set uuid=VM_UUID bios-strings:bios-vendor=VALUE \
    bios-strings:bios-version=VALUE bios-strings:system-
       manufacturer=VALUE \
    bios-strings:system-product-name=VALUE bios-strings:system-
       version=VALUE \
    bios-strings:system-serial-number=VALUE bios-strings:enclosure
       -asset-tag=VALUE
<!--NeedCopy-->
```

   Por ejemplo:

```
xe vm-param-set uuid=7cd98710-bf56-2045-48b7-e4ae219799db \
    bios-strings:bios-vendor="vendor name" \
    bios-strings:bios-version=2.4 \
    bios-strings:system-manufacturer="manufacturer name" \
    bios-strings:system-product-name=guest1 \
    bios-strings:system-version=1.0 \
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    bios-strings:system-serial-number="serial number" \
    bios-strings:enclosure-asset-tag=abk58hr
<!--NeedCopy-->
```

> **Notes:**
>
> - Una vez que las cadenas de BIOS definidas por el usuario se configuran en una sola llamada a CLI o API, no se pueden modificar.
> - Puede decidir el número de parámetros que quiere proporcionar para establecer las cadenas de BIOS definidas por el usuario.

> **Advertencia:**
>
> Es su responsabilidad:
>
> - Cumpla con los CLUF y los estándares para los valores que se establecen en el BIOS de la VM.
> - Asegúrese de que los valores que proporciona para los parámetros sean parámetros de trabajo. Proporcionar parámetros incorrectos puede provocar un error en la instalación de arranque/medios.

Asignar una GPU a una VM de Windows (para usarla con Citrix Virtual Desktops)

XenServer le permite asignar una GPU física en el host de XenServer a una máquina virtual Windows que se ejecuta en el mismo host. Esta función de transferencia de GPU beneficia a los usuarios avanzados de gráficos, como los diseñadores de CAD, que requieren capacidades gráficas de alto rendimiento. Solo se admite para su uso con Citrix Virtual Desktops.

Si bien XenServer solo admite una GPU para cada máquina virtual, detecta y agrupa automáticamente las GPU físicas idénticas en los hosts del mismo grupo. Una vez asignada a un grupo de GPU, se puede iniciar una VM en cualquier host del grupo que tenga una GPU disponible en el grupo. Cuando se conecta a una GPU, una VM tiene ciertas funciones que ya no están disponibles, como la migración en vivo, las instantáneas de VM con memoria y la suspensión/reanudación.

La asignación de una GPU a una máquina virtual de un grupo no interfiere con el funcionamiento de otras máquinas virtuales del grupo. Sin embargo, las VM con GPU conectadas se consideran no ágiles. Si las VM con GPU conectadas son miembros de un grupo con alta disponibilidad habilitada, ambas funciones pasan por alto estas VM. Las VM no se pueden migrar automáticamente.

La transferencia de GPU se puede habilitar mediante XenCenter o la CLI xe.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Requisitos

El paso a través de GPU es compatible con máquinas y GPU específicas. En todos los casos, la función de chipset IOMMU (conocida como VT-d para los modelos Intel) debe estar disponible y habilitada en el host XenServer. Antes de habilitar la función de transferencia de GPU, visita la Lista de compatibilidad de hardware.

Antes de asignar una GPU a una VM

Antes de asignar una GPU a una máquina virtual, coloque las GPU físicas adecuadas en el host de XenServer y, a continuación, reinicie la máquina. Tras el reinicio, XenServer detecta automáticamente cualquier GPU física. Para ver todas las GPU físicas en los hosts del grupo, utilice el comando `xe pgpu-list`.

Asegúrese de que la función del chipset IOMMU está habilitada en el host. Para hacerlo, introduzca lo siguiente:

```
xe host-param-get uuid=uuid_of_host param-name=chipset-info param-key=
    iommu
<!--NeedCopy-->
```

Si el valor impreso es **`false`**, IOMMU no está habilitada y el paso a través de GPU no está disponible mediante el host XenServer especificado.

Para asignar una GPU a una VM de Windows mediante XenCenter:

1. Apague la VM a la que quiere asignar una GPU.
2. Abra las propiedades de VM: haga clic con el botón secundario en la VM y seleccione **Propiedades**
3. Asignar una GPU a la VM: seleccione GPU en la lista de propiedades de VM y, a continuación, seleccione un tipo de GPU. Haga clic en **Aceptar**.
4. Inicie la VM.

Para asignar una GPU a una VM de Windows mediante la CLI xe:

1. Apague la máquina virtual que quiere asignar un grupo de GPU mediante el comando `xe vm-shutdown`.
2. Busque el UUID del grupo de GPU al introducir lo siguiente:

   ```
   xe gpu-group-list
   <!--NeedCopy-->
   ```

   Este comando imprime todos los grupos de GPU del grupo. Anote el UUID del grupo de GPU apropiado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Conecte la VM a un grupo de GPU al introducir lo siguiente:

```
xe vpgu-create gpu-group-uuid=uuid_of_gpu_group vm-uuid=uuid_of_vm
<!--NeedCopy-->
```

   Para asegurarse de que se ha adjuntado el grupo de GPU, ejecute el comando `xe vgpu-list`.

4. Inicie la máquina virtual mediante el comando `xe vm-start`.

5. Una vez que se inicie la VM, instale los controladores de la tarjeta gráfica en la VM.

   La instalación de los controladores es esencial, ya que la VM tiene acceso directo al hardware del host. El proveedor de hardware proporciona los controladores.

> **Nota:**
>
> Si intenta iniciar una máquina virtual con transferencia de GPU en el host sin una GPU disponible en el grupo de GPU correspondiente, XenServer muestra un error.

Para desconectar una VM Windows de una GPU mediante XenCenter:

1. Apague la VM.
2. Abra las propiedades de VM: haga clic con el botón secundario en la VM y seleccione **Propiedades**
3. Separar la GPU de la VM: seleccione **GPU** en la lista de propiedades de VM y, a continuación, seleccione **Ninguno** como el tipo de GPU. Haga clic en **Aceptar**.
4. Inicie la VM.

Para desconectar una VM Windows de una GPU mediante la CLI xe:

1. Apague la VM mediante el comando `xe vm-shutdown`.
2. Busque el UUID de la vGPU conectada a la VM al introducir lo siguiente:

```
xe vgpu-list vm-uuid=uuid_of_vm
<!--NeedCopy-->
```

3. Separe la GPU de la VM al introducir lo siguiente:

```
xe vgpu-destroy uuid=uuid_of_vgpu
<!--NeedCopy-->
```

4. Inicie la máquina virtual mediante el comando `xe vm-start`.

Crea imágenes ISO

XenServer puede usar imágenes ISO como medios de instalación y fuentes de datos para máquinas virtuales Windows o Linux. En esta sección se describe cómo crear imágenes ISO a partir de CD/DVD.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para crear una ISO en un sistema Linux:

1. Coloque el disco CD o DVD-ROM en la unidad. Asegúrese de que el disco no esté montado. Para comprobarlo, ejecute el comando:

   ```
   mount
   <!--NeedCopy-->
   ```

   Si el disco está montado, desmóntelo. Consulte la documentación del sistema operativo para obtener ayuda si es necesario.

2. Como root, ejecute el comando

   ```
   dd if=/dev/cdrom of=/path/cdimg_filename.iso
   <!--NeedCopy-->
   ```

   Este comando lleva algún tiempo. Cuando la operación se completa correctamente, verá algo así como:

   ```
   1187972+0 records in
   1187972+0 records out
   <!--NeedCopy-->
   ```

   Su archivo ISO está listo.

Para crear una ISO en un sistema Windows:

Los equipos Windows no tienen un comando de sistema operativo equivalente para crear una ISO. La mayoría de las herramientas de grabación de CD tienen una forma de guardar un CD como archivo ISO.

Habilitar VNC para máquinas virtuales Linux

February 23, 2024

Es posible que las VM no estén configuradas para admitir Virtual Network Computing (VNC), que XenServer usa para controlar las VM de forma remota, de forma predeterminada. Antes de poder conectarse con XenCenter, asegúrese de que el servidor VNC y un administrador de pantallas X estén instalados en la máquina virtual y configurados correctamente. En esta sección se describe cómo configurar VNC en cada una de las distribuciones de sistemas operativos Linux compatibles para permitir interacciones adecuadas con XenCenter.

Para máquinas virtuales basadas en CentOS, use las instrucciones para las máquinas virtuales basadas en Red Hat a continuación, ya que usan el mismo código base para proporcionar acceso gráfico a VNC. CentOS *X* se basa en Red Hat Enterprise Linux *X*.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Habilitar una consola gráfica en las VM de Debian

> **Nota:**
>
> Antes de habilitar una consola gráfica en su máquina virtual Debian, asegúrese de haber instalado las herramientas de máquinas virtuales de XenServer para Linux. Para obtener más información, consulte Instalación de XenServer VM Tools para Linux.

La consola gráfica para las máquinas virtuales de Debian la proporciona un servidor VNC que se ejecuta dentro de la VM. En la configuración recomendada, un administrador de pantalla estándar controla la consola para que se proporcione un cuadro de diálogo de inicio de sesión.

1. Instale su huésped Debian con los paquetes del sistema de escritorio, o instale GDM (el administrador de visualización) usando apt (siguiendo los procedimientos estándar).
2. Instale el servidor Xvnc mediante`apt-get` (o similar):

```
apt-get install vnc4server
<!--NeedCopy-->
```

> **Nota:**
>
> El entorno gráfico de escritorio de Debian, que utiliza el demonio Gnome Display Manager versión 3, puede llevar mucho tiempo de CPU. Desinstale el paquete `gdm3` Gnome Display Manager e instale el paquete `gdm` de la siguiente manera:

```
apt-get install gdm
apt-get purge gdm3
<!--NeedCopy-->
```

3. Configure una contraseña de VNC (no tenerla supone un grave riesgo de seguridad) mediante el comando `vncpasswd`. Pase un nombre de archivo en el que escribir la información de la contraseña. Por ejemplo:

```
vncpasswd /etc/vncpass
<!--NeedCopy-->
```

4. `Modifique sugdm.confarchivo (/etc/gdm/gdm.conf) para configurar un servidor VNC para administrar la visualización0mediante la extensión[servers]y[daemon]secciones de la siguiente manera:`

```
    [servers]
    0=VNC
    [daemon]
    VTAllocation=false
    [server-VNC]
    name=VNC
    command=/usr/bin/Xvnc -geometry 800x600 -PasswordFile /etc/
       vncpass BlacklistTimeout=0
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    flexible=true
<!--NeedCopy-->
```

5. Reinicie GDM y espere a que XenCenter detecte la consola gráfica:

```
/etc/init.d/gdm restart
<!--NeedCopy-->
```

> **Nota:**
>
> Puede comprobar que el servidor VNC se está ejecutando mediante un comando como`ps ax | grep vnc`.

Habilite una consola gráfica en VM de Red Hat, CentOS u Oracle Linux

> **Nota:**
>
> Antes de configurar las máquinas virtuales de Red Hat para VNC, asegúrese de haber instalado las herramientas de máquinas virtuales de XenServer para Linux. Para obtener más información, consulte Instalación de XenServer VM Tools para Linux.

Para configurar VNC en las VM de Red Hat, modifique la configuración de GDM. La configuración de GDM se mantiene en un archivo cuya ubicación varía según la versión de Red Hat Linux que esté utilizando. Antes de modificarlo, primero determine la ubicación de este archivo de configuración. Este archivo se modifica en varios procedimientos posteriores de esta sección.

Determine la ubicación del archivo de configuración de VNC

Si utiliza Red Hat Linux, el archivo de configuración de GDM es `/etc/gdm/custom.conf`. Este archivo es un archivo de configuración dividido que contiene solo valores especificados por el usuario que anulan la configuración predeterminada. Este tipo de archivo se usa de forma predeterminada en las versiones más recientes de GDM. Se incluye en estas versiones de Red Hat Linux.

Configurar GDM para usar VNC

1. Como root en la CLI de texto de la VM, ejecute el comando `rpm -q vnc-server gdm`. Los nombres de los paquetes `vnc-server` y `gdm` aparecen, con sus números de versión especificados.

   Los nombres de paquetes que se muestran indican los paquetes que ya están instalados. Si ve un mensaje que indica que un paquete no está instalado, es posible que no haya seleccionado las opciones de escritorio gráfico durante la instalación. Instale estos paquetes antes de poder

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

continuar. Para obtener detalles sobre la instalación de más software en su VM, consulte la Guía de instalación de Red Hat Linux x86 apropiada.

2. Abra el archivo de configuración de GDM con su editor de texto preferido y agregue las siguientes líneas al archivo:

```
    [server-VNC]
    name=VNC Server
    command=/usr/bin/Xvnc -SecurityTypes None -geometry 1024x768 -
       depth 16 \
    -BlacklistTimeout 0
    flexible=true
<!--NeedCopy-->
```

   Con los archivos de configuración en Red Hat Linux, agregue estas líneas a la sección `[servers]` vacía.

3. Modifique la configuración para que se utilice el servidor `Xvnc` en lugar del servidor X estándar:

   - `0=Standard`

     Modifíquelo para que diga:

     `0=VNC`

   - Si está utilizando Red Hat Linux, agregue la línea anterior justo debajo de la sección `[servers]` y antes de la sección `[server-VNC]`.

4. Guarde el archivo y ciérrelo.

Reinicie GDM para que el cambio en la configuración surta efecto, ejecutando el comando `/usr/sbin/gdm-restart`.

> **Nota:**
>
> Red Hat Linux usa el nivel de ejecución 5 para el inicio gráfico. Si la instalación se inicia en el nivel de ejecución 3, cambie esta configuración para que se inicie el administrador de pantalla y obtenga acceso a una consola gráfica. Para obtener más información, consulte Comprobar niveles de ejecución.

Parámetros de firewall

La configuración del firewall de forma predeterminada no permite el paso del tráfico de VNC. Si tiene un firewall entre la máquina virtual y XenCenter, permita el tráfico a través del puerto que usa la conexión VNC. De forma predeterminada, un servidor VNC escucha las conexiones de un visor VNC en el puerto TCP `5900 + n`, donde `n` es el número de visualización (normalmente cero). Por lo tanto, una

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

configuración de servidor VNC para Display-0 escucha en el puerto TCP `5900`, Display-1 `TCP-5901`, y así sucesivamente. Consulte la documentación del firewall para asegurarse de que estos puertos estén abiertos. Para obtener más información, consulte Puertos de comunicación utilizados por XenServer.

Si quiere utilizar el seguimiento de la conexión IP o limitar el inicio de las conexiones a un solo lado, configure aún más el firewall.

Para configurar el firewall VMS basado en Red Hat para abrir el puerto VNC:

1. Para Red Hat Linux, utilice `system-config-securitylevel-tui`.
2. Seleccione **Personalizar** y agregue `5900` a la lista de otros puertos.

Alternativamente, puede inhabilitar el firewall hasta el próximo reinicio ejecutando el comando`service iptables stop`o ejecutando permanentemente`chkconfig iptables off`. Esta configuración puede exponer los servicios adicionales al mundo exterior y reducir la seguridad general de su VM.

Resolución de pantalla VNC

Después de conectarse a una VM con la consola gráfica, la resolución de la pantalla a veces no coincide. Por ejemplo, la pantalla de la VM es demasiado grande para caber cómodamente en el panel de la consola gráfica. Para controlar este comportamiento, configure el parámetro `geometry` del servidor VNC de la siguiente manera:

1. Abra el archivo de configuración de GDM con su editor de texto preferido. Para obtener más información, consulte Determinar la ubicación del archivo de configuración de VNC.
2. Encuentre la sección `[server-VNC]` que agregó antes.
3. Modifique la línea de comandos para leer, por ejemplo:

   ```
   command=/usr/bin/Xvnc -SecurityTypes None -geometry 800x600
   <!--NeedCopy-->
   ```

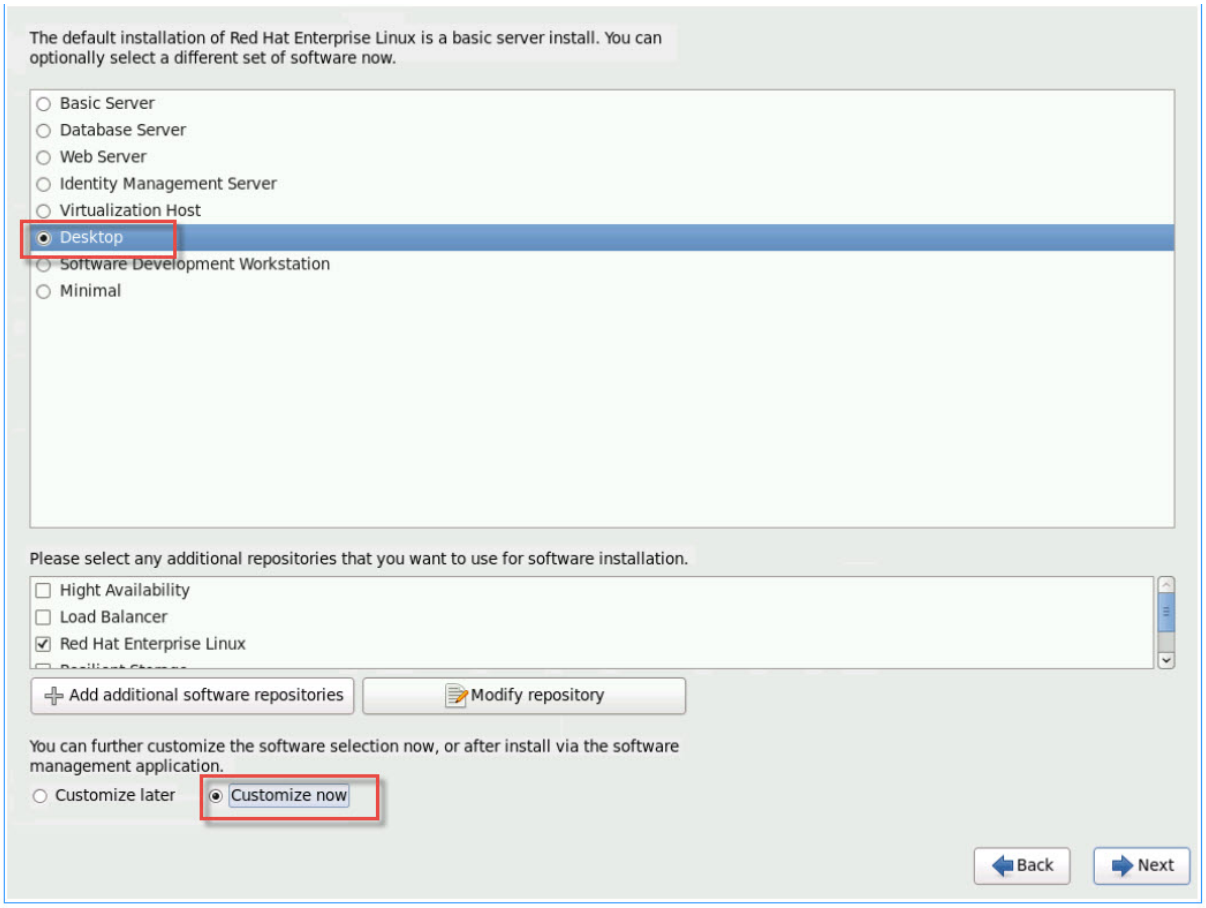
   El valor del parámetro `geometry` puede ser cualquier ancho y alto de pantalla válidos.
4. Guarde el archivo y ciérrelo.

Habilitar VNC para máquinas virtuales de RHEL, CentOS u OEL

Si utiliza Red Hat Linux, el archivo de configuración de GDM es `/etc/gdm/custom.conf`. Este archivo es un archivo de configuración dividido que contiene solo valores especificados por el usuario que anulan la configuración predeterminada. De forma predeterminada, este tipo de archivo se usa en las versiones más recientes de GDM y se incluye en estas versiones de Red Hat Linux.

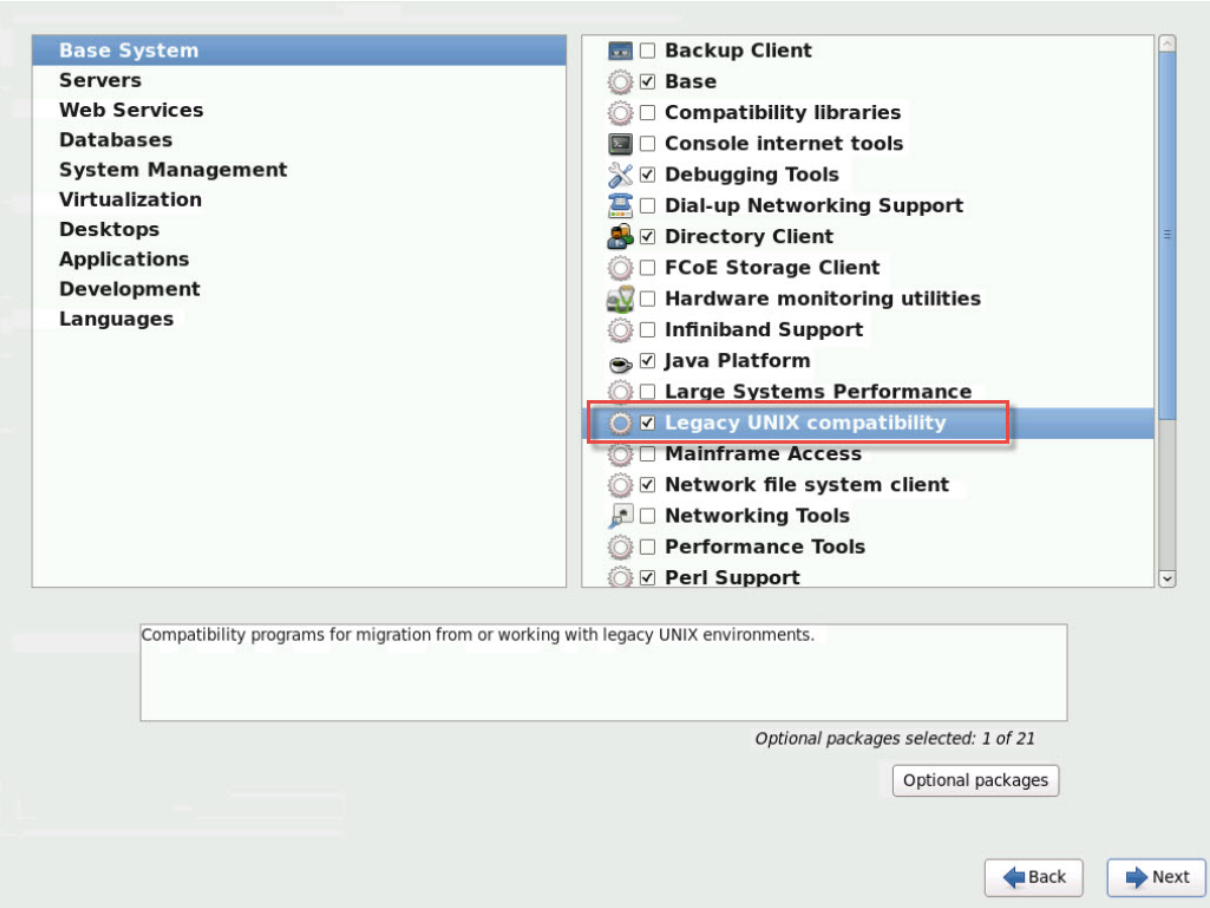
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Durante la instalación del sistema operativo, seleccione el modo **Escritorio**. En la pantalla de instalación de RHEL, seleccione **Escritorio** > **Personalizar ahora** y, a continuación, haga clic en **Siguiente**:



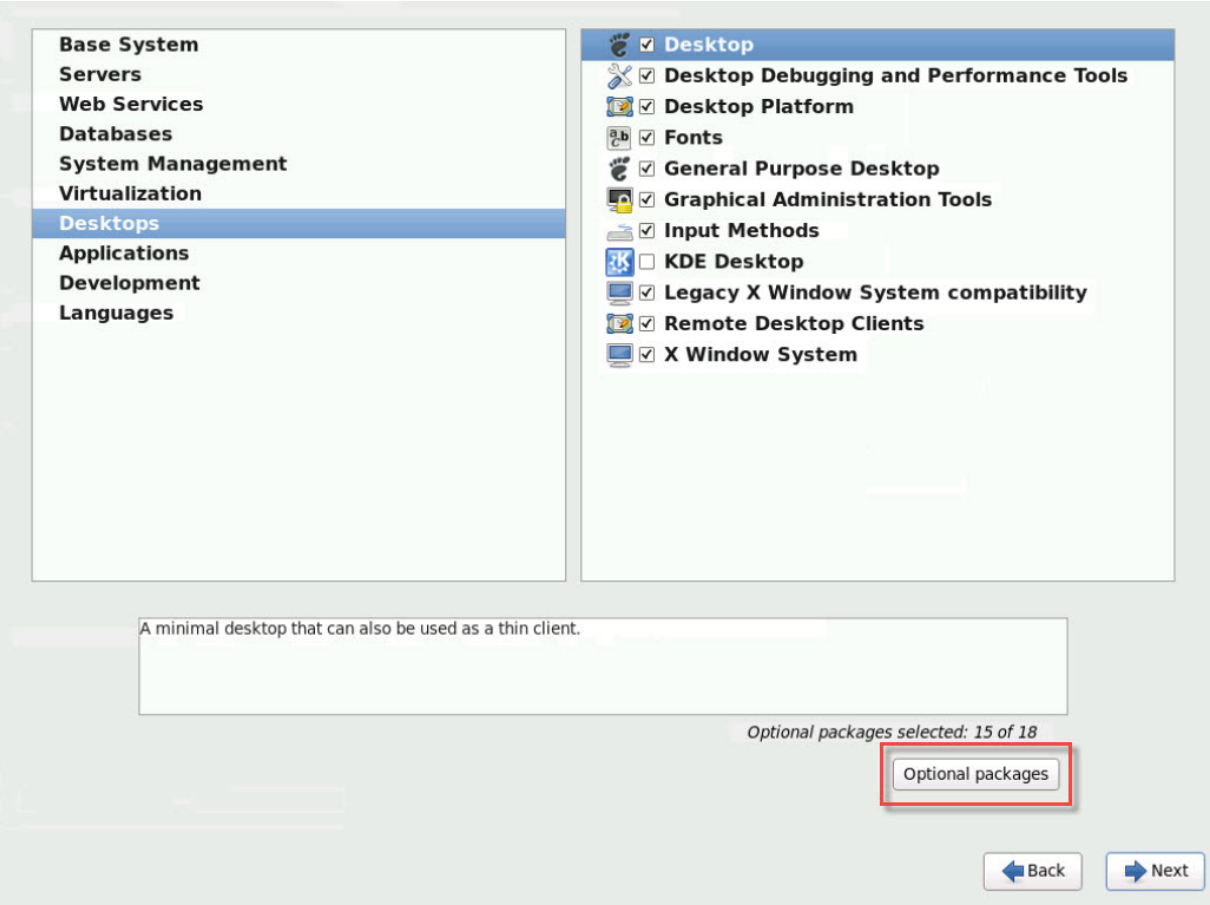
Esta acción muestra la pantalla Sistema base, asegúrese de que la **compatibilidad con UNIX heredado** esté seleccionada:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



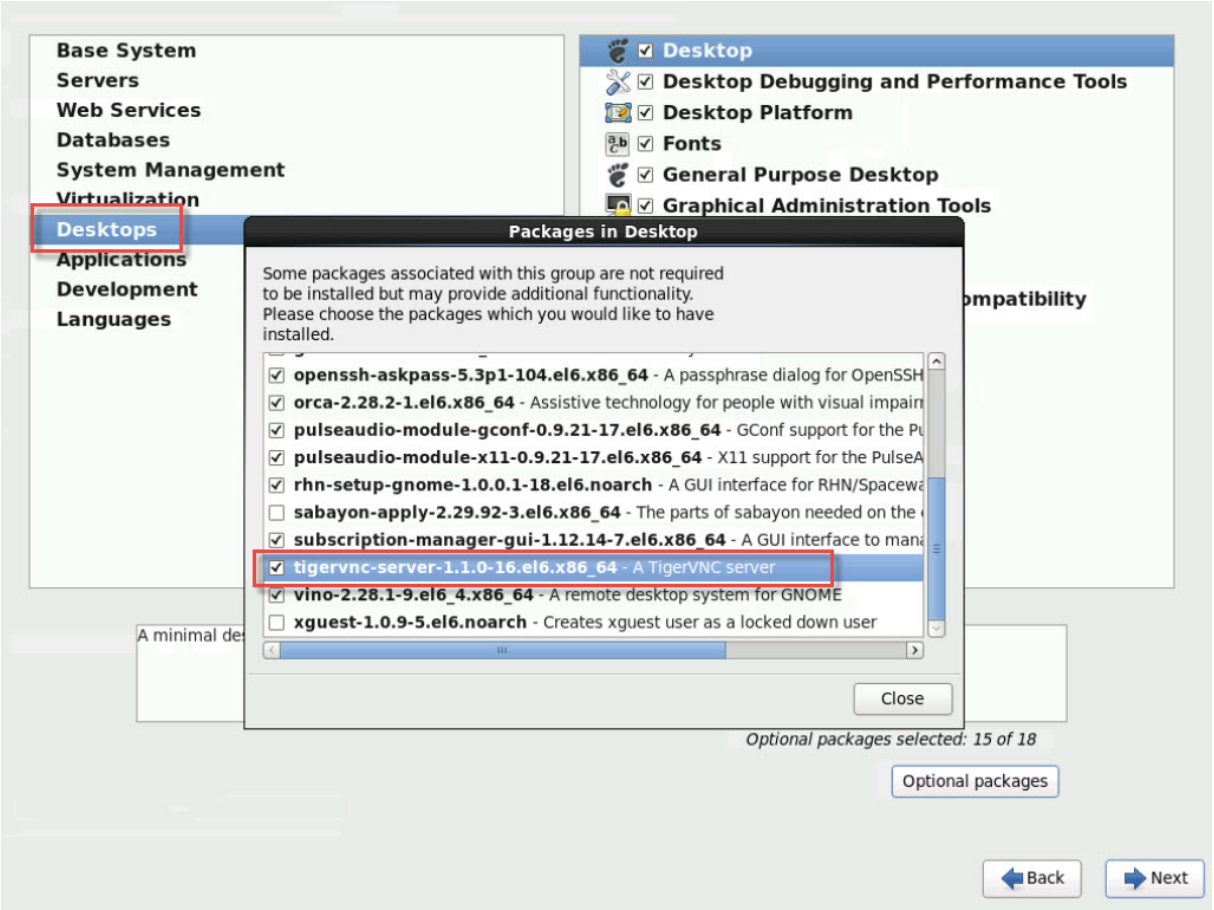
Seleccione **Escritorios** > **Paquetes opcionales**y haga clic en **Siguiente**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Esta acción muestra la ventana **Paquetes en el escritorio**, seleccione **tigervnc-server-<número_de_versión>** y, a continuación, haga clic en **Siguiente**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Realice los siguientes pasos para continuar con la configuración de sus máquinas virtuales de RHEL:

1. Abra el archivo de configuración de GDM con su editor de texto preferido y agregue las siguientes líneas a las secciones correspondientes:

```
    [security]
    DisallowTCP=false

    [xdmcp]
    Enable=true
<!--NeedCopy-->
```

2. Cree el archivo `/etc/xinetd.d/vnc-server-stream`:

```
    service vnc-server
    {

                    id = vnc-server
                disable = no
                   type = UNLISTED
                   port = 5900
             socket_type = stream
                   wait = no
                   user = nobody
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                group = tty
               server = /usr/bin/Xvnc
          server_args = -inetd -once -query localhost -
              SecurityTypes None \
          -geometry 800x600 -depth 16
      }

<!--NeedCopy-->
```

3. Escriba el siguiente comando para iniciar el servicio `xinetd`:

```
# service xinetd start
<!--NeedCopy-->
```

4. Abra el archivo `/etc/sysconfig/iptables`. Agregue la siguiente línea por encima de la línea que dice `-A INPUT -j REJECT --reject-with icmp-host-prohibited`:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 5900 -j ACCEPT
<!--NeedCopy-->
```

5. Escriba el siguiente comando para reiniciar `iptables`:

```
# service iptables restart
<!--NeedCopy-->
```

6. Escriba el siguiente comando para reiniciar `gdm`:

```
    # telinit 3
    # telinit 5
<!--NeedCopy-->
```

> **Nota:**
>
> Red Hat Linux usa el nivel de ejecución 5 para el inicio gráfico. Si la instalación se inicia en el nivel de ejecución 3, cambie esta configuración para que se inicie el administrador de pantalla y obtenga acceso a una consola gráfica. Para obtener más información, consulte Comprobar los niveles de ejecución.

Configurar máquinas virtuales basadas en SLES para VNC

> **Nota:**
>
> Antes de configurar las máquinas virtuales de SUSE Linux Enterprise Server para VNC, asegúrese de haber instalado las herramientas de máquinas virtuales de XenServer para Linux. Consulte Instalar las herramientas de máquina virtual de XenServer para Linux para obtener más información.

SLES es compatible con la habilitación de “Administración remota”como opción de configuración en `YaST`. Puede seleccionar habilitar la Administración remota en el momento de la instalación,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

disponible en la pantalla **Servicios de red** del instalador de SLES. Esta función le permite conectar un visor VNC externo a su invitado para que pueda ver la consola gráfica. El método para usar la función de administración remota de SLES es ligeramente diferente del método que proporciona XenCenter. Sin embargo, es posible modificar los archivos de configuración en la máquina virtual SUSE Linux para que se integre con la función de consola gráfica.

Comprobar si hay un servidor VNC

Antes de realizar cambios en la configuración, compruebe que tiene un servidor VNC instalado. SUSE envía el servidor `tightvnc` de forma predeterminada. Este servidor es un servidor VNC adecuado, pero también puede utilizar la distribución RealVNC estándar.

Puede comprobar que tiene instalado el software `tightvnc` mediante el comando:

```
rpm -q tightvnc
<!--NeedCopy-->
```

Habilitar la administración remota

Si la administración remota no se habilitó durante la instalación del software de SLES, puede habilitarla de la siguiente manera:

1. Abra una consola de texto en la VM y ejecute la utilidad `YaST`:

   ```
   yast
   <!--NeedCopy-->
   ```

2. Use las teclas de flecha para seleccionar **Servicios de red** en el menú de la izquierda. **Haga clic** en el menú de la derecha y utilice las teclas de flecha para seleccionar **Administración remota**. Presiona **Entrar** .

3. En la pantalla **Administración remota**, presione **Tab** para ir a la sección **Configuración de administración remota**. Utilice las teclas de flecha para seleccionar **Permitir administración remota** y pulse **Entrar** para colocar una X en la casilla de verificación.

4. **Vaya** a la sección **Configuración del firewall**. Utilice las teclas de flecha para seleccionar **Abrir puerto en el firewall** y presione **Entrar** para colocar una X en la casilla de verificación.

5. **Vaya** al botón **Finalizar** y presione **Entrar**.

6. Se muestra un cuadro de mensaje que le indica que reinicie el administrador de pantalla para que la configuración surta efecto. Presione **Entrar** para confirmar el mensaje.

7. `YaST` aparece el menú original de nivel superior de. Presione la tecla **Tab** hasta llegar a **Salir** y presione **Entrar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Modificar la configuración `xinetd`

Después de habilitar la Administración remota, modifique un archivo de configuración si quiere permitir la conexión de XenCenter. Como alternativa, use un cliente VNC de terceros.

1. Abra el archivo `/etc/xinetd.d/vnc` en su editor de texto preferido.
2. El archivo contiene secciones como las siguientes:

```
    service vnc1
    {

    socket_type = stream
    protocol    = tcp
    wait        = no
    user        = nobody
    server      = /usr/X11R6/bin/Xvnc
    server_args = :42 -inetd -once -query localhost -geometry 1024
       x768 -depth 16
    type        = UNLISTED
    port        = 5901
     }

<!--NeedCopy-->
```

3. Modificar la línea `port` para leerla

```
port = 5900
<!--NeedCopy-->
```

4. Guarde el archivo y ciérrelo.
5. Reinicie el administrador de pantalla y el servicio `xinetd` con los siguientes comandos:

```
/etc/init.d/xinetd restart
rcxdm restart
<!--NeedCopy-->
```

SUSE Linux utiliza el nivel de ejecución 5 para el inicio gráfico. Si el escritorio remoto no aparece, compruebe que la máquina virtual esté configurada para iniciarse en el nivel de ejecución 5. Para obtener más información, consulte Comprobar niveles de ejecución.

Parámetros de firewall

De forma predeterminada, la configuración del firewall no permite el paso del tráfico de VNC. Si tiene un firewall entre la máquina virtual y XenCenter, permita el tráfico a través del puerto que usa la conexión VNC. De forma predeterminada, un servidor VNC escucha las conexiones de un visor VNC en el puerto TCP `5900 + n`, donde `n` es el número de visualización (normalmente cero). Por lo tanto, una

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

configuración de servidor VNC para Display-0 escucha en el puerto TCP 5900, Display-1 TCP-5901 , y así sucesivamente. Consulte la documentación del firewall para asegurarse de que estos puertos estén abiertos. Para obtener más información, consulte Puertos de comunicación utilizados por XenServer.

Si quiere utilizar el seguimiento de la conexión IP o limitar el inicio de las conexiones a un solo lado, configure aún más el firewall.

Para abrir el puerto VNC en el firewall de VM de SLES 11.x:

1. Abra una consola de texto en la VM y ejecute la utilidad YaST:

```
yast
<!--NeedCopy-->
```

2. Use las teclas de flecha para seleccionar **Seguridad y Usuarios** en el menú de la izquierda. **Haga clic** en el menú de la derecha y utilice las teclas de flecha para seleccionar **Firewall**. Presiona **Entrar** .
3. En la pantalla **Firewall**, utilice las teclas de flecha para seleccionar **Reglas personalizadas** en el menú de la izquierda y, a continuación, presione **Entrar**.
4. **Vaya** al botón **Agregar** en la sección **Reglas permitidas personalizadas** y, a continuación, presione **Entrar**.
5. En el campo **Red de origen**, escriba *0/0*. **Vaya** al campo **Puerto de destino** e introduzca *5900*.
6. **Vaya** al botón **Agregar** y, a continuación, presione **Entrar**.
7. Presione la tecla**Tab** hasta el botón **Siguiente** y presione **Entrar**.
8. En la pantalla **Resumen**, **vaya** al botón **Finalizar** y presione **Entrar**.
9. En la pantalla YaST de nivel superior **Ficha**, vaya al botón **Salir** y presione **Entrar**.
10. Reinicie el administrador de pantalla y el servicio `xinetd` con los siguientes comandos:

```
/etc/init.d/xinetd restart
rcxdm restart
<!--NeedCopy-->
```

Alternativamente, puede inhabilitar el firewall hasta el próximo reinicio ejecutando el comando **rcSuSEfirewall2 stop**, o de forma permanente mediante YaST. Esta configuración puede exponer los servicios adicionales al mundo exterior y reducir la seguridad general de su VM.

Resolución de pantalla VNC

Después de conectarse a una máquina virtual con la consola gráfica, la resolución de la pantalla a veces no coincide. Por ejemplo, la pantalla de la VM es demasiado grande para caber cómodamente en el

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

panel de la consola gráfica. Para controlar este comportamiento, configure el parámetro `geometry` del servidor VNC de la siguiente manera:

1. Abra el archivo `/etc/xinetd.d/vnc` con su editor de texto preferido y busque la sección `service_vnc1` (correspondiente a `displayID` 1).
2. Modifique el argumento `geometry` de la línea `server-args` con la resolución de visualización deseada. Por ejemplo,

   ```
   server_args  = :42 -inetd -once -query localhost -geometry 800x600
       -depth 16
   <!--NeedCopy-->
   ```

   El valor del parámetro `geometry` puede ser cualquier ancho y alto de pantalla válidos.
3. Guarde el archivo y ciérrelo.
4. Reinicie el servidor VNC:

   ```
   /etc/init.d/xinetd restart
   rcxdm restart
   <!--NeedCopy-->
   ```

Comprobar niveles de ejecución

Las VM de Red Hat y SUSE Linux usan el nivel de ejecución 5 para el inicio gráfico. En esta sección se describe cómo verificar que la VM se inicia en el nivel de ejecución 5 y cómo cambiar esta configuración.

1. Compruebe `/etc/inittab` en qué se establece el nivel de ejecución predeterminado. Busque la línea que dice:

   ```
   id:n:initdefault:
   <!--NeedCopy-->
   ```

   Si *n* no es 5, modifique el archivo para hacerlo así.
2. Puede ejecutar el comando `telinit q ; telinit 5` después de este cambio para evitar tener que reiniciar para cambiar los niveles de ejecución.

Solucionar problemas de VM

August 24, 2023

XenServer ofrece dos formas de soporte:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Soporte de autoayuda gratuito en el sitio web de XenServer
- Servicios de soporte de pago, que puede comprar en el sitio de soporte.

Con el soporte técnico de XenServer, puede abrir un caso de soporte en línea o ponerse en contacto con el centro de soporte por teléfono si tiene dificultades técnicas.

El sitio de soporte de XenServer alberga varios recursos que pueden serle útiles si experimenta un comportamiento inusual, bloqueos u otros problemas. Los recursos incluyen: foros de soporte, artículos de la base de conocimientos y documentación del producto.

Si observa un comportamiento inusual de la VM, esta sección tiene como objetivo ayudarlo a resolver el problema. En esta sección se describe dónde se encuentran los registros de las aplicaciones y otra información que puede ayudar a su proveedor de soluciones de XenServer a rastrear y resolver el problema.

> **Importante:**
>
> Siga la información de solución de problemas de esta sección únicamente bajo la supervisión de su proveedor de soluciones de XenServer o del equipo de soporte.
>
> Actualizaciones de proveedores: mantenga sus máquinas virtuales actualizadas con las actualizaciones del sistema operativo suministradas por el proveedor. Es posible que el proveedor haya proporcionado correcciones para fallas de VM y otras fallas.

La VM se bloquea

Si experimenta fallas de VM, es posible que un volcado de memoria del kernel pueda ayudar a identificar el problema. Reproduzca el bloqueo, si es posible, y siga este procedimiento. Consulte a su proveedor de SO invitado para obtener más información sobre este problema.

El comportamiento de crashdump de las máquinas virtuales se puede controlar mediante el parámetro `actions-after-crash`. Los valores posibles son los siguientes:

Valor	Descripción
`preserve`	Deje la VM en estado de pausa. (Para análisis)
`restart`	Sin volcado de memoria, reinicie la VM. (Este es el valor predeterminado)
`destroy`	Sin volcado de memoria, deje la VM detenida.

Para habilitar el almacenamiento de los volcados de fallos de máquinas virtuales:

1. En el host XenServer, determine el UUID de la máquina virtual deseada ejecutando el siguiente comando:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe vm-list name-label=<name> params=uuid --minimal
<!--NeedCopy-->
```

2. Cambie el valor `actions-after-crash` mediante `xe vm-param-set`; por ejemplo, ejecute el siguiente comando en dom0:

```
xe vm-param-set uuid=<vm_uuid> actions-after-crash=preserve
<!--NeedCopy-->
```

3. Bloquee la VM.

   a) Determine el ID de dominio de la máquina virtual ejecutando el siguiente comando en dom0:

```
xe vm-param-get uuid=<vm_uuid> param-name=dom-id
<!--NeedCopy-->
```

   b) Ejecute el comando `xl trigger` en dom0 para provocar el bloqueo:

```
xl trigger <dom_id> nmi
<!--NeedCopy-->
```

Comportamiento de crashdump de máquinas virtuales de Windows

De forma predeterminada, los volcados de memoria de Windows se colocan en `%SystemRoot%\Minidump` en la propia máquina virtual de Windows. Puede configurar el nivel de volcado de máquinas virtuales siguiendo la ruta de menú **Mi PC > Propiedades > Avanzado > Inicio y recuperación**.

Problemas de UEFI y Secure Boot

¿Cómo cambio la resolución de pantalla de la consola de XenCenter en una máquina virtual habilitada para UEFI?

Para cambiar la resolución de pantalla de la consola de XenCenter en una máquina virtual habilitada para UEFI:

1. Abra la **configuración de Windows**.
2. Haga clic en el botón **Actualización y seguridad**.
3. En la ficha de recuperación, presiona el botón **Reiniciar ahora**.
4. Vaya a **Solucionar problemas** > **Opciones avanzadas** > **Configuración del firmware UEFI**.
5. Presiona **Reiniciar**. Durante el reinicio, se carga el menú de configuración de UEFI.
6. Vaya a **Device Manager** > **Configuración de plataforma OVMF**. Muestra la resolución de pantalla actual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

7. Presione **Entrar** para ver las opciones de resolución de pantalla.
8. Use las teclas de flecha para seleccionar la resolución de pantalla deseada y presione **Entrar**.
9. Presione **F10** para guardar los cambios y confirmar su elección.
10. Reinicie la VM para ver la consola de XenCenter en una resolución de pantalla actualizada.

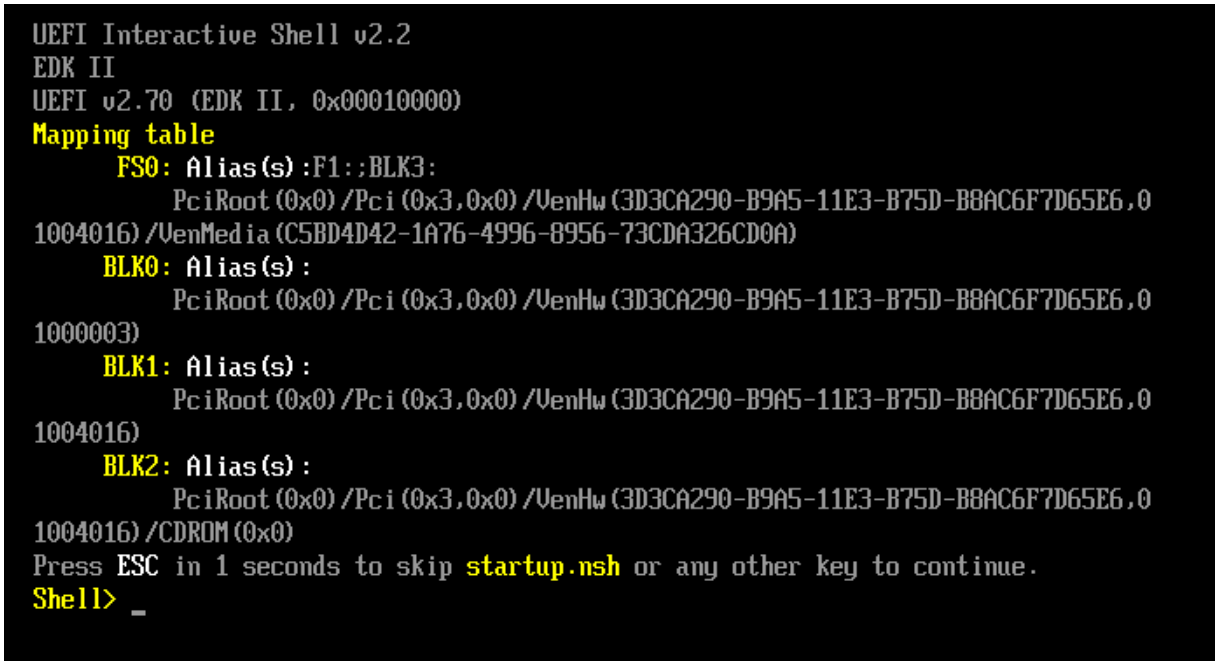
¿Por qué no puedo crear una VM de arranque seguro UEFI?

Compruebe que el sistema operativo de su máquina virtual admita el modo de arranque seguro UEFI. Los siguientes sistemas operativos admiten el arranque seguro:

- Windows 10 (64 bits)
- Windows 11 (64 bits)
- Windows Server 2016 (64 bits)
- Windows Server 2019 (64 bits)
- Windows Server 2022 (64 bits)

¿Por qué mi máquina virtual de arranque seguro UEFI no se inicia?

Si ve los siguientes mensajes en la consola de su máquina virtual de arranque seguro UEFI y una alerta en XenCenter, el proceso de arranque seguro falló y la máquina virtual no se inicia.



Esto suele deberse a la instalación de controladores sin firmar en la VM. Investigue qué controladores se han actualizado o instalado desde el último arranque seguro correcto.

Puede inhabilitar el arranque seguro e iniciar la máquina virtual en modo de configuración para eliminar los controladores sin firmar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Importante:**
>
> Antes de hacerlo, haga una copia de seguridad de la VM tomando una instantánea.

Para convertir una máquina virtual de arranque seguro UEFI en una máquina virtual de arranque UEFI, ejecute el siguiente comando en el host de XenServer que aloja la máquina virtual:

```
varstore-sb-state <VM_UUID> setup
```

Después de haber reparado la VM, ejecute el siguiente comando para volver a habilitar el arranque seguro:

```
varstore-sb-state <VM_UUID> user
```

¿Secure Boot está causando problemas en mi máquina virtual?

Para diagnosticar si un problema en la máquina virtual se debe a que el arranque seguro está activado para la máquina virtual, desactive el arranque seguro e intente reproducir el problema.

Para deshabilitar el arranque seguro, ejecute el siguiente comando en el host de XenServer que aloja la máquina virtual:

```
varstore-sb-state <VM_UUID> setup
```

Después de depurar el problema, puede ejecutar el siguiente comando para volver a habilitar el arranque seguro:

```
varstore-sb-state <VM_UUID> user
```

¿Cómo ejecuto el depurador de Windows en una máquina virtual Windows de arranque seguro?

No puede ejecutar la depuración de Windows en una máquina virtual Windows de arranque seguro. Para ejecutar la depuración de Windows en su máquina virtual, puede hacer una de las siguientes cosas:

- Cambie su VM al modo de arranque UEFI ejecutando el siguiente comando:

  ```
  xe vm-param-set uuid=<UUID> platform:secureboot=false
  ```

  Reinicie la máquina virtual.

  Después de depurar el problema, puede ejecutar el siguiente comando para volver a habilitar el arranque seguro:

  ```
  xe vm-param-set uuid=<UUID> platform:secureboot=auto
  ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Reinicie la máquina virtual.

- Para deshabilitar el arranque seguro, ejecute el siguiente comando en el host de XenServer que aloja la máquina virtual:

```
varstore-sb-state <VM_UUID> setup
```

Después de depurar el problema, puede ejecutar el siguiente comando para volver a habilitar el arranque seguro:

```
varstore-sb-state <VM_UUID> user
```

¿Por qué solo aparecen dos NIC en mi máquina virtual de Windows habilitada para UEFI?

Incluso si configuró más de dos NIC cuando creó su VM habilitada para UEFI, cuando la VM se inicia por primera vez, solo verá dos NIC. Una vez instaladas las herramientas de máquina virtual de XenServer para Windows en la máquina virtual, esta información se muestra correctamente.

¿Por qué mis dispositivos emulados se muestran como tipos diferentes de los esperados en una máquina virtual UEFI de Windows?

Las máquinas virtuales UEFI Secure Boot utilizan NVME y E1000 para los dispositivos emulados. Sin embargo, cuando la VM se inicia por primera vez, los dispositivos emulados se muestran como tipos diferentes. Una vez instaladas las herramientas de máquina virtual de XenServer para Windows en la máquina virtual, esta información se muestra correctamente.

¿Por qué no puedo convertir mis plantillas del modo BIOS al modo de arranque seguro UEFI o UEFI?

Solo puede crear una plantilla de máquina virtual habilitada para UEFI a partir de una plantilla suministrada con XenServer.

No utilice el comando `xe template-param-set` para plantillas que tengan algo instalado ni para plantillas que haya creado a partir de una instantánea. El modo de arranque de estas instantáneas no se puede cambiar y, si intenta cambiar el modo de arranque, la VM no arranca.

¿Cómo compruebo las variables de arranque seguro UEFI y UEFI?

En el host de XenServer donde está alojada la máquina virtual UEFI o UEFI Secure Boot, ejecute los siguientes comandos:

```
varstore-ls
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Este comando enumera los GUID y los nombres de las variables disponibles. Use el GUID y el nombre en el siguiente comando:

```
varstore-get <VM\_ID> <GUID> <name> | hexdump -C
```

¿Por qué no puedo usar un controlador de "prueba"con una máquina virtual de arranque seguro?

Si también trabajas con un tercero para depurar y solucionar problemas en su máquina virtual de arranque seguro UEFI, el proveedor externo podría proporcionar controladores sin firmar para fines de prueba o verificación. Estos controladores no funcionan en una máquina virtual de arranque seguro UEFI.

Solicita un conductor firmado por un tercero. O bien, puede cambiar su máquina virtual de arranque seguro UEFI al modo de configuración para que se ejecute con el controlador sin firmar.

Utilidad Xentop

La utilidad xentop muestra información en tiempo real sobre un sistema XenServer y los dominios en ejecución en un formato semigráfico. Puede utilizar esta herramienta para investigar el estado del dominio asociado a una máquina virtual.

Para ejecutar la utilidad xentop:

1. **Conéctese al host de XenServer a través de SSH o, en XenCenter, vaya a la pestaña Consola del host.**
2. Ejecute el siguiente comando: `xentop`

   La consola muestra información sobre el host en una tabla. La información se actualiza periódicamente.

Columnas de salida

La utilidad xentop muestra las siguientes columnas en la consola:

- **NOMBRE**: El nombre del dominio. «Domain-0"es el dominio de control de XenServer. Otros dominios pertenecen a las máquinas virtuales.
- **ESTADO**: El estado del dominio. El estado puede tener uno de los siguientes valores:
  - d: El dominio está muriendo
  - s —el dominio se está cerrando
  - b: El dominio está bloqueado

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - c: El dominio se ha cerrado de forma inesperada
  - p —el dominio está en pausa
  - r: El dominio se ejecuta activamente en una de las CPU

- **CPU (segundos)**: El uso de la CPU del dominio en segundos
- **CPU (%)**: El uso de CPU del dominio como porcentaje
- **MEM (k)**: El uso actual de memoria del dominio en KiB
- **MEM (%)**: El uso de memoria actual del dominio como porcentaje
- **MAXMEM (k)**: El uso máximo de memoria de dominio en KiB
- **MAXMEM (%)**: El uso máximo de memoria del dominio como porcentaje
- **VCPUS**: La cantidad de CPU virtuales asignadas al dominio
- **NETS**: La cantidad de redes virtuales utilizadas por el dominio
- **NETTX (k)**: La cantidad total de tx de la red en KiB
- **NETRX (k)**: La cantidad total de rx de red en KiB
- **VBDS**: La cantidad de dispositivos de bloques virtuales
- **VBD_OO**: El número total de veces que el VBD ha detectado un error de falta de solicitudes. Cuando eso ocurre, las solicitudes de E/S para el VBD se retrasan.
- **VBD_RD**: El número total de solicitudes de lectura de VBD
- **VBD_WR**: El número total de solicitudes de escritura de VBD
- **VBD_RSECT**: Los sectores de lectura de VBD
- **VBD_WSECT**: Los sectores de escritura de VBD

Parámetros de Xentop

Puede utilizar los siguientes parámetros para configurar la salida del comando xentop:

- **-h**: Muestra la ayuda del comando xentop.
- **-V**: Muestra la versión del comando xentop.
- **-d** o –**delay=SECONDS**: Establece el número de segundos entre actualizaciones
- **-n** o –**networks**: Genera los datos de cada red VIF asociada a un dominio
- **-x** o –**vbds**: Genera los datos de cada dispositivo de bloque VBD asociado a un dominio
- **-r** o **repeat-header**: Repite el encabezado de la tabla antes de cada dominio
- **-v** o –**vcpus**: Genera los datos de cada vCPU asociada a un dominio
- **-i** o –**iterations**: Número de iteraciones (actualizaciones) que se mostrarán antes de que xentop salga

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **-f** o –**full-name**: Muestra el nombre de dominio completo en lugar de un nombre truncado

También puede configurar la mayoría de estos parámetros desde la utilidad xentop.

---

layout: doc
description: Configure high availability in your XenServer pool to ensure that VMs continue to run in the case of disrupted networking or host hardware failures.—

Alta disponibilidad

La alta disponibilidad es un conjunto de funciones automáticas diseñadas para planificar y recuperarse de forma segura de los problemas que provocan el cierre de los hosts de XenServer o los hacen inaccesibles. Por ejemplo, durante fallos de hardware de host o redes interrumpidas físicamente.

Información general

La alta disponibilidad garantiza que, si un host se vuelve inaccesible o inestable, las máquinas virtuales que se ejecutan en ese host se reinicien automáticamente de forma segura en otro host. Esto elimina la necesidad de que las máquinas virtuales se reinicien manualmente, lo que reduce al mínimo el tiempo de inactividad de las máquinas virtuales.

Cuando el coordinador de grupos se vuelve inaccesible o inestable, la alta disponibilidad también puede recuperar el control administrativo de un grupo. La alta disponibilidad garantiza que el control administrativo se restaure automáticamente sin ninguna intervención manual.

De manera opcional, la alta disponibilidad también puede automatizar el proceso de reinicio de las máquinas virtuales en hosts que se sabe que están en buen estado sin intervención manual. Estas máquinas virtuales se pueden programar para que se reinicien en grupos para dar tiempo a iniciar los servicios. Permite que las máquinas virtuales de infraestructura se inicien antes que las máquinas virtuales dependientes (por ejemplo, un servidor DHCP antes que su servidor SQL dependiente).

> **Advertencias:**
>
> Utilice la alta disponibilidad junto con el almacenamiento de rutas múltiples y las redes conectadas. Configure el almacenamiento de rutas múltiples y las redes conectadas antes de intentar configurar la alta disponibilidad. Los clientes que no configuran el almacenamiento de rutas múltiples y las redes conectadas pueden ver un comportamiento inesperado de reinicio del host (autodelimitación) cuando hay una inestabilidad en la infraestructura.
>
> Todas las soluciones gráficas (NVIDIA vGPU, Intel GVT-D, Intel GVT-G y vGPU pass-Through) se

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> pueden utilizar en un entorno que utilice alta disponibilidad. Sin embargo, las máquinas virtuales que usan estas soluciones de gráficos no se pueden proteger con alta disponibilidad. Estas máquinas virtuales se pueden reiniciar según el mejor esfuerzo mientras haya hosts con los recursos gratuitos adecuados.

Comprometerse en exceso

Un grupo se compromete en exceso cuando las máquinas virtuales que se están ejecutando actualmente no se pueden reiniciar en otro lugar después de una cantidad de errores de host definida por el usuario. La sobreasignación puede ocurrir si no hay suficiente memoria libre en el grupo para ejecutar esas máquinas virtuales después de un error. Sin embargo, también hay cambios más sutiles que pueden hacer que la alta disponibilidad sea insostenible: los cambios en los dispositivos de bloques virtuales (VBD) y en las redes pueden afectar a las máquinas virtuales que se pueden reiniciar y en qué hosts. XenServer no puede comprobar todas las posibles acciones y determinar si infringen las exigencias de alta disponibilidad. Sin embargo, se envía una notificación asíncrona si la alta disponibilidad se vuelve insostenible.

XenServer mantiene de forma dinámica un plan de conmutación por error que detalla qué hacer cuando un conjunto de hosts de un grupo falla en un momento dado. Un concepto importante que hay que entender es el `host failures to tolerate` valor, que se define como parte de la configuración de alta disponibilidad. El valor de `host failures to tolerate` determina la cantidad de errores de host que se permiten y, al mismo tiempo, se pueden reiniciar todas las máquinas virtuales protegidas. Por ejemplo, considere un grupo de recursos que consta de 64 hosts y `host failures to tolerate` se establece en 3. En este caso, el grupo calcula un plan de conmutación por error que permite que tres hosts fallen y, a continuación, reinicie las máquinas virtuales en otros hosts. Si no se puede encontrar un plan, se considera que la agrupación está comprometida en exceso. El plan se recalcula dinámicamente en función de las operaciones y el movimiento del ciclo de vida de la VM Si los cambios (por ejemplo, la adición de nuevas máquinas virtuales al grupo) provocan que el grupo se comprometa en exceso, las alertas se envían a través de XenCenter o por correo electrónico.

Aviso de sobrecompromiso

Si algún intento de iniciar o reanudar una máquina virtual provoca que el grupo se comprometa en exceso, se muestra una alerta de advertencia en XenCenter. A continuación, puede optar por cancelar la operación o continuar de todos modos. Al continuar, el grupo se compromete en exceso y se envía un mensaje a cualquier dirección de correo electrónico configurada. También está disponible como instancia de mensaje a través de la API de administración. La cantidad de memoria que utilizan las máquinas virtuales de diferentes prioridades se muestra en los niveles de host y grupo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Esgrima host

A veces, un host puede fallar debido a la pérdida de conectividad de la red o cuando se produce un problema con la pila de control. En esos casos, el host de XenServer se autocontrola para garantizar que las máquinas virtuales no se ejecuten en dos hosts simultáneamente. Cuando se realiza una acción de protección, el host se reinicia de forma inmediata y abrupta, lo que provoca que todas las máquinas virtuales que se estén ejecutando en él se detengan. Los demás hosts detectan que las máquinas virtuales ya no se están ejecutando y, a continuación, las máquinas virtuales se reinician según las prioridades de reinicio que se les hayan asignado. El host protegido entra en una secuencia de reinicio y, cuando se reinicia, intenta volver a unirse al grupo de recursos.

> **Nota:**
>
> Los hosts de los grupos agrupados también pueden autoprotegerse cuando no pueden comunicarse con más de la mitad de los demás hosts del grupo de recursos. Para obtener más información, consulte Grupos agrupados.

Requisitos de configuración

Para utilizar la función de alta disponibilidad, necesita:

- Grupo de XenServer (esta función proporciona alta disponibilidad a nivel de host dentro de un único grupo de recursos).

  > **Nota:**
  >
  > Se recomienda habilitar la alta disponibilidad solo en grupos que contengan al menos 3 hosts XenServer. Para obtener más información, consulte CTX129721: Comportamiento de alta disponibilidad cuando se pierde el latido en un grupo.

- Almacenamiento compartido, que incluye al menos un LUN iSCSI, NFS o Fibre Channel de 356 MB o superior: El *SR latido*. El mecanismo de alta disponibilidad crea dos volúmenes en la SR de latido:

  - Volumen de latido cardíaco de 4 MB: se usa para proporcionar latidos cardíacos.
  - Volumen de metadatos de 256 MB: para almacenar los metadatos del coordinador del grupo que se utilizarán en caso de que se produzca una conmutación por error del coordinador del grupo.

  > **Nota:**
  >
  > Anteriormente, recomendábamos utilizar un repositorio de almacenamiento NFS o iSCSI dedicado como disco de latido de alta disponibilidad. Sin embargo, esto solo es beneficioso si el repositorio de almacenamiento no comparte recursos en el dispositivo de alma-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> cenamiento subyacente; de lo contrario, simplemente aumenta la complejidad y el uso de los recursos en el dominio de control (dom0) del host.
>
> Si su grupo es un grupo agrupado, su SR de latido debe ser un SR GFS2.
>
> El almacenamiento conectado mediante SMB o iSCSI cuando se autentica mediante CHAP no se puede usar como SR de latido.

- Direcciones IP estáticas para todos los hosts.

  > **Advertencia:**
  >
  > Si la dirección IP de un host cambia mientras la alta disponibilidad está habilitada, la alta disponibilidad supone que la red del host ha fallado. El cambio en la dirección IP puede cercar el host y dejarlo en un estado de no arranque. Para solucionar esta situación, inhabilite la alta disponibilidad mediante el comando `host-emergency-ha-disable`, restablezca el coordinador del grupo mediante y `pool-emergency-reset-master`, a continuación, vuelva a habilitar la alta disponibilidad.

- Para obtener la máxima fiabilidad, le recomendamos que utilice una interfaz de enlace dedicada como red de administración de alta disponibilidad.

Para que una VM esté protegida por una alta disponibilidad, debe ser ágil. Esto significa que la máquina virtual:

- Debe tener sus discos virtuales en un almacenamiento compartido. Puede usar cualquier tipo de almacenamiento compartido. El LUN iSCSI, NFS o Fibre Channel solo es necesario para el latido del almacenamiento y se puede usar para el almacenamiento en disco virtual.
- Puede utilizar la migración en vivo.
- No tiene configurada una conexión a una unidad de DVD local.
- Tiene sus interfaces de red virtuales en redes de todo el grupo.

Además, las máquinas virtuales con un vTPM adjunto no se pueden proteger con alta disponibilidad.

> **Nota:**
>
> Cuando la alta disponibilidad está habilitada, recomendamos encarecidamente utilizar una interfaz de administración integrada en los hosts del grupo y un almacenamiento con múltiples rutas para el Heartbeat SR.

Si crea VLAN e interfaces enlazadas desde la CLI, es posible que no estén conectadas y activas a pesar de haber sido creadas. En esta situación, una VM puede parecer que no es ágil y no está protegida por una alta disponibilidad. Puede usar el comando de la interfaz de línea de comandos `pif-plug` para

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

activar la VLAN y los PIF de enlace, de modo que la VM pueda volverse ágil. También puede determinar con precisión por qué una VM no es ágil mediante el comando `xe diagnostic-vm-status` de la CLI. Este comando analiza sus restricciones de posición y puede tomar medidas correctivas si es necesario.

Reiniciar la configuración

Las máquinas virtuales se pueden considerar protegidas, con el mejor esfuerzo o desprotegidas por la alta disponibilidad. El valor de `ha-restart-priority` define si una VM se trata como protegida, con el mejor esfuerzo o sin protección. El comportamiento de reinicio de las VM en cada una de estas categorías es diferente.

Protegido

La alta disponibilidad garantiza reiniciar una VM protegida que se desconecta o cuyo host se desconecta, siempre que el grupo no se comprometa en exceso y la VM sea ágil.

Si una máquina virtual protegida no se puede reiniciar cuando falla un host, High Availability intenta iniciar la máquina virtual cuando hay capacidad adicional en un grupo. Los intentos de iniciar la VM cuando hay capacidad adicional ahora pueden tener éxito.

`ha-restart-priority` Valor: `restart`

Mejor esfuerzo

Si el host de una máquina virtual con el mejor esfuerzo se desconecta, la alta disponibilidad intenta reiniciar la máquina virtual con el mejor esfuerzo en otro host. Hace este intento solo después de que todas las VM protegidas se hayan reiniciado correctamente. La alta disponibilidad solo hace un intento de reiniciar una VM con el mejor esfuerzo. Si este intento falla, la alta disponibilidad no hace más intentos de reiniciar la VM.

`ha-restart-priority` Valor: `best-effort`

Sin protección

Si se detiene una máquina virtual desprotegida o el host en el que se ejecuta, la alta disponibilidad no intenta reiniciar la máquina virtual.

`ha-restart-priority` Valor: el valor es una cadena vacía

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> La alta disponibilidad nunca detiene ni migra una VM en ejecución para liberar recursos para que se reinicie una VM protegida o de mejor esfuerzo.

Si el grupo experimenta errores en el host y el número de errores tolerables cae a cero, no se garantiza que las máquinas virtuales protegidas se reinicien. En tales casos, se genera una alerta del sistema. Si se produce otro error, todas las VM que tienen una prioridad de reinicio establecida se comportan de acuerdo con el comportamiento de mejor esfuerzo.

Comenzar pedido

El orden de inicio es el orden en el que XenServer High Availability intenta reiniciar las máquinas virtuales protegidas cuando se produce un error. Los valores de la propiedad `order` para cada una de las máquinas virtuales protegidas determinan el orden de inicio.

La propiedad `order` de una VM es utilizada por la alta disponibilidad y también por otras funciones que inician y apagan las VM. Cualquier máquina virtual puede tener la propiedad `order` establecida, no solo las máquinas virtuales marcadas como protegidas para alta disponibilidad. Sin embargo, la alta disponibilidad utiliza la propiedad `order` solo para máquinas virtuales protegidas.

El valor de la propiedad `order` es un entero. El valor predeterminado es 0, que es la prioridad más alta. Las máquinas virtuales protegidas con un valor `order` de 0 se reinician primero por la alta disponibilidad. Cuanto mayor sea el valor de la propiedad `order`, más tarde en la secuencia se reiniciará la VM.

Puede establecer el valor de la propiedad `order` de una máquina virtual mediante la interfaz de línea de comandos:

```
xe vm-param-set uuid=VM_UUID order=int
<!--NeedCopy-->
```

O bien, en XenCenter, en el panel de **opciones de inicio** de una máquina virtual, defina el **orden de inicio** en el valor requerido.

Habilite la alta disponibilidad en su grupo de XenServer

Puede habilitar la alta disponibilidad en un grupo mediante XenCenter o la interfaz de línea de comandos (CLI). En cualquier caso, se especifica un conjunto de prioridades que determinan qué máquinas virtuales reciben la prioridad de reinicio más alta cuando un grupo está sobrecomprometido.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Advertencias:**
>
> - Al habilitar la alta disponibilidad, es posible que se inhabiliten algunas operaciones que comprometen el plan de reinicio de las máquinas virtuales (como eliminar un host de un grupo). Puede inhabilitar temporalmente la alta disponibilidad para realizar dichas operaciones o, alternativamente, hacer que las máquinas virtuales protegidas por alta disponibilidad no estén protegidas.
> - Si la alta disponibilidad está habilitada, no puede habilitar la agrupación en clústeres en su grupo. Desactive temporalmente la alta disponibilidad para habilitar la agrupación en clústeres A continuación, puede habilitar la alta disponibilidad en su agrupación en clústeres. Algunos comportamientos de alta disponibilidad, como la autodelimitación, son diferentes para los grupos agrupados en clúster. Para obtener más información, consulte Grupos agrupados.

Habilite la alta disponibilidad mediante la CLI

1. Compruebe que tiene un repositorio de almacenamiento (SR) compatible conectado a su grupo. Los SR iSCSI, NFS o Fibre Channel son compatibles. Para obtener información sobre cómo configurar dicho repositorio de almacenamiento mediante la CLI, consulte Administrar repositorios de almacenamiento.
2. Para cada máquina virtual que quiera proteger, establezca una prioridad de reinicio y orden de inicio. Puede establecer la prioridad de reinicio de la siguiente manera:

```
xe vm-param-set uuid=vm_uuid ha-restart-priority=restart order=1
<!--NeedCopy-->
```

3. Habilite la alta disponibilidad en el grupo y, opcionalmente, especifique un tiempo de espera:

```
xe pool-ha-enable heartbeat-sr-uuids=sr_uuid ha-config:timeout=
   timeout in seconds
<!--NeedCopy-->
```

   El tiempo de espera es el período durante el cual los hosts de su grupo no pueden acceder a la red o al almacenamiento. Si no especifica un tiempo de espera al habilitar la alta disponibilidad, XenServer utiliza el tiempo de espera predeterminado de 60 segundos. Si algún host de XenServer no puede acceder a la red o al almacenamiento dentro del período de espera, puede autoprotegerse y reiniciarse.

4. Ejecute el comando `pool-ha-compute-max-host-failures-to-tolerate`. Este comando devuelve la cantidad máxima de hosts que pueden fallar antes de que no haya recursos suficientes para ejecutar todas las VM protegidas del grupo.

```
xe pool-ha-compute-max-host-failures-to-tolerate
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<!--NeedCopy-->
```

El número de errores a tolerar determina cuándo se envía una alerta. El sistema vuelve a calcular un plan de conmutación por error a medida que cambia el estado del grupo. Utiliza este cálculo para identificar la capacidad del grupo y cuántos errores más son posibles sin perder la garantía de vida para las VM protegidas. Se genera una alerta del sistema cuando este valor calculado cae por debajo del valor especificado para `ha-host-failures-to-tolerate`.

5. Especifique el parámetro `ha-host-failures-to-tolerate`. El valor debe ser menor o igual que el valor calculado:

```
xe pool-param-set ha-host-failures-to-tolerate=2 uuid=pool-uuid
<!--NeedCopy-->
```

Eliminar la protección de alta disponibilidad de una VM mediante la CLI

Para inhabilitar las funciones de alta disponibilidad de una máquina virtual, utilice el comando `xe vm-param-set` para establecer el parámetro `ha-restart-priority` como una cadena vacía. Al establecer el parámetro `ha-restart-priority` no se borra la configuración del orden de inicio. Puede volver a habilitar la alta disponibilidad para una máquina virtual configurando el parámetro `ha-restart-priority` en `restart` o `best-effort` según corresponda.

Recuperar un host inalcanzable

Si, por alguna razón, un host no puede acceder al archivo de estado de alta disponibilidad, es posible que un host se vuelva inaccesible. Para recuperar la instalación de XenServer, es posible que deba inhabilitar la alta disponibilidad mediante el comando `host-emergency-ha-disable`:

```
xe host-emergency-ha-disable --force
<!--NeedCopy-->
```

Si el host era el coordinador del grupo, se inicia normalmente con la alta disponibilidad inhabilitada. Los miembros del grupo se vuelven a conectar y desactivan automáticamente la alta disponibilidad Si el anfitrión era miembro del grupo y no puede ponerse en contacto con el coordinador del grupo, es posible que deba realizar una de las siguientes acciones:

- Forzar al host a reiniciarse como coordinador de grupos (`xe pool-emergency-transition-to-master`)

```
xe pool-emergency-transition-to-master uuid=host_uuid
<!--NeedCopy-->
```

- Dígale al anfitrión dónde está el nuevo coordinador de la agrupación (`xe pool-emergency-reset-master`):

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe pool-emergency-reset-master master-address=
   new_pool_coordinator_hostname
<!--NeedCopy-->
```

Cuando todos los hosts se hayan reiniciado correctamente, vuelva a habilitar la alta disponibilidad:

```
xe pool-ha-enable heartbeat-sr-uuid=sr_uuid
<!--NeedCopy-->
```

Apagar un host cuando la alta disponibilidad está habilitada

Tenga especial cuidado al apagar o reiniciar un host para evitar que el mecanismo de alta disponibilidad asuma que el host ha fallado. Para cerrar un host de forma limpia cuando la alta disponibilidad está habilitada, inhabilite el host, evacúe el host y, por último, apague el host mediante XenCenter o la CLI. Para apagar un host en un entorno en el que la alta disponibilidad esté habilitada, ejecute estos comandos:

```
xe host-disable host=host_name
xe host-evacuate uuid=host_uuid
xe host-shutdown host=host_name
<!--NeedCopy-->
```

Apagar una VM protegida por alta disponibilidad

Cuando una máquina virtual está protegida por un plan de alta disponibilidad y se configura para que se reinicie automáticamente, no se puede cerrar mientras esta protección está activa. Para apagar una máquina virtual, primero desactive su protección de alta disponibilidad y, a continuación, ejecute el comando CLI. XenCenter le ofrece un cuadro de diálogo para automatizar la desactivación de la protección cuando selecciona el botón **Apagar** de una máquina virtual protegida.

> **Nota:**
>
> Si apaga una VM desde el huésped y la VM está protegida, se reinicia automáticamente en las condiciones de falla de alta disponibilidad. El reinicio automático ayuda a garantizar que el error del operador no provoque que una VM protegida se apague accidentalmente. Si desea cerrar esta máquina virtual, inhabilite primero la protección de alta disponibilidad.

Copia de seguridad y recuperación ante desastres

November 28, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La función de recuperación ante desastres (DR) de XenServer le permite recuperar máquinas virtuales (VM) y vApps en caso de un fallo de hardware que destruya todo un grupo o un sitio. Para obtener información sobre la protección contra errores de un solo host, consulte Alta disponibilidad.

> **Nota:**
>
> Debe iniciar sesión con su cuenta *raíz* o tener el rol de *operador de grupo* o superior para usar la función DR.

Descripción de XenServer DR

XenServer DR funciona almacenando toda la información necesaria para recuperar las máquinas virtuales y vApps críticas para la empresa en repositorios de almacenamiento (SR). A continuación, los SR se replican desde su entorno principal (de producción) a un entorno de reserva. Cuando un grupo protegido en su sitio principal deja de funcionar, puede recuperar las máquinas virtuales y las vApps de ese grupo desde el almacenamiento replicado recreado en un sitio secundario (DR) con un tiempo de inactividad mínimo de las aplicaciones o los usuarios.

La configuración de **recuperación ante desastres** en XenCenter se puede usar para consultar el almacenamiento e importar máquinas virtuales y vApps seleccionadas a un grupo de recuperación durante un desastre. Cuando las máquinas virtuales se ejecutan en el grupo de recuperación, también se replican los metadatos del grupo de recuperación. La replicación de los metadatos del grupo permite que cualquier cambio en la configuración de la máquina virtual se complete de nuevo en el grupo principal cuando el grupo principal se recupere. A veces, la información de la misma máquina virtual puede encontrarse en varios lugares. Por ejemplo, almacenamiento desde el sitio principal, almacenamiento desde el sitio de recuperación ante desastres y también en el grupo al que se van a importar los datos. Si XenCenter descubre que la información de la máquina virtual está presente en dos o más lugares, se asegura de que solo utilice la información más reciente.

La función de recuperación ante desastres se puede usar con XenCenter y la CLI xe. Para los comandos de CLI, consulte Comandos de recuperación ante desastres

> **Sugerencia:**
>
> También puede usar la configuración de recuperación ante desastres para ejecutar conmutaciones por error de prueba para realizar pruebas no disruptivas de su sistema de recuperación ante desastres. En una conmutación por error de prueba, todos los pasos son los mismos que los de la conmutación por error. Sin embargo, las máquinas virtuales y las vApps no se inician una vez que se han recuperado en el sitio de recuperación ante desastres. Cuando se completa la prueba, se realiza una limpieza para eliminar todas las VM, vApps y almacenamiento recreados en el sitio de recuperación ante desastres.

Las máquinas virtuales de XenServer constan de dos componentes:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Discos vDisk que utiliza la máquina virtual, almacenados en repositorios de almacenamiento (SR) configurados en el grupo donde se encuentran las máquinas virtuales.
- Metadatos que describen el entorno VM. Esta información es necesaria para volver a crear la máquina virtual si la máquina virtual original no está disponible o está dañada. La mayoría de los datos de configuración de metadatos se escriben cuando se crea la VM y se actualizan solo cuando se cambia la configuración de la VM. En el caso de las máquinas virtuales de un grupo, se almacena una copia de estos metadatos en cada host del grupo.

En un entorno de recuperación ante desastres, las VM se vuelven a crear en un sitio secundario mediante los metadatos del grupo y la información de configuración de todas las VM y vApp del grupo. Los metadatos de cada VM incluyen su nombre, descripción e identificador único universal (UUID), y su memoria, CPU virtual y configuración de redes y almacenamiento. También incluye opciones de inicio de VM: orden de inicio, intervalo de demora, alta disponibilidad y prioridad de reinicio. Las opciones de inicio de VM se utilizan cuando se reinicia la VM en un entorno de alta disponibilidad o DR. Por ejemplo, cuando se recuperan máquinas virtuales durante la recuperación ante desastres, las máquinas virtuales dentro de una vApp se reinician en el grupo de DR en el orden especificado en los metadatos de la máquina virtual y se usan los intervalos de demora especificados.

Requisitos de infraestructura de DR

Configure la infraestructura de DR adecuada en los sitios principal y secundario para usar XenServer DR.

- El almacenamiento utilizado para los metadatos del grupo *y* los discos virtuales que utilizan las máquinas virtuales se deben replicar desde el entorno principal (de producción) a un entorno de respaldo. La replicación del almacenamiento, como el uso de espejado, varía según los dispositivos. Por lo tanto, consulte a su proveedor de soluciones de almacenamiento para gestionar la replicación del almacenamiento
- Después de que las máquinas virtuales y vApp que recuperó en un grupo de su sitio de recuperación ante desastres estén en funcionamiento, se deben replicar los SRs que contienen los metadatos del grupo de recuperación ante desastres y los discos vDisk. La replicación permite que las VM y vApps recuperadas se restauren en el sitio principal *(error de retorno)* cuando el sitio principal vuelve a estar en línea.
- La infraestructura de hardware de su sitio de DR no tiene que coincidir con el sitio principal. Sin embargo, el entorno XenServer debe tener el mismo nivel de versión y parche.
- Los hosts y los grupos del sitio secundario deben tener la misma edición de licencia que los del sitio principal. Estas licencias de XenServer se suman a las asignadas a los hosts del sitio principal.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Se deben configurar recursos suficientes en el grupo de destino para permitir que todas las VM de conmutación por error se vuelvan a crear e iniciar.

> **Advertencia:**
>
> La configuración de recuperación ante desastres no controla ninguna funcionalidad de arreglo de almacenamiento.
>
> Los usuarios de la función de recuperación ante desastres deben asegurarse de que el almacenamiento de metadatos se replique de alguna manera entre los dos sitios. Algunos arreglos de almacenamiento contienen funciones de "duplicación"para lograr la replicación automáticamente. Si usa estas funciones, debe inhabilitar la función de duplicación ("la duplicación no funciona") antes de reiniciar las máquinas virtuales en el sitio de recuperación.

Consideraciones sobre la implementación

Revise los siguientes pasos antes de habilitar la recuperación ante desastres.

Pasos a seguir antes de un desastre

En la siguiente sección se describen los pasos a seguir antes de un desastre.

- Configure sus máquinas virtuales y vApps.
- Observe cómo sus máquinas virtuales y vApps se asignan a los SR y los SR a los LUN. Tenga especial cuidado con la denominación de los parámetros `name_label` y `name_description`. La recuperación de máquinas virtuales y vApps del almacenamiento replicado es más fácil si los nombres de las SR capturan la forma en que las VM y las vApps se asignan a los SR y los SR a los LUN.
- Organice la replicación de los LUN.
- Habilite la replicación de metadatos del grupo en uno o más SR en estos LUN.
- Asegúrese de que los SR en los que está replicando los metadatos del grupo principal estén adjuntos a un solo grupo.

Pasos a seguir después de un desastre

En la siguiente sección se describen los pasos a seguir después de que se haya producido un desastre.

- Rompe cualquier réplica de almacenamiento existente para que el sitio de recuperación tenga acceso de lectura y escritura al almacenamiento compartido.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Asegúrese de que los LUNs de los que quiere recuperar los datos de las máquinas virtuales no estén conectados a ningún otro grupo o de que se produzcan daños.
- Si quiere proteger el sitio de *recuperación* de un desastre, debe habilitar la replicación de metadatos del grupo en uno o más SR del sitio de recuperación.

Pasos a seguir después de una recuperación

En la siguiente sección se describen los pasos que se deben seguir después de una recuperación de datos satisfactoria.

- Vuelva a sincronizar las réplicas de almacenamiento.
- En el sitio de recuperación, cierre de forma limpia las máquinas virtuales o vApp que quiera volver al sitio principal.
- En el sitio principal, siga el mismo procedimiento que para la conmutación por error de la sección anterior, para devolver las VM o vApps seleccionadas a la principal
- Para proteger el sitio principal contra desastres futuros, debe volver a habilitar la replicación de metadatos del grupo en uno o más SR en los LUN replicados.

Habilitar recuperación ante desastres

August 24, 2023

En esta sección se describe cómo habilitar la recuperación ante desastres en XenCenter. Use la opción **Configurar DR** para identificar los repositorios de almacenamiento donde se almacenan los metadatos del grupo y la información de configuración de todas las máquinas virtuales y vApps del grupo. Los metadatos se actualizan cada vez que cambia la configuración de VM o vApp dentro del grupo.

> **Nota:**
>
> Puede habilitar la recuperación ante desastres solo cuando utilice LVM sobre HBA o LVM sobre iSCSI. Se requiere una pequeña cantidad de espacio en este almacenamiento para un LUN nuevo que contenga la información de recuperación del grupo.

Antes de comenzar, asegúrese de que los SR utilizados para DR estén conectados únicamente al grupo en el sitio principal. Los SR utilizados para la recuperación ante desastres no deben adjuntarse al grupo en el sitio secundario.

Para configurar la recuperación ante desastres, lleve a cabo los siguientes pasos:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. En el sitio principal, seleccione el grupo que desea proteger. En el menú **Agrupación**, seleccione **Disaster Recovery**y, a continuación, seleccione **Configurar**.
2. Seleccione hasta 8 SR en los que se puedan almacenar los metadatos del grupo. Se requiere una pequeña cantidad de espacio en este almacenamiento para un LUN nuevo que contenga la información de recuperación del grupo.

   > **Nota:**
   >
   > La información de todas las VM del grupo se almacena, no es necesario seleccionar las VM de forma independiente para su protección.

3. Seleccione **OK**. Su agrupación ahora está protegida.

Recuperar máquinas virtuales y vApps durante un desastre (conmutación por error)

En esta sección se explica cómo recuperar las máquinas virtuales y las vApps en el sitio secundario (recuperación).

1. En XenCenter, seleccione el grupo secundario y, en el menú **Agrupación**, seleccione **Recuperación ante desastres** y, a continuación, **Asistente para la recuperación ante desastres**.

   El asistente de recuperación ante desastres muestra tres opciones de recuperación: **conmutación por error,**conmutación**por error** y **conmutación por error de prueba**. Para recuperar en el sitio secundario, seleccione **Conmutación por error** y, a continuación, seleccione **Siguiente**.

   > **Advertencia:**
   >
   > Si usa almacenamiento compartido Fibre Channel con espejado de LUN para replicar datos en el sitio secundario, rompa el espejado antes de intentar recuperar las VM. La duplicación debe interrumpirse para garantizar que el sitio secundario tenga acceso de lectura y escritura.

2. Seleccione los repositorios de almacenamiento (SR) que contienen los metadatos del grupo para las VM y vApps que quiere recuperar.

   De forma predeterminada, la lista de esta página del asistente muestra todos los SR que están conectados actualmente dentro del grupo. Para buscar más SR, seleccione **Buscar repositorios de almacenamiento** y, a continuación, seleccione el tipo de almacenamiento que desea buscar:

   - Para buscar todos los SR de HBA de hardware disponibles, seleccione **Buscar SR de HBA de hardware**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Para buscar SR iSCSI de software, seleccione **Buscar SR iSCSI de software y, a** continuación, escriba los detalles del host, el IQN y el LUN de destino.

Cuando haya seleccionado los SR requeridos en el asistente, seleccione **Siguiente** para continuar.

3. Seleccione las VM y vApps que quiere recuperar. Seleccione la opción **Estado de energía adecuada después de la recuperación** para especificar si quiere que el asistente los inicie automáticamente cuando se hayan recuperado. Como alternativa, puede iniciarlos manualmente una vez finalizada la conmutación por error.

   Seleccione **Siguiente** para pasar a la siguiente página del asistente e iniciar las comprobaciones previas de conmutación por error.

4. El asistente realiza varias comprobaciones previas antes de iniciar la conmutación por error. Por ejemplo, para garantizar que todo el almacenamiento requerido por las máquinas virtuales y vApps seleccionadas esté disponible. Si falta algún almacenamiento en este momento, puede seleccionar **Adjuntar SR** en esta página para buscar y adjuntar el SR correspondiente.

   Resuelva cualquier problema en la página de comprobaciones previas y, a continuación, seleccione **Conmutación por error** para iniciar el proceso de recuperación.

5. Una página de progreso muestra el resultado del proceso de recuperación de cada VM y vApp. El proceso de conmutación por error exporta los metadatos de las máquinas virtuales y las vApps desde el almacenamiento replicado. Por lo tanto, el tiempo que tarda la conmutación por error depende de las máquinas virtuales y las vApps que recupere. Las máquinas virtuales y vApp se vuelven a crear en el grupo primario y los SRs que contienen los discos vDisk se conectan a las máquinas virtuales recreadas. Si se especifica, se inician las VM.

6. Cuando se complete la conmutación por error, seleccione **Siguiente** para ver el informe resumido. Seleccione **Finalizar** en la página del informe resumido para cerrar el asistente.

Cuando el sitio principal esté disponible, trabaje a través del asistente de recuperación ante desastres y seleccione **Failback** para volver a ejecutar las máquinas virtuales en ese sitio.

Restaurar máquinas virtuales y vApps en el sitio principal después de un desastre (conmutación por recuperación)

En esta sección se explica cómo restaurar máquinas virtuales y vApps desde el almacenamiento replicado. Puede restaurar máquinas virtuales y vApps en un grupo en su sitio principal (de producción) cuando el sitio principal vuelva a funcionar después de un desastre. Para hacer una conmutación por recuperación de máquinas virtuales y vApps a su sitio principal, use el asistente de recuperación ante desastres.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. En XenCenter, seleccione el grupo principal y, en el menú Agrupación, seleccione **Recuperación ante desastres** y, a continuación, **Asistente para recuperación ante desastres**.

   El asistente de recuperación ante desastres muestra tres opciones de recuperación: **conmutación por error,**conmutación**por error** y **conmutación por error de prueba**. **Para restaurar las máquinas virtuales y las vApps en su sitio principal, seleccione**Failback**y, a continuación, seleccione Siguiente.**

   > **Advertencia:**
   >
   > Cuando utiliza almacenamiento compartido Fibre Channel con espejado de LUN para replicar datos en el sitio principal, rompa el espejado antes de intentar restaurar las VM. La duplicación debe interrumpirse para garantizar que el sitio principal tenga acceso de lectura y escritura.

2. Seleccione los repositorios de almacenamiento (SR) que contienen los metadatos del grupo para las VM y vApps que quiere recuperar.

   De forma predeterminada, la lista de esta página del asistente muestra todos los SR que están conectados actualmente dentro del grupo. Para buscar más SR, elija **Buscar repositorios de almacenamiento** y, a continuación, seleccione el tipo de almacenamiento que quiere analizar:

   - Para buscar todos los SR de HBA de hardware disponibles, seleccione **Buscar SR de HBA de hardware**.
   - Para buscar SR iSCSI de software, seleccione **Buscar SR iSCSI de software y, a** continuación, escriba los detalles del host, el IQN y el LUN de destino.

   Cuando haya seleccionado los SR requeridos en el asistente, seleccione **Siguiente** para continuar.

3. Seleccione las VM y vApp que quiere restaurar. Seleccione la opción **Estado de energía adecuada después de la recuperación** para especificar si quiere que el asistente los inicie automáticamente cuando se hayan recuperado. Como alternativa, puede iniciarlos manualmente una vez finalizada la conmutación por recuperación.

   Seleccione **Siguiente** para pasar a la siguiente página del asistente e iniciar las comprobaciones previas de conmutación por recuperación.

4. El asistente realiza varias comprobaciones previas antes de iniciar la conmutación por recuperación. Por ejemplo, para garantizar que todo el almacenamiento requerido por las máquinas virtuales y vApps seleccionadas esté disponible. Si falta algún almacenamiento en este momento, puede seleccionar **Adjuntar SR en esta página** para buscar y adjuntar el SR correspondiente.

   Resuelva cualquier problema en la página de comprobaciones previas y, a continuación, seleccione **Failback** para iniciar el proceso de recuperación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Una página de progreso muestra el resultado del proceso de recuperación de cada VM y vApp. El proceso de conmutación por recuperación exporta los metadatos de las máquinas virtuales y las vApps desde el almacenamiento replicado. Por lo tanto, la conmutación por recuperación puede tardar algún tiempo en función de la cantidad de máquinas virtuales y vApps que esté restaurando. Las máquinas virtuales y vApp se vuelven a crear en el grupo primario y los SRs que contienen los discos vDisk se conectan a las máquinas virtuales recreadas. Si se especifica, se inician las VM.
6. Cuando se complete la conmutación por recuperación, seleccione **Siguiente** para ver el informe resumido. Seleccione **Finalizar** en la página del informe resumido para cerrar el asistente.

Prueba de conmutación por error

Las pruebas de conmutación por error son un componente esencial en la planificación de recuperación ante desastres. Puede usar el asistente de recuperación ante desastres para realizar pruebas no disruptivas de su sistema de recuperación ante desastres. Durante una operación de conmutación por error de prueba, los pasos son los mismos que para la conmutación por error. Sin embargo, en lugar de iniciarse después de que se hayan recuperado en el sitio de recuperación ante desastres, las máquinas virtuales y las vApps se colocan en estado de pausa. Al final de una operación de conmutación por error de prueba, todas las máquinas virtuales, vApps y almacenamiento recreados en el sitio de recuperación ante desastres se eliminan automáticamente. Después de la configuración inicial de DR y después de realizar cambios de configuración significativos en un grupo habilitado para DR, compruebe que la conmutación por error funciona correctamente realizando una conmutación por error de prueba.

1. En XenCenter, seleccione el grupo secundario y, en el menú **Grupo**, seleccione **Recuperación ante desastres** para abrir el **Asistente para recuperación de desastres.**

   El asistente de recuperación ante desastres muestra tres opciones de recuperación: **conmutación por error,**conmutación**por error** y **conmutación por error de prueba**. Para probar el sistema de recuperación ante desastres, selecciona **Probar conmutación por error** y, a continuación, selecciona **Siguiente**.

   > **Nota:**
   >
   > Si utiliza almacenamiento compartido Fibre Channel con espejado de LUN para replicar datos en el sitio secundario, rompa el espejado antes de intentar recuperar los datos. La duplicación debe interrumpirse para garantizar que el sitio secundario tenga acceso de lectura y escritura.

2. Seleccione los repositorios de almacenamiento (SR) que contienen los metadatos del grupo para las VM y vApps que quiere recuperar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

De forma predeterminada, la lista de esta página del asistente muestra todos los SR que están conectados actualmente dentro del grupo. Para buscar más SR, seleccione **Buscar repositorios de almacenamiento** y, a continuación, el tipo de almacenamiento que desea buscar:

- Para buscar todos los SR de HBA de hardware disponibles, seleccione **Buscar SR de HBA de hardware**.
- Para buscar SR iSCSI de software, seleccione **Buscar SR iSCSI de software y, a** continuación, escriba los detalles del host, el IQN y el LUN de destino en el cuadro.

Cuando haya seleccionado los SR requeridos en el asistente, seleccione **Siguiente** para continuar.

3. Seleccione las VM y vApp que quiere recuperar y, a continuación, seleccione **Siguiente** para avanzar a la página siguiente y comenzar las comprobaciones previas de conmutación por error.
4. Antes de iniciar la conmutación por error de prueba, el asistente realiza varias comprobaciones previas. Por ejemplo, para garantizar que todo el almacenamiento requerido por las máquinas virtuales y vApps seleccionadas esté disponible.

   - **Compruebe que haya espacio de almacenamiento disponible**. Si falta algún almacenamiento, puede seleccionar Adjuntar SR en esta página para buscar y adjuntar el SR relevante.
   - **Compruebe que la alta disponibilidad no esté habilitada en el grupo de DR de destino**. La alta disponibilidad debe inhabilitarse en el grupo secundario para evitar que las mismas máquinas virtuales se ejecuten tanto en la agrupación principal como en la agrupación de DR. Se debe inhabilitar la alta disponibilidad para garantizar que no inicie las VM y vApps recuperados automáticamente después de la recuperación. Para inhabilitar la alta disponibilidad en el grupo secundario, simplemente seleccione **Desactivar HA** en la página. Si la alta disponibilidad está inhabilitada en este punto, se vuelve a habilitar automáticamente al final del proceso de conmutación por error de prueba.

   Resuelva cualquier problema en la página de comprobaciones previas y, a continuación, seleccione **Conmutación por error** para iniciar la conmutación por error de prueba.
5. Una página de progreso muestra el resultado del proceso de recuperación de cada VM y vApp. El proceso de conmutación por error recupera los metadatos de las máquinas virtuales y las vApps del almacenamiento replicado. Por lo tanto, la conmutación por error puede tardar algún tiempo en función de la cantidad de máquinas virtuales y vApps que esté recuperando. Las máquinas virtuales y vApp se vuelven a crear en el grupo DR, los SRs que contienen los discos vDisk están conectados a las máquinas virtuales recreadas.

   Las máquinas virtuales recuperadas se colocan en un estado de pausa: no se inician en el sitio secundario durante una conmutación por error de prueba.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Cuando esté seguro de que la conmutación por error de prueba se realizó correctamente, seleccione Siguiente en el asistente para que el asistente limpie el sitio de recuperación ante desastres:

   - Las máquinas virtuales y las vApps que se recuperaron durante la conmutación por error de prueba se eliminan.
   - El almacenamiento que se recuperó durante la conmutación por error de prueba se desconecta.
   - Si se inhabilitó la alta disponibilidad en el grupo de DR en la etapa de comprobaciones previas para permitir que se llevara a cabo la conmutación por error de prueba, se vuelve a habilitar automáticamente.

   El progreso del proceso de limpieza aparece en el asistente.

7. Seleccione **Finalizar** para cerrar el asistente.

vApps

August 24, 2023

Una vApp es un grupo lógico de una o más máquinas virtuales (VM) relacionadas. Las vApps se pueden iniciar como una sola entidad cuando se produce un desastre. Cuando se inicia una vApp, las VM contenidas en la vApp se inician en un orden predefinido por el usuario. El orden de inicio permite que las VM que dependen unas de otras se secuencien automáticamente. Un administrador ya no tiene que secuenciar manualmente el inicio de las VM dependientes cuando se requiere reiniciar todo un servicio. Por ejemplo, durante una actualización de software. Las máquinas virtuales dentro de la vApp no tienen que residir en un host y se distribuyen dentro de un grupo mediante las reglas normales. La función vApp es útil en la situación de recuperación ante desastres (DR). En un caso de DR, un administrador puede agrupar todas las máquinas virtuales en el mismo repositorio de almacenamiento o que estén relacionadas con el mismo acuerdo de nivel de servicio (SLA).

Para agrupar las máquinas virtuales en una vApp, siga el procedimiento:

1. Seleccione el grupo y, en el menú **Agrupación**, haga clic en **Administrar vApps**.
2. Escriba un nombre para la vApp y, si lo quiere, una descripción y, a continuación, haga clic en **Siguiente**.

   Puede elegir el nombre que quieras, pero lo mejor es un nombre informativo. Aunque le recomendamos evitar tener múltiples vApps con el mismo nombre, no es un requisito. XenCenter no aplica ninguna restricción con respecto a los nombres únicos de vApp. No es necesario usar comillas para los nombres que incluyan espacios.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Seleccione qué máquinas virtuales desea incluir en la nueva vApp y, a continuación, haga clic en **Siguiente**.

   Puede usar la opción de búsqueda para enumerar solo las máquinas virtuales con nombres que incluyan la cadena de texto especificada.

4. Especifique la secuencia de inicio de las máquinas virtuales en la vApp y, a continuación, haga clic en **Siguiente**.

   Orden de inicio: especifica el orden en que se inician las VM individuales dentro de la vApp, lo que permite que ciertas VM se reinicien antes que otras. Las máquinas virtuales con un valor de orden inicial de 0 (cero) se inician primero. A continuación, se inician las VM con un valor de orden inicial de 1 y, a continuación, las VM con un valor de 2, y así sucesivamente.

   Intentar iniciar la siguiente máquina virtual después: Un intervalo de demora que especifica cuánto tiempo se debe esperar después de iniciar la máquina virtual antes de intentar iniciar el siguiente grupo de máquinas virtuales en la secuencia de inicio.

5. Puede revisar la configuración de vApp en la página final. Haga clic en **Anterior** para volver y cambiar cualquier configuración, o en **Finalizar** para crear la vApp.

> **Nota:**
>
> Una vApp puede abarcar varios hosts en un solo grupo, pero no puede abarcar varios grupos.

Administrar vApps en XenCenter

La configuración **Administrar vApps** en XenCenter le permite crear, eliminar y cambiar vApps. También le permite iniciar y cerrar vApps, e importar y exportar vApps dentro del grupo seleccionado. Cuando selecciona una vApp en la lista, las máquinas virtuales que contiene se enumeran en el panel de detalles. Para obtener más información, consulte vApps en la documentación de XenCenter.

Realizar copias de seguridad y restaurar hosts y máquinas virtuales

August 24, 2023

Siempre que sea posible, deje inalterado el estado de instalación de los hosts de XenServer. Es decir, no instale ningún paquete adicional ni inicie servicios adicionales en los hosts de XenServer ni los trate como dispositivos. Por lo tanto, la mejor forma de restaurar es volver a instalar el software host de XenServer desde el medio de instalación. Si tiene varios hosts de XenServer, lo mejor es configurar un servidor TFTP y los archivos de respuesta adecuados para este fin. Para obtener más información, consulte Instalaciones de arranque en red.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Le recomendamos que utilice una solución de reserva ofrecida por uno de nuestros socios certificados. Para obtener más información, consulte Citrix Ready Marketplace.

Los clientes de XenServer Premium Edition pueden aprovechar el respaldo más rápido de solo bloques modificados. Para obtener más información, consulta la documentación sobre el seguimiento de bloques modificados.

Le recomendamos que realice con frecuencia tantos de los siguientes procedimientos de copia de seguridad como sea posible para recuperarse de una posible falla del servidor y del software.

Para hacer una copia de seguridad de los metadatos:

1. Ejecute el comando:

```
xe pool-dump-database file-name=backup
<!--NeedCopy-->
```

2. Para restaurar la base de datos, ejecute el comando:

```
xe pool-restore-database file-name=backup dry-run=true
<!--NeedCopy-->
```

   Este comando comprueba que la máquina de destino tenga un número adecuado de NIC con el nombre adecuado, lo cual es necesario para que la copia de seguridad se realice correctamente.

Para hacer una copia de seguridad de la configuración y el software:

1. Ejecute el comando:

```
xe host-backup host=host file-name=hostbackup
<!--NeedCopy-->
```

> **Notas:**
>
> - No cree la copia de seguridad en el dominio de control.
> - El procedimiento de reserva puede crear un archivo de reserva grande.
> - Para completar una restauración, debe reiniciar el CD de instalación original.
> - Estos datos solo se pueden restaurar en el equipo original.

Para hacer copias de seguridad de una VM:

1. Asegúrese de que la VM de la que se va a realizar la copia de seguridad esté
2. Ejecute el comando:

```
xe vm-export vm=vm_uuid filename=backup
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Esta copia de seguridad también hace una copia de todos los datos de la VM. Al importar una VM, puede especificar el mecanismo de almacenamiento que se utilizará para los datos de los que se hizo una copia.
>
> **Advertencia:**
>
> El proceso de reserva puede tardar más en completarse, ya que crea una copia de todos los datos de la VM.

Para respaldar solo los metadatos de la VM:

Ejecute el comando:

```
xe vm-export vm=vm_uuid filename=backup metadata=true
<!--NeedCopy-->
```

Realizar una copia de seguridad de los metadatos

Los hosts XenServer utilizan una base de datos en cada host para almacenar metadatos sobre las máquinas virtuales y los recursos asociados, como el almacenamiento y las redes. Cuando se combina con SR, esta base de datos forma la vista completa de todas las VM disponibles en el grupo. Por lo tanto, es importante entender cómo hacer una copia de seguridad de esta base de datos para recuperarse de una falla de hardware físico y otras situaciones de desastre.

En esta sección se describe primero cómo hacer una copia de seguridad de los metadatos para instalaciones de host único y, a continuación, para configuraciones de grupos más complejas.

Realizar copias de seguridad de instalaciones de host

Use la CLI para hacer una copia de seguridad de la base de datos Para obtener un archivo de respaldo de metadatos de grupo coherente, ejecútelo `pool-dump-database` en el host de XenServer y archive el archivo resultante. El archivo de copia de seguridad contiene información de autenticación confidencial sobre el grupo, así que asegúrese de que se almacene de forma segura.

Para restaurar la base de datos del grupo, utilice el comando `xe pool-restore-database` de un archivo de volcado anterior. Si el host de XenServer ha muerto por completo, primero debe realizar una instalación nueva y, a continuación, ejecutar el `pool-restore-database` comando en el host de XenServer recién instalado.

Después de restaurar la base de datos del grupo, es posible que algunas VM sigan registrándose como `Suspended`. Sin embargo, si el repositorio de almacenamiento con el estado de memoria suspendida definido en el campo `suspend-VDI-uuid`, es un SR local, es posible que el SR no

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

esté disponible ya que el host se ha reinstalado. Para restablecer estas máquinas virtuales al estado `Halted` de modo que puedan volver a iniciarse, utilice el comando `xe vm-shutdown vm=vm_name -force` o el comando `xe vm-reset-powerstate vm=vm_name -force`.

> **Advertencia:**
>
> XenServer conserva los UUID de los hosts restaurados mediante este método. Si restaura en una máquina física diferente mientras el host original de XenServer aún está en ejecución, es posible que haya UUID duplicados. Como resultado, XenCenter se niega a conectarse al segundo host de XenServer. La copia de seguridad de bases de datos de grupos no es el mecanismo recomendado para clonar hosts En su lugar, utilice el soporte de instalación automatizada. Para obtener más información, consulte Instalación.

Realizar copias de seguridad de instalaciones agrupadas

En un escenario de grupo, el coordinador del grupo proporciona una base de datos autorizada que se refleja sincrónicamente en todos los hosts miembros del grupo. Este proceso proporciona un nivel de redundancia incorporada a un grupo. Cualquier miembro del grupo puede reemplazar al coordinador del grupo porque cada miembro del grupo tiene una versión precisa de la base de datos del grupo. Para obtener más información sobre cómo hacer la transición de un miembro para que se convierta en coordinador de grupos, consulte Anfitriones y grupos de recursos.

Este nivel de protección puede no ser suficiente. Por ejemplo, cuando se realiza una copia de seguridad del almacenamiento compartido que contiene los datos de la VM en varios sitios, pero el almacenamiento del servidor local (que contiene los metadatos del grupo) no. Para volver a crear un grupo dado un conjunto de almacenamiento compartido, primero debe hacer una copia de seguridad del archivo `pool-dump-database` en el host del coordinador del grupo y archivarlo. Para restaurar esta copia de seguridad más adelante en un conjunto de hosts completamente nuevo:

1. Instale un conjunto nuevo de hosts XenServer desde el medio de instalación o, si corresponde, arranque en red desde su servidor TFTP.
2. Úselo `xe pool-restore-database` en el anfitrión designado para ser el nuevo coordinador de la piscina.
3. Ejecute el comando `xe host-forget` en el nuevo coordinador de grupos para eliminar las máquinas miembro antiguas.
4. Utilice el comando `xe pool-join` en los hosts miembros para conectarlos al nuevo grupo.

Realice copias de seguridad de los hosts de XenServer

En esta sección se describen los procedimientos de copia de seguridad y restauración del dominio de control de host de XenServer. Estos procedimientos *no hacen copias* de seguridad de los repositorios

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de almacenamiento que albergan las máquinas virtuales, sino solo del dominio de control privilegiado que ejecuta Xen y el agente XenServer.

> **Nota:**
>
> Es mejor dejar el dominio de control privilegiado como instalado, sin personalizarlo con otros paquetes. Se recomienda configurar un entorno de arranque de red para instalar XenServer de forma limpia desde el dispositivo XenServer como estrategia de recuperación. Por lo general, no necesita hacer una copia de seguridad del dominio de control, pero le recomendamos que guarde los metadatos del grupo (consulte Realizar una copia de seguridad de los metadatos de la máquina virtual). Considere este método de reserva como complementario a la copia de seguridad de los metadatos del grupo.

El uso de los comandos xe `host-backup` y `host-restore` es otro enfoque que puede adoptar. El comando xe `host-backup` archiva la partición activa en un archivo que especifique. El comando xe `host-restore` extrae un archivo creado por xe `host-backup` sobre la partición de disco actualmente inactiva del host. Esta partición se puede activar iniciando desde el CD de instalación y seleccionando restaurar la copia de seguridad apropiada.

Después de completar los pasos de la sección anterior y reiniciar el host, asegúrese de que los metadatos de la VM se restauren a un estado coherente. Ejecute `xe pool-restore-database` en `/var/backup/pool-database-${ DATE }` para restaurar los metadatos de la VM. Este archivo se crea `xe host-backup` mediante el uso de un comando `xe pool-dump-database` antes de archivar el sistema de archivos en ejecución, para crear una instantánea de un estado coherente de los metadatos de la máquina virtual.

Para hacer una copia de seguridad del host de XenServer:

En un host remoto con suficiente espacio en disco, ejecute el siguiente comando

```
xe host-backup file-name=filename -h hostname -u root -pw password
<!--NeedCopy-->
```

Este comando crea una imagen comprimida del sistema de archivos de dominio de control. La imagen se almacena en la ubicación especificada por el argumento `file-name`.

Para restaurar un host de XenServer en ejecución:

1. Si quiere restaurar el host de XenServer a partir de una copia de seguridad específica, ejecute el siguiente comando mientras el host de XenServer esté activo y accesible:

   ```
   xe host-restore file-name=filename -h hostname -u root -pw
      password
   <!--NeedCopy-->
   ```

   Este comando restaura la imagen comprimida en el disco duro del host de XenServer que ejecuta este comando (no en el host en el que `filename` reside). En este contexto, “restaurar”

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

puede ser un nombre inapropiado, ya que la palabra generalmente sugiere que el estado de copia de seguridad se ha establecido completamente. El comando restore solo desempaqueta el archivo de copia de seguridad comprimido y lo restaura a su forma normal. Sin embargo, se escribe en otra partición (/dev/sda2) y *no* sobrescribe la versión actual del sistema de archivos.

2. **Para usar la versión restaurada del sistema de archivos raíz, reinicie el host de XenServer mediante el CD de instalación de XenServer y seleccione la opción Restaurar desde copia de seguridad.**

   Una vez completada la restauración desde la copia de seguridad, reinicie el host XenServer y se iniciará desde la imagen restaurada.

3. Por último, restaure los metadatos de la VM con el siguiente comando:

```
xe pool-restore-database file-name=/var/backup/pool-database-* -h
   hostname -u root -pw password
<!--NeedCopy-->
```

> **Nota:**
>
> La restauración desde una copia de seguridad como se describe en esta sección no destruye la partición de copia de seguridad.

Para reiniciar un host de XenServer bloqueado:

Si el host de XenServer se ha bloqueado y no se puede acceder a él, utilice el CD de instalación de XenServer para realizar una instalación de actualización. Cuando se complete la instalación de la actualización, reinicie la máquina y asegúrese de que se pueda acceder al host con XenCenter o CLI remota.

A continuación, realice una copia de seguridad de los hosts de XenServer tal y como se describe en esta sección.

Realizar copias de seguridad de máquinas virtuales

Le recomendamos que utilice una solución de reserva ofrecida por uno de nuestros socios certificados. Para obtener más información, consulte Citrix Ready Marketplace.

Los clientes de XenServer Premium Edition pueden aprovechar el respaldo más rápido de solo bloques modificados. Para obtener más información, consulte el blog de Citrix sobre las API de reserva de seguimiento de bloques cambiados.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

layout: doc
description: Understand how to take a snapshot of your VM storage and metadata in order to restore your VM to a previous state. Use the Scheduled Snapshots feature to back up and restore your critical service VMs.—

Instantáneas de VM

XenServer proporciona un mecanismo práctico que puede tomar una instantánea del almacenamiento y los metadatos de una máquina virtual en un momento dado. Cuando es necesario, la E/S se detiene temporalmente mientras se toma la instantánea para garantizar que se pueda capturar una imagen de disco autocoherente.

Las operaciones de instantáneas dan como resultado una máquina virtual de instantáneas que es similar a una plantilla. La instantánea de VM contiene toda la información de almacenamiento y la configuración de VM, incluidas las VIF adjuntas, lo que permite exportarlas y restaurarlas con fines de reserva. Las instantáneas se admiten en todos los tipos de almacenamiento. Sin embargo, para los tipos de almacenamiento basados en LVM, se deben cumplir los siguientes requisitos:

- Si el repositorio de almacenamiento se creó en una versión anterior de XenServer, debe haberse actualizado
- El volumen debe estar en el formato predeterminado (no se puede tomar una instantánea de los volúmenes `type=raw`)

La operación de instantánea es un proceso de dos pasos:

- Captura de metadatos como plantilla.
- Crear una instantánea de VDI de los discos.

Se admiten los siguientes tipos de instantáneas de máquinas virtuales: normales e instantáneas con memoria.

Instantáneas regulares

Las instantáneas normales son coherentes con los bloqueos y se pueden realizar en todos los tipos de VM, incluidas las VM de Linux.

Instantáneas con memoria

Además de guardar la memoria (almacenamiento) y los metadatos de las máquinas virtuales, las instantáneas con memoria también guardan el estado de las máquinas virtuales (RAM). Esta función

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

puede ser útil cuando actualiza o aplica parches al software, pero también desea tener la opción de volver al estado de VM (RAM) previo al cambio. Para volver a una instantánea con memoria, no es necesario reiniciar la VM.

Puede tomar una instantánea con memoria de una máquina virtual en ejecución o suspendida mediante la API de administración, la CLI xe o XenCenter.

Crear una instantánea de VM

Antes de tomar una instantánea, consulte la siguiente información sobre cualquier configuración y consideraciones específicas del sistema operativo especial:

- Prepararse para clonar una VM Windows mediante Sysprep
- Prepararse para clonar una VM Linux

En primer lugar, asegúrese de que la VM esté en ejecución o suspendida para que se pueda capturar el estado de la memoria. La forma más sencilla de seleccionar la máquina virtual en la que se realizará la operación es proporcionando el argumento `vm=name` o `vm=vm uuid`.

Ejecute el `vm-snapshot`comando para tomar una instantánea de una VM.

```
xe vm-snapshot vm=vm uuid new-name-label=vm_snapshot_name
<!--NeedCopy-->
```

Crea una instantánea con memoria

Ejecute el comando `vm-checkpoint`, dando un nombre descriptivo para la instantánea con memoria, para que pueda identificarla más adelante:

```
xe vm-checkpoint vm=vm uuid new-name-label=name of the checkpoint
<!--NeedCopy-->
```

Cuando XenServer haya terminado de crear la instantánea con memoria, se mostrará su UUID.

Por ejemplo:

```
xe vm-checkpoint vm=2d1d9a08-e479-2f0a-69e7-24a0e062dd35 \
new-name-label=example_checkpoint_1
b3c0f369-59a1-dd16-ecd4-a1211df29886
<!--NeedCopy-->
```

Una instantánea con memoria requiere al menos 4 MB de espacio en disco por disco, más el tamaño de la RAM, además de un 20% de sobrecarga. Por lo tanto, un punto de control con 256 MB de RAM requeriría aproximadamente 300 MB de almacenamiento.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Durante el proceso de creación del punto de control, la máquina virtual se detiene durante un breve período y no se puede usar durante este período.

Para enumerar todas las instantáneas del grupo de XenServer

Ejecute el comando `snapshot-list`.

```
xe snapshot-list
<!--NeedCopy-->
```

Este comando muestra todas las instantáneas del grupo de XenServer.

Para enumerar las instantáneas de una máquina virtual en particular

Obtenga el UUID de la VM en particular ejecutando el comando `vm-list`.

```
xe vm-list
<!--NeedCopy-->
```

Este comando muestra una lista de todas las VM y sus UUID. Por ejemplo:

```
xe vm-list
uuid ( RO): 116dd310-a0ef-a830-37c8-df41521ff72d
name-label ( RW): Windows Server 2016 (1)
power-state ( RO): halted

uuid ( RO): dff45c56-426a-4450-a094-d3bba0a2ba3f
name-label ( RW): Control domain on host
power-state ( RO): running
<!--NeedCopy-->
```

Las máquinas virtuales también se pueden especificar filtrando la lista completa de máquinas virtuales por los valores de los campos.

Por ejemplo, al especificar `power-state=halted`, se seleccionan todas las máquinas virtuales cuyo campo de estado de energía sea igual a “detenido”. Cuando coinciden varias máquinas virtuales, se debe especificar la opción `--multiple` para realizar la operación. Obtenga la lista completa de campos que se pueden hacer coincidir mediante el comando `xe vm-list params=all`.

Busque la máquina virtual requerida y, a continuación, introduzca lo siguiente:

```
xe snapshot-list snapshot-of=vm uuid
<!--NeedCopy-->
```

Por ejemplo:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe snapshot-list snapshot-of=2d1d9a08-e479-2f0a-69e7-24a0e062dd35
<!--NeedCopy-->
```

Este comando enumera las instantáneas que se encuentran actualmente en esa máquina virtual:

```
    uuid ( RO): d7eefb03-39bc-80f8-8d73-2ca1bab7dcff
    name-label ( RW): Regular
    name-description ( RW):
    snapshot_of ( RO): 2d1d9a08-e479-2f0a-69e7-24a0e062dd35
    snapshot_time ( RO): 20090914T15:37:00Z

    uuid ( RO): 1760561d-a5d1-5d5e-2be5-d0dd99a3b1ef
    name-label ( RW): Snapshot with memory
    name-description ( RW):
    snapshot_of ( RO): 2d1d9a08-e479-2f0a-69e7-24a0e062dd35
    snapshot_time ( RO): 20090914T15:39:45Z
<!--NeedCopy-->
```

Restaurar una VM a su estado anterior

Asegúrese de que tiene el UUID de la instantánea a la que quiere volver y, a continuación, ejecute el comando `snapshot-revert`:

1. Ejecute el comando `snapshot-list` para buscar el UUID de la instantánea o el punto de control al que quiere revertir:

   ```
   xe snapshot-list
   <!--NeedCopy-->
   ```

2. Anote el UUID de la instantánea y, a continuación, ejecute el siguiente comando para revertir:

   ```
   xe snapshot-revert snapshot-uuid=snapshot uuid
   <!--NeedCopy-->
   ```

   Por ejemplo:

   ```
   xe snapshot-revert snapshot-uuid=b3c0f369-59a1-dd16-ecd4-
      a1211df29886
   <!--NeedCopy-->
   ```

   Después de revertir una VM a un punto de control, la VM se suspende.

> **Notas:**
>
> - Si no hay suficiente espacio en disco disponible para aprovisionar la instantánea en gran medida, no podrá restaurar la instantánea hasta que se haya liberado el estado actual del disco. Si se produce este problema, vuelva a intentar la operación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - Es posible volver a cualquier instantánea. Las instantáneas y los puntos de control existentes no se eliminan durante la operación de reversión.

Eliminar una instantánea

Asegúrese de tener el UUID del punto de control o la instantánea que desea eliminar y, a continuación, ejecute el siguiente comando:

1. Ejecute el comando `snapshot-list` para buscar el UUID de la instantánea o el punto de control al que quiere revertir:

```
xe snapshot-list
<!--NeedCopy-->
```

2. Anote el UUID de la instantánea y, a continuación, ejecute el comando `snapshot-uninstall` para eliminarla:

```
xe snapshot-uninstall snapshot-uuid=snapshot-uuid
<!--NeedCopy-->
```

3. Este comando le alerta sobre la VM y los VDI que se eliminan. Escriba `yes` para confirmar.

Por ejemplo:

```
    xe snapshot-uninstall snapshot-uuid=1760561d-a5d1-5d5e-2be5-
       d0dd99a3b1ef
    The following items are about to be destroyed
    VM : 1760561d-a5d1-5d5e-2be5-d0dd99a3b1ef (Snapshot with memory)
    VDI: 11a4aa81-3c6b-4f7d-805a-b6ea02947582 (0)
    VDI: 43c33fe7-a768-4612-bf8c-c385e2c657ed (1)
    VDI: 4c33c84a-a874-42db-85b5-5e29174fa9b2 (Suspend image)
    Type 'yes' to continue
    yes
    All objects destroyed
<!--NeedCopy-->
```

Si solo desea eliminar los metadatos de un punto de control o instantánea, ejecute el siguiente comando:

```
xe snapshot-destroy snapshot-uuid=snapshot-uuid
<!--NeedCopy-->
```

Por ejemplo:

```
xe snapshot-destroy snapshot-uuid=d7eefb03-39bc-80f8-8d73-2ca1bab7dcff
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Plantillas de instantáneas

Crear una plantilla a partir de una instantánea

Puede crear una plantilla de VM a partir de una instantánea. Sin embargo, se elimina su estado de memoria.

1. Use el comando `snapshot-copy` y especifique un **`new`**`-name-`**`label`** para la plantilla:

```
xe snapshot-copy new-name-label=vm-template-name \
      snapshot-uuid=uuid of the snapshot
<!--NeedCopy-->
```

   Por ejemplo:

```
xe snapshot-copy new-name-label=example_template_1
      snapshot-uuid=b3c0f369-59a1-dd16-ecd4-a1211df29886
<!--NeedCopy-->
```

   > **Nota:**
   >
   > Este comando crea un objeto de plantilla en la misma agrupación. Esta plantilla solo existe en la base de datos de XenServer para el grupo actual.

2. Para comprobar que se ha creado la plantilla, ejecute el comando `template-list`:

```
xe template-list
<!--NeedCopy-->
```

   Este comando muestra todas las plantillas del host de XenServer.

Exportar una instantánea a una plantilla

Cuando exporta una instantánea de VM, se almacena una copia completa de la VM (incluidas las imágenes de disco) como un solo archivo en su máquina local. Este archivo tiene una extensión de nombre de archivo `.xva`.

1. Use el comando `snapshot-export-to-template` para crear un archivo de plantilla:

```
xe snapshot-export-to template snapshot-uuid=snapshot-uuid \
      filename=template-  filename
<!--NeedCopy-->
```

   Por ejemplo:

```
xe snapshot-export-to-template snapshot-uuid=b3c0f369-59a1-dd16-
   ecd4-a1211df29886 \
      filename=example_template_export
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La función de exportación/importación de VM se puede utilizar de varias maneras diferentes:

- Como una práctica instalación de copia de seguridad para sus máquinas virtuales. Un archivo de VM exportado se puede usar para recuperar una VM completa en un caso de desastre.
- Como una forma de copiar rápidamente una VM, por ejemplo, una configuración de servidor especial que se usa muchas veces. Solo tiene que configurar la VM de la forma que quiera, exportarla y, a continuación, importarla para crear copias de la VM original.
- Como un método sencillo para mover una máquina virtual a otro host.

Para obtener más información sobre el uso de plantillas, consulte Crear máquinas virtuales y también el artículo Administración de máquinas virtuales en la documentación de XenCenter.

Instantáneas programadas

La función de instantáneas programadas proporciona una sencilla utilidad de copia de seguridad y restauración para sus máquinas virtuales de servicio críticas. Las instantáneas programadas regulares se toman automáticamente y se pueden usar para restaurar máquinas virtuales individuales. Las instantáneas programadas funcionan al tener programaciones de instantáneas de todo el grupo para las VM seleccionadas del grupo. Cuando se habilita una programación de instantáneas, las instantáneas de la máquina virtual especificada se toman a la hora programada cada hora, día o semana. Se pueden habilitar varias instantáneas programadas en un grupo, que cubren diferentes VM y con diferentes programaciones. Una máquina virtual solo se puede asignar a una programación de instantáneas a la vez.

XenCenter proporciona una variedad de herramientas para ayudarlo a usar esta función:

- Para definir una instantánea programada, utilice el asistente de **programación de nuevas instantáneas**.
- Para habilitar, inhabilitar, modificar y eliminar instantáneas programadas de un grupo, utilice el cuadro de diálogo **Programaciones de instantáneas de VM**.
- Para modificar una programación de instantáneas, abra su cuadro de diálogo **Propiedades** desde el cuadro de diálogo **Programaciones de instantáneas de VM**.
- Para revertir una VM a una instantánea programada, seleccione la instantánea en la ficha **Instantáneas** y revierta la VM a ella.

Para obtener más información, consulte Instantáneas programadas en la documentación de XenCenter.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hacer frente a los fallos de las

August 24, 2023

En esta sección se proporcionan detalles sobre cómo recuperarse de varios casos de error. Todos los casos de recuperación de errores requieren el uso de uno o más de los tipos de copia de seguridad enumerados en Copia de seguridad.

Fallas de miembros

En ausencia de HA, los nodos coordinadores del grupo detectan las fallas de los miembros al recibir mensajes de latidos regulares. Si no se ha recibido ningún latido durante 600 segundos, el coordinador del grupo asume que el miembro está muerto. Hay dos maneras de recuperarse de este problema:

- Repare el host muerto (por ejemplo, reiniciándolo físicamente). Cuando se restablece la conexión con el miembro, el coordinador del grupo vuelve a marcar al miembro como vivo.
- Apague el host e indique al coordinador del grupo que se olvide del nodo miembro mediante el comando de la interfaz de línea de comandos `xe host-forget`. Una vez que se olvida al miembro, todas las máquinas virtuales que se estaban ejecutando allí se marcan como desconectadas y se pueden reiniciar en otros hosts de XenServer.

  Es importante asegurarse de que el host de XenServer esté realmente desconectado; de lo contrario, podrían dañarse los datos de la máquina virtual.

  No divida su grupo en varios grupos de un solo host mediante el uso de `xe host-forget`. Esta acción puede provocar que todos asignen el mismo almacenamiento compartido y corrompan los datos de la VM.

> **Advertencia:**
>
> - Si va a volver a utilizar el host olvidado como host activo, realice una nueva instalación del software XenServer.
> - No utilice el comando `xe host-forget` si HA está habilitada en el grupo. Inhabilite primero HA, luego olvide el host y, a continuación, vuelva a habilitar HA.

Cuando se produce un error en un host de XenServer miembro, es posible que aún haya máquinas virtuales registradas en estado de ejecución. Si está seguro de que el host de XenServer miembro está definitivamente inactivo, utilice el comando `xe vm-reset-powerstate` CLI para configurar el estado de alimentación de las máquinas virtuales. `halted` Consulte vm-reset-powerstate para obtener más información.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Advertencia:**
>
> El uso incorrecto de este comando puede provocar daños en los datos. Utilice este comando solo si es necesario.

Antes de poder iniciar las máquinas virtuales en otro host de XenServer, también debe liberar los bloqueos del almacenamiento de las máquinas virtuales. Solo en un host a la vez puede usar cada disco en una SR. Es fundamental hacer que el disco sea accesible para otros hosts de XenServer una vez que se produce un error en un host. Para ello, ejecute el siguiente script en el coordinador del grupo de cada SR que contenga los discos de las máquinas virtuales afectadas: `/opt/xensource/sm/resetvdis.py host_UUID SR_UUID master`

Solo necesita proporcionar la tercera cadena («maestra») si el host que falló era el coordinador del grupo de SR en el momento del accidente. (El coordinador del grupo SR es el coordinador del grupo o un host de XenServer que utiliza almacenamiento local).

> **Advertencia:**
>
> Asegúrese de que el host esté inactivo antes de ejecutar este comando. El uso incorrecto de este comando puede provocar daños en los datos.

Si intenta iniciar una máquina virtual en otro host de XenServer antes de ejecutar el `resetvdis.py` script, recibirá el siguiente mensaje de error:. `VDI <UUID> already attached RW`

Fallos del coordinador de la piscina

Cada miembro de un grupo de recursos contiene toda la información necesaria para asumir el papel de coordinador del grupo si es necesario. Cuando se produce un error en un nodo coordinador de grupos, se produce la siguiente secuencia de eventos:

1. Si HA está habilitada, se elige automáticamente otro coordinador del grupo.
2. Si HA no está habilitada, cada miembro espera a que regrese el coordinador del grupo.

Si el coordinador de la agrupación vuelve a subir en este punto, restablece la comunicación con sus miembros y el funcionamiento vuelve a la normalidad.

Si el coordinador del grupo está muerto, elija uno de los miembros y ejecute el comando `xe pool-emergency-transition-to-master` en él. Una vez que se haya convertido en el coordinador de la piscina, ejecute el comando `xe pool-recover-slaves` y los miembros ahora señalarán al nuevo coordinador de la piscina.

Si repara o reemplaza el host que era el coordinador original del grupo, simplemente puede abrirlo, instalar el software XenServer y agregarlo al grupo. Dado que los hosts XenServer del grupo deben ser homogéneos, no hay necesidad real de convertir al host reemplazado en el coordinador del grupo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cuando un host miembro de XenServer pase a ser coordinador de grupos, compruebe que el repositorio de almacenamiento de grupo predeterminado tenga un valor adecuado. Esta comprobación se puede realizar mediante el comando `xe pool-param-list` y verificando que el parámetro **`default`**`-SR` apunta a un repositorio de almacenamiento válido.

Fallos de agrupación

En el desafortunado caso de que falle toda la agrupación de recursos, debe volver a crear la base de datos del grupo desde cero. Asegúrese de realizar copias de seguridad periódicas de los metadatos de su grupo mediante el comando `xe pool-dump-database` CLI (consulte `pool-dump-database`).

Para restaurar un grupo que ha fallado por completo:

1. Instale un conjunto nuevo de hosts. No los juntes en esta etapa.
2. Para el host designado como coordinador del grupo, restaure la base de datos del grupo desde la copia de seguridad mediante el comando `xe pool-restore-database` (consulte pool-restore-database).
3. Conéctese al coordinador del grupo mediante XenCenter y asegúrese de que todo el almacenamiento compartido y las máquinas virtuales estén disponibles de nuevo.
4. Realice una operación de unión a un grupo en los hosts miembros recién instalados restantes e inicie las máquinas virtuales en los hosts apropiados.

Hacer frente a la falla debido a errores de configuración

Si la máquina host física está operativa pero la configuración del software o del host está dañada:

1. Ejecute el siguiente comando para restaurar el software y la configuración del host:

```
1 xe host-restore host=host file-name=hostbackup
2 <!--NeedCopy-->
```

2. Reinicie en el CD de instalación del host y seleccione **Restaurar desde la copia de seguridad**.

Fallo de máquina física

Si la máquina host física ha fallado, utilice el procedimiento apropiado de la siguiente lista para recuperarse.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Advertencia:**
>
> Las máquinas virtuales que se ejecuten en un miembro anterior (o en el host anterior) que hayan fallado seguirán marcadas como `Running` en la base de datos. Este comportamiento es por seguridad. Iniciar simultáneamente una VM en dos hosts diferentes provocaría una corrupción grave del disco. Si está seguro de que las máquinas (y las máquinas virtuales) están fuera de línea, puede restablecer el estado de energía de la máquina virtual a `Halted`:
>
> `xe vm-reset-powerstate vm=vm_uuid --force`
>
> Las máquinas virtuales se pueden reiniciar mediante XenCenter o la CLI.

Para reemplazar un coordinador de grupo fallido por un miembro que aún está en funcionamiento:

1. Ejecute los comandos siguientes:

```
xe pool-emergency-transition-to-master
xe pool-recover-slaves
<!--NeedCopy-->
```

2. Si los comandos se ejecutan correctamente, reinicie las VM.

Para restaurar un grupo con todos los hosts fallidos:

1. Ejecute el comando:

```
xe pool-restore-database file-name=backup
<!--NeedCopy-->
```

> **Advertencia:**
>
> Este comando solo se ejecuta correctamente si el equipo de destino tiene un número adecuado de NIC con el nombre adecuado.

2. Si la máquina de destino tiene una vista del almacenamiento diferente a la de la máquina original, modifique la configuración de almacenamiento mediante el comando `pbd-destroy`. A continuación, ejecute el comando `pbd-create` para volver a crear configuraciones de almacenamiento. Consulte comandos pbd para obtener documentación de estos comandos.
3. Si ha creado una configuración de almacenamiento, utilice `pbd-plug` o el elemento de menú **Almacenamiento > Reparar repositorio de almacenamiento** en XenCenter para usar la nueva configuración.
4. Reinicie todas las VM.

Para restaurar una VM cuando el almacenamiento de VM no esté disponible:

1. Ejecute este comando:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe vm-import filename=backup metadata=true
<!--NeedCopy-->
```

2. Si la importación de metadatos falla, ejecute el comando:

```
xe vm-import filename=backup metadata=true --force
<!--NeedCopy-->
```

   Este comando intenta restaurar los metadatos de la máquina virtual según el "mejor esfuerzo".

3. Reinicie todas las VM.

---

layout: doc
description: Use Workload Balancing to create reports and recommendations about the placement of VMs in your XenServer pool.—

Balance de carga

> **Notas:**
>
> - Workload Balancing está disponible para los clientes de XenServer Premium Edition. Para obtener más información sobre las licencias de XenServer, consulte Licencias. Para actualizar o comprar una licencia de XenServer, visite el sitio web de XenServer.
> - Workload Balancing 8.3.0 y versiones posteriores son compatibles con XenServer 8. Si realiza una actualización sucesiva de grupos de Citrix Hypervisor 8.2 CU1 a XenServer 8, no podrá usar Workload Balancing 8.2.2 con los grupos de XenServer 8. Actualice el dispositivo virtual Workload Balancing a la versión 8.3.0 antes de realizar la actualización sucesiva del grupo. Puede descargar la versión más reciente del dispositivo virtual Workload Balancing desde la página de descargas de XenServer.

Workload Balancing es un componente de XenServer Premium Edition, empaquetado como un dispositivo virtual, que ofrece las siguientes funciones:

- Crear informes sobre el rendimiento de las máquinas virtuales (VM) en su entorno de XenServer
- Evaluar la utilización de los recursos y ubicar las máquinas virtuales en los mejores hosts posibles del grupo conforme a su carga de trabajo
- Equilibre las cargas de trabajo de máquinas virtuales entre los hosts de un grupo de recursos de XenServer
- Determinar el mejor host en el que iniciar una VM

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Determine el mejor host en el que reanudar una máquina virtual que apagó
- Determinar el mejor host al que mover una máquina virtual cuando se produce un error en un host
- Determine el servidor óptimo para cada una de las máquinas virtuales del host cuando ponga un host en modo de mantenimiento o lo saque de él

Según sus preferencias, el equilibrio de carga de trabajo puede llevar a cabo estas tareas automáticamente o solicitarle que acepte sus recomendaciones de reequilibrio y ubicación. También puede configurar Equilibrio de carga de trabajo para que apague los hosts automáticamente en momentos específicos del día. Por ejemplo, configure sus hosts para que se apaguen por la noche para ahorrar energía.

Workload Balancing puede enviar notificaciones en XenCenter sobre las acciones que realiza. Para obtener más información sobre cómo configurar el nivel de alerta para las alertas de equilibrio de carga de trabajo mediante la CLI xe, consulte Establecer el nivel de alerta para las alertas de equilibrio de carga de trabajo en XenCenter.

Funciones de equilibrio de carga de trabajo mediante la evaluación del uso de máquinas virtuales en un grupo. Cuando un host supera un umbral de rendimiento, Equilibrio de carga de trabajo reubica la VM en un host con menos impuestos del grupo. Para reequilibrar las cargas de trabajo, Equilibrio de carga de trabajo mueve las VM para equilibrar el uso de recursos en los hosts.

Para garantizar que las recomendaciones de reequilibrio y ubicación se alineen con las necesidades de su entorno, puede configurar Equilibrio de carga de trabajo para optimizar las cargas de trabajo de una de las siguientes maneras:

- Para maximizar el rendimiento de los recursos
- Para maximizar la cantidad de máquinas virtuales que caben en los hosts

Estos modos de optimización se pueden configurar para cambiar automáticamente en momentos predefinidos o permanecer siempre igual. Para obtener una granularidad adicional, ajuste la ponderación de las métricas de recursos individuales: CPU, red, disco y memoria.

Para ayudarle a realizar la planificación de la capacidad, el equilibrio de carga de trabajo proporciona informes históricos sobre el estado del host y el grupo, la optimización y el rendimiento de VM, y el historial de movimiento de VM.

Dado que el equilibrio de carga de trabajo captura datos de rendimiento, también puede utilizar este componente para generar informes, conocidos como informes de carga de trabajo, sobre su entorno virtualizado. Para obtener más información, consulte Generar informes de carga de trabajo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Conceptos básicos de equilibrio de carga

Cuando las máquinas virtuales se ejecutan, consumen recursos informáticos en el host físico. Estos recursos incluyen CPU, memoria, lecturas de red, escrituras de red, lecturas de disco y escrituras de disco. Algunas máquinas virtuales, según su carga de trabajo, pueden consumir más recursos de CPU que otras máquinas virtuales en el mismo host. La carga de trabajo se define por las aplicaciones que se ejecutan en una máquina virtual y sus transacciones de usuario. El consumo combinado de recursos de todas las máquinas virtuales de un host reduce los recursos disponibles en el host.

Workload Balancing captura datos para el rendimiento de los recursos en máquinas virtuales y hosts físicos y los almacena en una base de datos. Workload Balancing utiliza estos datos, combinados con las preferencias que establezca, para proporcionar recomendaciones de optimización y ubicación.

Las optimizaciones son una forma de "mejorar"los hosts para alinearlos con sus objetivos: Workload Balancing hace recomendaciones para redistribuir las máquinas virtuales entre los hosts del grupo a fin de aumentar el rendimiento o la densidad. Cuando el equilibrio de carga de trabajo hace recomendaciones, las hace a la luz de su objetivo: crear equilibrio o armonía en todos los hosts del grupo. Si el equilibrio de carga de trabajo actúa de acuerdo con estas recomendaciones, la acción se conoce como optimización.

Cuando se habilita el equilibrio de carga de trabajo, XenCenter proporciona clasificaciones de estrellas para indicar los hosts óptimos para iniciar una VM. También se proporcionan estas calificaciones:

- Cuándo quiere iniciar la VM cuando está apagada
- Cuándo quiere iniciar la VM cuando está suspendida
- Cuando quiera migrar la máquina virtual a un host diferente (modo de migración y mantenimiento)

Dentro de un contexto de equilibrio de carga de trabajo:

- El**rendimiento** es el uso de recursos físicos en un host (por ejemplo, la utilización de CPU, memoria, red y disco en un host). Al configurar Workload Balancing para maximizar el rendimiento, se recomienda colocar las máquinas virtuales para garantizar que haya la cantidad máxima de recursos disponibles para cada máquina virtual.
- La**densidad** es la cantidad de máquinas virtuales en un host. Cuando configura Equilibrio de carga de trabajo para maximizar la densidad, se recomienda colocar las VM para que pueda reducir la cantidad de hosts encendidos en un grupo. Garantiza que las VM tengan una potencia de cálculo adecuada.

El equilibrio de carga de trabajo no entra en conflicto con la configuración que ya especificó para la alta disponibilidad: estas funciones son compatibles.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

layout: doc
description: Discover the features added in the latest Workload Balancing virtual appliance.—

Novedades del equilibrio de carga de trabajo

La versión más reciente del dispositivo virtual de equilibrio de carga de trabajo es la versión 8.3.0. Puede descargar esta versión del dispositivo virtual Workload Balancing desde la página de descargas de XenServer.

Novedades de la versión 8.3.0

Publicado el 23 de febrero de 2023

Esta actualización incluye las siguientes mejoras:

- Ahora puede establecer el nivel de alerta para las alertas de Workload Balancing en XenCenter mediante la API de administración.

Esta actualización incluye cambios en la base de datos del WLB. Asegúrese de utilizar el script de migración proporcionado cuando actualice su WLB a esta versión. Para obtener más información sobre el uso del script de migración, consulte Migrar datos de un dispositivo virtual existente.

Problemas resueltos en la versión 8.3.0

Esta actualización corrige los siguientes problemas:

- Durante la ventana de mantenimiento del equilibrio de carga de trabajo, el equilibrio de carga de trabajo no puede proporcionar recomendaciones de ubicación Cuando se produce esta situación, aparece el error: "La detección de grupos 4010 no se ha completado. Mediante el algoritmo original". La ventana de mantenimiento del equilibrio de carga de trabajo dura menos de 20 minutos y, de forma predeterminada, se programa a medianoche.
- Para un dispositivo virtual de equilibrio de carga de trabajo versión 8.2.2 y posteriores que no use LVM, no puede ampliar el espacio disponible en disco.
- Debido a que una llamada a la API no responde, el equilibrio de carga de trabajo a veces se bloquea durante la detección de grupos.
- En XenCenter, el intervalo de fechas y algunas marcas de tiempo que se muestran en el informe de auditoría del grupo de equilibrio de carga de trabajo son incorrectos.
- En XenCenter, algunas cadenas no se muestran correctamente en los informes de carga de trabajo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si el dispositivo virtual de equilibrio de carga de trabajo se ejecuta durante mucho tiempo, el sistema operativo lo apaga por consumir mucha memoria.
- La base de datos no se reinicia automáticamente después de que el dispositivo virtual de equilibrio de carga de trabajo se cierre de forma anormal.

Versiones anteriores

En esta sección se enumeran las funciones de las versiones anteriores junto con sus problemas resueltos. Estas versiones anteriores se sustituyen por la versión más reciente del dispositivo virtual Workload Balancing. Actualice a la versión más reciente del dispositivo virtual de equilibrio de carga de trabajo cuando esté disponible.

XenCenter 8.2.2

Publicado el 30 de septiembre de 2021

Esta actualización incluye cambios en la base de datos del WLB. Asegúrese de utilizar el script de migración proporcionado cuando actualice su WLB a esta versión. Para obtener más información sobre el uso del script de migración, consulte Migrar datos de un dispositivo virtual existente.

Problemas resueltos Esta actualización incluye correcciones para los siguientes problemas:

- La base de datos de equilibrio de carga de trabajo puede crecer muy rápido y llenar el disco.
- Una condición de carrera a veces puede hacer que los registros se dupliquen en la base de datos del WLB. Cuando esto ocurre, es posible que el usuario vea el error: "WLB recibió una excepción desconocida".

XenCenter 8.2.1

Publicado el 15 de septiembre de 2020

Esta actualización incluye las siguientes mejoras:

- El script de migración ahora le permite migrar la base de datos de equilibrio de carga de trabajo del dispositivo virtual de equilibrio de carga de trabajo 8.0.0 (que se proporcionaba con Citrix Hypervisor 8.0 y 8.1) al dispositivo virtual de equilibrio de carga de trabajo 8.2.1 suministrado con Citrix Hypervisor 8.2.

  Para obtener más información sobre el uso del script de migración, consulte Migrar datos de un dispositivo virtual existente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problemas resueltos Esta actualización incluye correcciones para los siguientes problemas:

- Cuando se inician varias máquinas virtuales al mismo tiempo, Workload Balancing recomienda equilibrar la ubicación de las máquinas virtuales en todos los hosts del grupo de manera uniforme. Sin embargo, a veces Workload Balancing puede recomendar colocar varias máquinas virtuales en el mismo host de XenServer. Este problema se produce cuando Workload Balancing recibe comentarios tardíos de XAPI sobre la ubicación de VM.

---

layout: doc
description: Install and set up the Workload Balancing virtual appliance to benefit from the Workload Balancing feature in your XenServer pools.—

Comience con el equilibrio de carga de trabajo

Puede configurar el dispositivo virtual de Workload Balancing en solo unos pocos pasos:

1. Revise la información de requisitos previos y planifique el uso del equilibrio de cargade trabajo
2. Descargue el dispositivo virtual de equilibrio de cargade trabajo.
3. Importe el dispositivo virtual de equilibrio de carga de trabajo en XenCenter.
4. Configure el dispositivo virtual de equilibrio de carga de trabajo desde la consola del dispositivo virtual.
5. (Opcional) Si ya tiene una versión anterior de Workload Balancing instalada, puede migrar los datos de un dispositivo virtual existente.

   > **Nota:**
   >
   > Si realiza una actualización sucesiva de grupos de Citrix Hypervisor 8.2 CU1 a XenServer 8, no podrá usar Workload Balancing 8.2.2 y versiones anteriores con los grupos de XenServer 8. Actualice su dispositivo virtual Workload Balancing a la versión 8.3.0 antes de realizar la actualización sucesiva del grupo. Puede descargar la versión más reciente del dispositivo virtual Workload Balancing desde la página de descargas de XenServer.

6. Conecte el grupo al dispositivo virtual de Workload Balancing mediante XenCenter.

   La ficha Workload Balancing solo aparece en XenCenter si su grupo tiene la licencia requerida para usar Workload Balancing.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Antes de comenzar

El dispositivo virtual Workload Balancing es una única máquina virtual preinstalada diseñada para ejecutarse en un host XenServer. Antes de importarlo, revise la información y las consideraciones previas.

Requisitos previos

- Workload Balancing 8.3.0 y versiones posteriores son compatibles con XenServer 8. Recomendamos usar la consola de administración de XenCenter para importar el dispositivo virtual.
- Si realiza una actualización sucesiva de grupos de Citrix Hypervisor 8.2 CU1 a XenServer 8, no podrá usar Workload Balancing 8.2.2 y versiones anteriores con los grupos de XenServer 8. Actualice su dispositivo virtual Workload Balancing a la versión 8.3.0 antes de realizar la actualización sucesiva del grupo. Puede descargar la versión más reciente del dispositivo virtual Workload Balancing desde la página de descargas de XenServer.
- Si actualmente utiliza una versión anterior del dispositivo virtual de equilibrio de carga de trabajo, puede utilizar el script de migración para migrar los datos existentes cuando actualice a la versión más reciente. Para obtener más información, consulte Migrar desde un dispositivo virtual existente.
- El dispositivo virtual de Workload Balancing requiere un mínimo de 2 GB de RAM y 30 GB de espacio en disco para ejecutarse. De forma predeterminada, al dispositivo virtual de Workload Balancing se le asignan 2 vCPU. Este valor es suficiente para grupos que alojan 1000 VM. Por lo general, no es necesario aumentarlo. Reduzca la cantidad de CPU virtuales asignadas al dispositivo virtual solo si tiene un entorno pequeño. Para obtener más información, consulte Cambiar la configuración del dispositivo virtual de equilibrio de cargade trabajo.

Requisitos del grupo

Para equilibrar un grupo con Workload Balancing, el grupo debe cumplir los siguientes requisitos:

- Todos los anfitriones tienen una licencia de edición Premium
- Todos los hosts cumplen los requisitos para la migración en vivo:
  - Almacenamiento remoto compartido
  - Configuraciones de procesador similares
  - Gigabit Ethernet
- El grupo no contiene máquinas virtuales habilitadas para vGPU. Equilibrio de carga de trabajo no puede crear un plan de capacidad para las VM que tienen vGPU conectadas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Un solo dispositivo virtual de equilibrio de carga de trabajo puede administrar varios grupos hasta un máximo de 100 grupos, según los recursos del dispositivo virtual (vCPU, memoria, tamaño del disco). En estos grupos, el dispositivo virtual puede administrar hasta 1000 máquinas virtuales. Sin embargo, si un grupo tiene una gran cantidad de máquinas virtuales (por ejemplo, más de 400 máquinas virtuales), le recomendamos que utilice un dispositivo virtual de equilibrio de carga de trabajo solo para ese grupo.

Consideraciones

Antes de importar el dispositivo virtual, tenga en cuenta la siguiente información y realice los cambios apropiados en su entorno, según corresponda.

- **Puerto de comunicaciones**. Antes de iniciar el Asistente para configuración de equilibrio de carga de trabajo, determine el puerto sobre el que quiere que se comunique el dispositivo virtual de Workload Balancing. Se le solicitará este puerto durante la configuración de equilibrio de carga de trabajo. De forma predeterminada, el servidor de Workload Balancing usa 8012.

  > **Nota:**
  >
  > No configure el puerto de equilibrio de carga de trabajo en el puerto 443. El dispositivo virtual de Workload Balancing no puede aceptar conexiones a través del puerto 443 (el puerto TLS/HTTPS estándar).

- **Cuentas para equilibrio de carga de trabajo**. Hay tres cuentas diferentes que se utilizan al configurar el dispositivo virtual Workload Balancing y conectarlo a XenServer.

  El Asistente de configuración de equilibrio de carga de trabajo crea las siguientes cuentas con un nombre de usuario y una contraseña que especifique:

  - *Cuenta Workload Balancing*

    El host de XenServer utiliza esta cuenta para conectarse al servidor de equilibrio de carga de trabajo. De forma predeterminada, el nombre de usuario de esta cuenta es `wlbuser`. Este usuario se crea en el dispositivo virtual de Workload Balancing durante la configuración del equilibrio de carga

  - *Cuenta base de datos*

    Esta cuenta se utiliza para acceder a la base de datos de PostgreSQL en el dispositivo virtual de Workload Balancing. De forma predeterminada, el nombre de usuario es `postgres`. Establezca la contraseña para esta cuenta durante la configuración del equilibrio de carga de trabajo.

  Al conectar el dispositivo virtual Workload Balancing a un grupo de XenServer, debe especificar una cuenta existente:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - *Cuenta de XenServer*

    El dispositivo virtual Workload Balancing utiliza esta cuenta para conectarse al grupo de XenServer y leer los RRD. Asegúrese de que esta cuenta de usuario tenga los permisos para leer el grupo, el host y los RRD de máquinas virtuales de XenServer. Por ejemplo, proporcione las credenciales de un usuario que tenga la función `pool-admin` o `pool-operator`.

- **Monitorización en todos los grupos**. Puede colocar el dispositivo virtual de Workload Balancing en un grupo y supervisar un grupo diferente con él. (Por ejemplo, el dispositivo virtual de Workload Balancing está en el grupo A, pero lo utiliza para supervisar el grupo B.)
- **Sincronización horaria**. El dispositivo virtual de Workload Balancing requiere que el tiempo en el equipo físico que aloja el dispositivo virtual coincida con el que está en uso por el grupo supervisado. No hay forma de cambiar la hora en el dispositivo virtual de Workload Balancing. Recomendamos apuntar tanto el equipo físico que aloja Workload Balancing como los hosts del grupo que está supervisando al mismo servidor de hora de red (NTP).
- **XenServer y Workload Balancing se comunican a través de HTTPS**. Por tanto, durante la configuración del equilibrio de carga de trabajo, el equilibrio de carga de trabajo crea automáticamente un certificado autofirmado en su nombre Puede cambiar este certificado por uno de una entidad emisora de certificados o configurar XenServer para que verifique el certificado, o ambas opciones. Para obtener información, consulte los Certificados.
- **Almacenamiento de datos históricos y el tamaño del espacio en disco**. La cantidad de datos históricos que puede almacenar se basa en lo siguiente:

  - El tamaño del disco vDisk asignado a Workload Balancing (de forma predeterminada 30 GB)
  - El espacio mínimo requerido en disco, que es de 2048 MB de forma predeterminada y se controla mediante el parámetro `GroomingRequiredMinimumDiskSizeInMB` del archivo `wlb.conf`.

  Cuantos más datos históricos recopila el equilibrio de carga de trabajo, más precisas y equilibradas son las recomendaciones. Si quiere almacenar muchos datos históricos, puede realizar una de las siguientes acciones:

  - Archivar los datos tal como se describe en Archivar datos de base
  - Aumente el tamaño del disco virtual asignado al dispositivo virtual de equilibrio de carga de trabajo, tal como se describe en Ampliar el disco del dispositivo virtual

  Por ejemplo, si quiere utilizar la función de seguimiento de auditoría del grupo de equilibrio de carga de trabajo y configurar la granularidad del informe a media o superior.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Equilibrio de carga Equilibrio** Si quiere utilizar el dispositivo virtual de Workload Balancing para administrarse a sí mismo, especifique el almacenamiento remoto compartido al importar el dispositivo virtual.

  > **Nota:**
  >
  > Equilibrio de carga de trabajo no puede realizar la recomendación de ubicación Start On para el dispositivo virtual de Workload Balancing cuando se utiliza Equilibrio de carga La razón por la que Workload Balancing no puede hacer recomendaciones de ubicación cuando se administra a sí mismo es porque el dispositivo virtual debe estar en ejecución para realizar esa función. Sin embargo, puede equilibrar el dispositivo virtual de Workload Balancing del mismo modo que equilibraría cualquier otra VM que esté administrando.

- **Planifique el tamaño del grupo de recursos**. El equilibrio de carga de trabajo requiere configuraciones específicas para ejecutarse correctamente en grupos grandes. Para obtener más información, consulte Cambiar la configuración del dispositivo virtual de equilibrio de cargade trabajo.

Descargue el dispositivo virtual

El dispositivo virtual de Workload Balancing se empaqueta en el formato `.xva`. Puede descargar el dispositivo virtual desde la página de descargas de XenServer. Al descargar el archivo, guárdelo en una carpeta del disco duro local (normalmente en el equipo donde está instalado XenCenter).

Cuando se complete la descarga de `.xva`, puede importarla en XenCenter como se describe en Importar el dispositivo virtual de equilibrio de carga de trabajo.

Importar el dispositivo virtual de equilibrio de carga

Use XenCenter para importar el dispositivo virtual de Workload Balancing en un grupo.

Para importar el dispositivo virtual a XenServer:

1. Abra XenCenter.
2. Haga clic con el botón derecho en el grupo (o host) en el que quiere importar el paquete del dispositivo virtual y seleccione **Importar**.
3. Busque el paquete `vpx-wlb.xva`.
4. Seleccione el grupo o el servidor doméstico en el que quiere ejecutar el dispositivo virtual de Workload Balancing.

   Cuando selecciona el grupo, la VM se inicia automáticamente en el host más adecuado de ese grupo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Como alternativa, si no administra el dispositivo virtual de Workload Balancing mediante Workload Balancing, puede configurar un servidor doméstico para el dispositivo virtual de Workload Balancing. Esta configuración garantiza que el dispositivo virtual siempre se inicie en el mismo host.

5. Elija un repositorio de almacenamiento en el que almacenar el disco vDisk para el dispositivo virtual de Workload Balancing. Este repositorio debe tener un mínimo de 30 GB de espacio libre.

   Puede elegir entre almacenamiento local o remoto. Sin embargo, si elige almacenamiento local, no puede administrar el dispositivo virtual con Workload Balancing.

6. Defina las interfaces virtuales para el dispositivo virtual de Workload Balancing. En esta versión, Workload Balancing está diseñado para comunicarse en una única interfaz virtual.
7. Elija una red que pueda acceder al grupo que quiere que administre Workload Balancing.
8. Deje activada la casilla de verificación **Iniciar máquinas virtuales después de la importación** y haga clic en **Finalizar** para importar el dispositivo virtual.
9. Cuando termine de importar el archivo `.xva` de equilibrio de carga de trabajo, aparece la VM de equilibrio de carga de trabajo en el panel **Recursos** de XenCenter.

Después de importar el dispositivo virtual de equilibrio de carga de trabajo, configure el dispositivo virtual como se describe en Configuración del dispositivo virtual de equilibrio de cargade trabajo.

Configurar el dispositivo virtual Equilibrio de carga

Cuando termine de importar el dispositivo virtual de Workload Balancing, debe configurarlo antes de poder usarlo para administrar su grupo. Para guiarlo en la configuración, el dispositivo virtual de Workload Balancing le proporciona un asistente de configuración en XenCenter. Para mostrarlo, seleccione el dispositivo virtual en el panel **Recursos** y haga clic en la ficha **Consola**. Para todas las opciones, presione **Entrar** para aceptar la opción predeterminada.

1. **Después de importar el dispositivo virtual de Workload Balancing, haga clic en la ficha**
2. Escriba `yes` para aceptar los términos del acuerdo de licencia. Para rechazar el CLUF, escriba `no`.

   > **Nota:**
   >
   > El dispositivo virtual de Workload Balancing también está sujeto a las licencias contenidas en el directorio `/opt/vpx/wlb` del dispositivo virtual de equilibrio de carga de trabajo.

3. Introduzca y confirme una nueva contraseña raíz para la máquina virtual de Workload Balancing. Recomendamos seleccionar una contraseña segura.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Al introducir la contraseña, la consola no muestra marcadores de posición, como asteriscos, para los caracteres.

4. Introduzca el nombre del equipo que quiere asignar al dispositivo virtual de Workload Balancing.
5. Introduzca el sufijo de dominio para el dispositivo virtual.

   Por ejemplo, si el nombre de dominio completo (FQDN) del dispositivo virtual es `wlb-vpx-pos-pool.domain4.bedford4.ctx`, introduzca `domain4.bedford4.ctx`.

   > **Nota:**
   >
   > El dispositivo virtual de Workload Balancing no agrega automáticamente su FQDN al servidor del Sistema de nombres de dominio (DNS). Por lo tanto, si quiere que el grupo use un FQDN para conectarse a Workload Balancing, debe agregar el FQDN a su servidor DNS.

6. Ingrese `y` para usar DHCP para obtener la dirección IP automáticamente para la máquina virtual de Workload Balancing. De lo contrario, introduzca `n` y, a continuación, introduzca una dirección IP estática, una máscara de subred y una puerta de enlace para la máquina virtual.

   > **Nota:**
   >
   > El uso de DHCP es aceptable siempre que la concesión de la dirección IP no caduque. Es importante que la dirección IP no cambie: cuando cambia, interrumpe la conexión entre XenServer y Workload Balancing.

7. Introduzca un nombre de usuario para la base de datos de equilibrio de carga de trabajo o presione **Entrar** para utilizar el nombre de usuario predeterminado (postgres) de la cuenta de la base de datos.

   Va a crear una cuenta para la base de datos de equilibrio de carga de trabajo. Los servicios de equilibrio de carga de trabajo utilizan esta cuenta para leer/escribir en la base de datos de equilibrio de carga de Anote el nombre de usuario y la contraseña. Es posible que los necesite si alguna vez quiere administrar directamente a la base de datos PostgreSQL de equilibrio de carga de trabajo (por ejemplo, si quiere exportar datos).

8. Introduzca una contraseña para la base de datos de equilibrio de carga de trabajo Después de presionar **Entrar**, aparecen mensajes que indican que el Asistente de configuración está cargando objetos de base de datos.
9. Introduzca un nombre de usuario y una contraseña para Workload Balancing Server.

   Esta acción crea la cuenta que XenServer usa para conectarse a Workload Balancing. El nombre de usuario predeterminado es **wlbuser**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

10. Introduzca el puerto para el servidor de equilibrio de carga de trabajo. El servidor de equilibrio de carga de trabajo se comunica mediante este puerto.

    De forma predeterminada, el servidor de Workload Balancing usa 8012. El número de puerto no se puede establecer en 443, que es el número de puerto TLS predeterminado.

    > **Nota:**
    >
    > Si cambia el puerto aquí, especifique ese nuevo número de puerto cuando conecte el grupo a Workload Balancing. Por ejemplo, especificando el puerto en el cuadro de diálogo **Conectar al servidor WLB**.

    Asegúrese de que el puerto que especifique para Workload Balancing esté abierto en cualquier firewall.

    Después de presionar **Entrar**, el equilibrio de carga de trabajo continúa con la configuración del dispositivo virtual, incluida la creación de certificados autofirmados.

11. Ahora, también puede iniciar sesión en el dispositivo virtual al introducir el nombre de usuario de la VM (normalmente `root`) y la contraseña raíz que creó anteriormente. Sin embargo, solo es necesario iniciar sesión cuando quiere ejecutar comandos de Workload Balancing o modificar el archivo de configuración de Workload Balancing.

Después de configurar el equilibrio de carga de trabajo, conecte su grupo al dispositivo virtual de equilibrio de carga de trabajo como se describe en Conectarse al dispositivo virtual de equilibrio de cargade trabajo

Si es necesario, puede encontrar el archivo de configuración de equilibrio de carga de trabajo en la siguiente ubicación: `/opt/vpx/wlb/wlb.conf`. Para obtener más información, consulte Modificar el archivo de configuración de equilibrio de cargade trabajo

El archivo de registro de equilibrio de carga de trabajo se encuentra en esta ubicación: `/var/log/wlb/LogFile.log`. Para obtener más información, consulte Aumentar los detalles en el registro de equilibrio de cargade trabajo.

Conectarse al dispositivo virtual de equilibrio de carga de trabajo

Después de configurar el equilibrio de carga de trabajo, conecte los grupos que quiere administrar al dispositivo virtual de equilibrio de carga de trabajo mediante la CLI o XenCenter.

> **Nota:**
>
> Un solo dispositivo virtual de equilibrio de carga de trabajo puede administrar varios grupos hasta un máximo de 100 grupos, según los recursos del dispositivo virtual (vCPU, memoria, tamaño del disco). En estos grupos, el dispositivo virtual puede administrar hasta 1000

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> máquinas virtuales. Sin embargo, si un grupo tiene una gran cantidad de máquinas virtuales (por ejemplo, más de 400 máquinas virtuales), le recomendamos que utilice un dispositivo virtual de equilibrio de carga de trabajo solo para ese grupo.

Para conectar un grupo a su dispositivo virtual de equilibrio de carga de trabajo, necesita la siguiente información:

- Dirección IP o FQDN del dispositivo virtual de Workload Balancing
  - Para obtener la dirección IP del dispositivo virtual de Workload Balancing:
    1. En XenCenter, vaya a la ficha **Consola** del dispositivo virtual de Workload Balancing.
    2. Inicie sesión como `root` con la contraseña raíz que creó al importar el dispositivo.
    3. Ejecute el siguiente comando: `ifconfig`.
  - Para especificar el FQDN de equilibrio de carga de trabajo al conectarse al servidor de equilibrio de carga de trabajo, primero agregue su nombre de host y dirección IP a su servidor DNS.
- El número de puerto del dispositivo virtual de Workload Balancing. De forma predeterminada, XenServer se conecta al equilibrio de carga de trabajo en el puerto 8012.

  Modifique únicamente el número de puerto cuando lo haya cambiado durante la configuración de equilibrio de carga de trabajo. El número de puerto especificado durante la configuración de equilibrio de carga de trabajo, en cualquier regla de firewall y en el cuadro de diálogo **Conectar al servidor WLB** debe coincidir.
- Credenciales para la cuenta de equilibrio de carga de trabajo que creó durante la configuración de equilibrio de

  Esta cuenta se conoce a menudo como cuenta de usuario de equilibrio de carga de trabajo. XenServer usa esta cuenta para comunicarse con Workload Balancing. Creó esta cuenta en el dispositivo virtual de Workload Balancing durante la configuración de equilibrio de carga
- Credenciales para el grupo de recursos (es decir, el coordinador del grupo) que quiere que supervise el equilibrio de carga de trabajo.

  El dispositivo virtual Workload Balancing utiliza esta cuenta para conectarse al grupo de XenServer. Esta cuenta se crea en el coordinador del grupo de XenServer y tiene la función `pool-admin` or `pool-operator` .

Cuando se conecta por primera vez al equilibrio de carga de trabajo, utiliza los umbrales y la configuración predeterminados para equilibrar cargas de trabajo. Las funciones automáticas, como el modo de optimización automatizada, la administración de energía y la automatización, están inhabilitadas de forma predeterminada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Trabajar con certificados

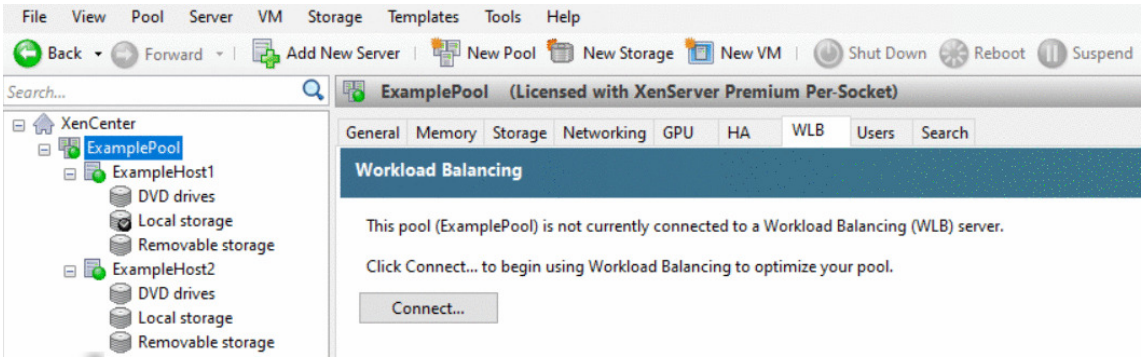
Si quiere cargar un certificado diferente (de confianza) o configurar la verificación de certificados, tenga en cuenta lo siguiente antes de conectar el grupo a Workload Balancing:

- Si quiere que XenServer verifique el certificado de equilibrio de carga de trabajo autofirmado, debe usar la dirección IP de equilibrio de carga de trabajo para conectarse a equilibrio de carga de trabajo. El certificado autofirmado se emite para Workload Balancing en función de su dirección IP.
- Si quiere utilizar un certificado de una entidad de certificación, es más fácil especificar el FQDN al conectarse a Workload Balancing. Sin embargo, puede especificar una dirección IP estática en el cuadro de diálogo **Conectar al servidor WLB**. Use esta dirección IP como el nombre alternativo del firmante (SAN) en el certificado.

Para obtener más información, consulte Certificados.

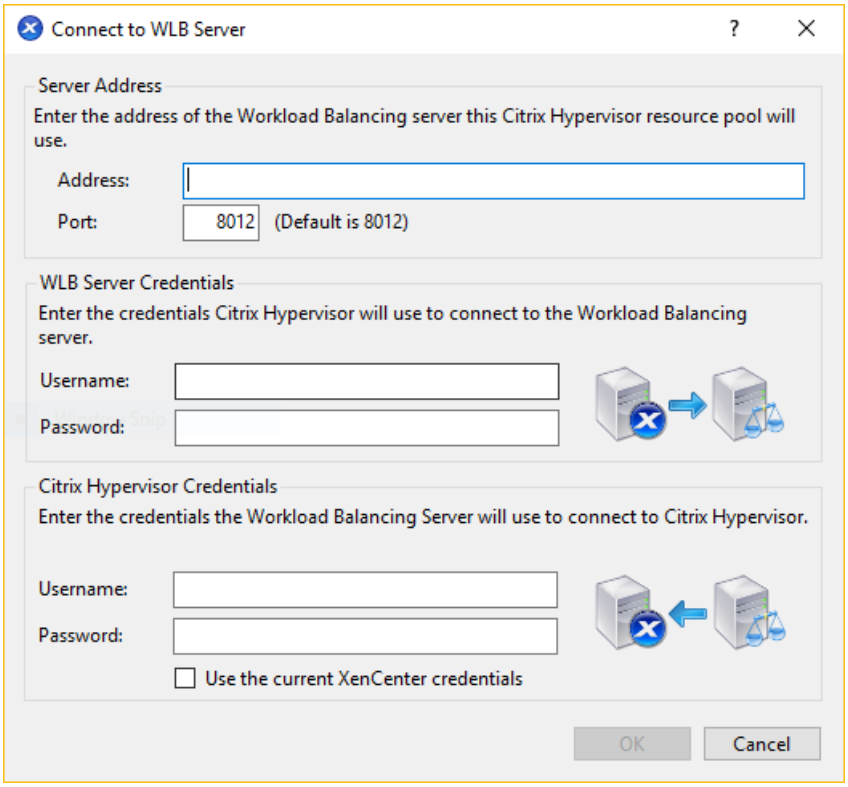
Para conectar su grupo al dispositivo virtual de Workload Balancing

1. En XenCenter, seleccione el grupo de recursos y, en su panel **Propiedades**, haga clic en la ficha **WLB**. La ficha **WLB** muestra el botón **Conectar**.



2. En la ficha **WLB**, haga clic en **Conectar**. Aparece el cuadro de diálogo **Conectarse al servidor WLB**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



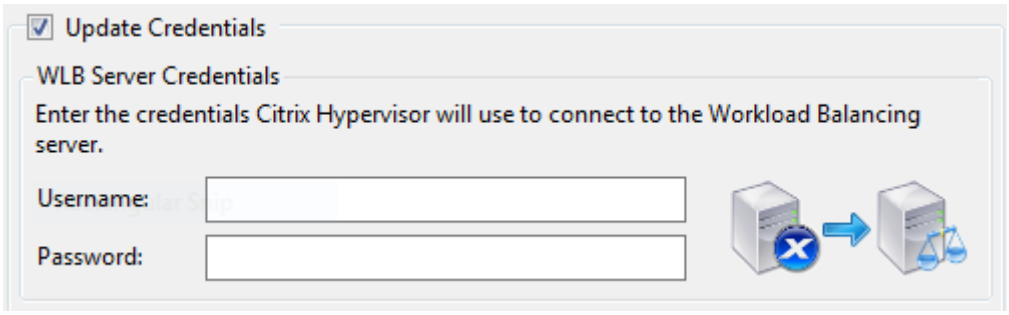
3. En la sección **Dirección del servidor**, introduzca lo siguiente:

   a) En el cuadro **Dirección**, escriba la dirección IP o el FQDN del dispositivo virtual de Workload Balancing. Por ejemplo, `WLB-appliance-computername.yourdomain.net`.

   b) (Opcional) Si cambió el puerto de equilibrio de carga de trabajo durante la configuración de equilibrio de carga de trabajo, introduzca el número de puerto en el cuadro **Puerto**. XenServer usa este puerto para comunicarse con Workload Balancing.

      De forma predeterminada, XenServer se conecta al equilibrio de carga de trabajo en el puerto 8012.

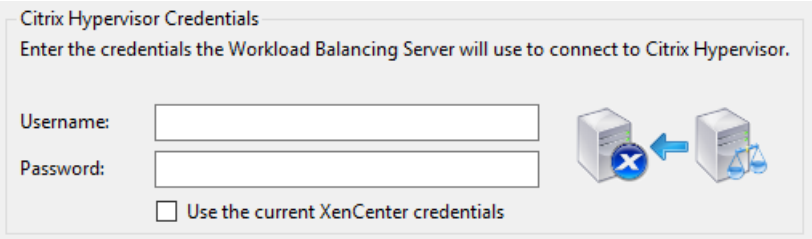
4. En la sección **Credenciales del servidor WLB**, introduzca el nombre de usuario y la contraseña que el grupo utiliza para conectarse al dispositivo virtual de Workload Balancing.



   Estas credenciales deben ser la cuenta que creó durante la configuración del equilibrio de carga de trabajo. De forma predeterminada, el nombre de usuario de esta cuenta es `wlbuser`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. En la sección **Credenciales de Citrix Hypervisor**, introduzca el nombre de usuario y la contraseña del grupo que está configurando. Workload Balancing utiliza estas credenciales para conectarse a los hosts del grupo.



   Para usar las credenciales con las que ha iniciado sesión actualmente en XenServer, seleccione **Usar las credenciales actuales de XenCenter**. Si ha asignado un rol a esta cuenta mediante la función Control de acceso (RBAC), asegúrese de que el rol tenga permisos suficientes para configurar Workload Balancing. Para obtener más información, consulte Permisos de control de acceso de equilibrio de cargade

Después de conectar el grupo al dispositivo virtual de Workload Balancing, el equilibrio de carga de trabajo comienza a supervisar automáticamente el grupo con la configuración de optimización predeterminada. Para modificar esta configuración o cambiar la prioridad dada a recursos específicos, espere al menos 60 segundos antes de continuar. O espere hasta que el registro de XenCenter muestre que la detección ha finalizado.

> **Importante:**
>
> Después de que el equilibrio de carga de trabajo se ejecute durante un tiempo, si no recibe recomendaciones de ubicación óptimas, evalúe sus umbrales de rendimiento. Esta evaluación se describe en Comprender cuándo el equilibrio de carga de trabajo hace recomendaciones. Es fundamental establecer el equilibrio de carga de trabajo en los umbrales correctos para su entorno o es posible que sus recomendaciones no sean apropiadas.

Migrar datos de un dispositivo virtual existente

Si utiliza el dispositivo virtual Workload Balancing suministrado con XenServer, puede usar el script de migración para migrar los datos existentes al actualizar a la versión más reciente (Workload Balancing 8.2.1 o posterior).

La versión de Workload Balancing que se proporciona actualmente con XenServer es 8.3.0. Sin embargo, Workload Balancing 8.2.0, 8.2.1 y 8.2.2 ya estaban disponibles con versiones anteriores de Citrix Hypervisor. También puede usar este script de migración para migrar de Workload Balancing 8.2.1 u 8.2.2 a Workload Balancing 8.3.0.

Para utilizar el script de migración, debe tener la siguiente información:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- La contraseña raíz del dispositivo virtual de equilibrio de carga de trabajo existente para el acceso SSH remoto
- La contraseña del usuario de la base de datos `postgres` en el dispositivo virtual de equilibrio de carga de trabajo existente
- La contraseña del usuario de la base de datos `postgres` en el nuevo dispositivo virtual de equilibrio de carga de trabajo

Deje el dispositivo virtual de Workload Balancing existente en ejecución en su grupo mientras completa los pasos de la migración.

1. Siga los pasos de la sección anterior para importar el nuevo dispositivo virtual de Workload Balancing.
2. En la consola SSH del nuevo dispositivo virtual de Workload Balancing, ejecute uno de los siguientes comandos.

   - Para el dispositivo virtual Workload Balancing 8.2.1, ejecute:

   ```
   /opt/vpx/wlb/migrate_db.sh 8.2.1 <IP of existing Workload Balancing appliance>
   ```

   - Para el dispositivo virtual Workload Balancing 8.2.2, ejecute:

   ```
   /opt/vpx/wlb/migrate_db.sh 8.2.2 <IP of existing Workload Balancing appliance>
   ```

   El comando le solicitará información sobre la contraseña cuando sea necesario.
3. Conecte el grupo de XenServer con el nuevo dispositivo virtual Workload Balancing.
4. Cuando esté satisfecho con el comportamiento de esta versión del dispositivo virtual de Workload Balancing, puede archivar la versión anterior del dispositivo virtual.

> **Notas:**
>
> - En el caso de un error no recuperable, vuelva a importar la versión más reciente del dispositivo virtual de Workload Balancing.
> - No desconecte el dispositivo virtual de equilibrio de carga de trabajo existente. De lo contrario, se eliminan los datos del dispositivo virtual existente.
> - Mantenga el dispositivo virtual de equilibrio de carga de trabajo existente hasta que se haya asegurado de que el nuevo dispositivo virtual de equilibrio de carga de trabajo funciona según sea necesario.
> - Si es necesario, puede revertir esta migración volviendo a conectar la versión anterior del dispositivo virtual Workload Balancing al grupo de XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

layout: doc
description: Use Workload Balancing to regularly perform these basic tasks that help you optimize your XenServer environment.—

Tareas básicas de equilibrio de carga

Cuando comienza a usar Equilibrio de carga de trabajo, hay algunas tareas básicas para las que utiliza el equilibrio de carga de trabajo con regularidad:

- Determinar el mejor host en el que ejecutar una máquina virtual
- Aceptar recomendaciones de optimización de equilibrio de carga
- Ejecución de informes sobre las cargas de trabajo en su entorno

Además de permitirle realizar estas tareas básicas, Workload Balancing es un potente componente de XenServer que optimiza las cargas de trabajo de su entorno. Las funciones que le permiten optimizar sus cargas de trabajo incluyen:

- Administración de energía del host
- Cambios en el modo de optimización de la programación
- Ejecución de informes
- Ajuste de los criterios que utiliza el equilibrio de carga de trabajo para hacer recomendaciones de optimización.

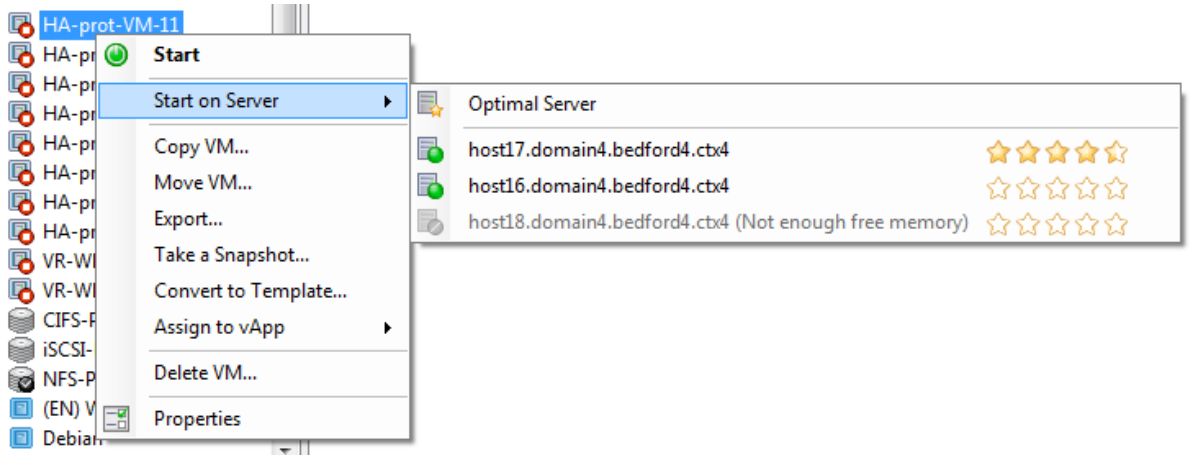
Para obtener más información sobre estas funciones más complejas, consulte Administrar el equilibrio de carga de trabajo.

> **Notas:**
>
> - Workload Balancing está disponible para los clientes de XenServer Premium Edition. Para obtener más información sobre las licencias de XenServer, consulte Licencias. Para actualizar o comprar una licencia de XenServer, visite el sitio web de XenServer.
> - Workload Balancing 8.3.0 es compatible con XenServer 8 y Citrix Hypervisor 8.2 CU1.

Determine el mejor host en el que ejecutar una máquina virtual

Cuando ha habilitado Equilibrio de carga de trabajo y reinicia una máquina virtual sin conexión, XenCenter recomienda los miembros del grupo óptimos para iniciar la máquina virtual. Las recomendaciones también se conocen como calificaciones con estrellas, ya que las estrellas se utilizan para indicar el mejor anfitrión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Cuando se habilita el equilibrio de carga de trabajo, XenCenter proporciona clasificaciones de estrellas para indicar los hosts óptimos para iniciar una VM. También se proporcionan estas calificaciones:

- Cuándo quiere iniciar la VM cuando está apagada
- Cuándo quiere iniciar la VM cuando está suspendida
- Cuando quiera migrar la máquina virtual a un host diferente (modo de migración y mantenimiento)

Cuando utiliza estas funciones con el equilibrio de carga de trabajo habilitado, las recomendaciones de host aparecen como clasificaciones de estrellas junto al nombre del host físico. Cinco estrellas vacías indican el anfitrión con la calificación más baja y, por lo tanto, el menos óptimo. Si no puede iniciar o migrar una máquina virtual a un host, el nombre del host aparece atenuado en el comando de menú para una función de ubicación. La razón por la que no puede aceptar la VM aparece junto a ella.

El término *óptimo* indica el host físico más adecuado para alojar su carga de trabajo. Existen varios factores que utiliza el equilibrio de carga de trabajo para determinar qué host es óptimo para una carga de trabajo:

- **La cantidad de recursos disponibles en cada host del grupo**. Cuando un grupo se ejecuta en modo de rendimiento máximo, Equilibrio de carga de trabajo intenta equilibrar las máquinas virtuales en los hosts para que todas las máquinas virtuales tengan un buen rendimiento. Cuando un grupo se ejecuta en modo de densidad máxima, el equilibrio de carga de trabajo coloca las máquinas virtuales en los hosts con la mayor densidad posible y, al mismo tiempo, garantiza que las máquinas virtuales tengan recursos suficientes.
- **El modo de optimización en el que se ejecuta la agrupación (rendimiento máximo o densidad máxima)**. Cuando un grupo se ejecuta en modo de rendimiento máximo, el equilibrio de carga de trabajo coloca las máquinas virtuales en los hosts con la mayor cantidad de recursos disponibles del tipo que requiere la máquina virtual. Cuando un grupo se ejecuta en modo

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Densidad máxima, Equilibrio de carga de trabajo coloca las máquinas virtuales en los hosts que ya tienen máquinas virtuales en ejecución. Este enfoque garantiza que las VM se ejecuten en el menor número posible de hosts.

- **La cantidad y el tipo de recursos que requiere la VM**. Después de que Equilibrio de carga de trabajo supervisa una VM durante un tiempo, utiliza las métricas de VM para hacer recomendaciones de ubicación de acuerdo con el tipo de recursos que requiere la VM. Por ejemplo, Equilibrio de carga de trabajo puede seleccionar un host con menos CPU disponible pero más memoria disponible si es lo que requiere la VM.

En general, el equilibrio de carga de trabajo funciona de manera más eficaz y hace recomendaciones de optimización mejores y menos frecuentes si inicia máquinas virtuales en los hosts que recomienda. Para seguir las recomendaciones del anfitrión, usa una de las funciones de ubicación para seleccionar el anfitrión con más estrellas a su lado. Las recomendaciones de ubicación también pueden resultar útiles en entornos de Citrix Virtual Desktops.

Para iniciar una máquina virtual en el host óptimo

1. En el panel Recursos de XenCenter, seleccione la máquina virtual que quiere iniciar.
2. En el menú VM, seleccione Iniciar en el servidor y, a continuación, seleccione una de las siguientes opciones:
   - **Servidor óptimo**. El servidor óptimo es el host físico que mejor se adapta a las demandas de recursos de la VM que está iniciando. Equilibrio de carga de trabajo determina el servidor óptimo en función de sus registros históricos de métricas de rendimiento y su estrategia de ubicación. El servidor óptimo es el anfitrión con más estrellas.
   - **Uno de los servidores con puntuaciones por estrellas** que figuran en el comando Servidor óptimo. Cinco estrellas indican el anfitrión más recomendado (óptimo) y cinco estrellas vacías indican el anfitrión menos recomendado.

> **Sugerencia:**
>
> También puede seleccionar Iniciar en el servidor haciendo clic con el botón derecho en la máquina virtual que quiere iniciar en el panel Recursos.

Para reanudar una máquina virtual en el host óptimo

1. En el panel Recursos de XenCenter, seleccione la máquina virtual suspendida que quiere reanudar.
2. En el menú VM, seleccione Reanudar en el servidor y, a continuación, seleccione una de las siguientes opciones:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Servidor óptimo**. El servidor óptimo es el host físico que mejor se adapta a las demandas de recursos de la VM que está iniciando. Equilibrio de carga de trabajo determina el servidor óptimo en función de sus registros históricos de métricas de rendimiento y su estrategia de ubicación. El servidor óptimo es el anfitrión con más estrellas.
- **Uno de los servidores con puntuaciones por estrellas** que figuran en el comando Servidor óptimo. Cinco estrellas indican el anfitrión más recomendado (óptimo) y cinco estrellas vacías indican el anfitrión menos recomendado.

> **Sugerencia:**
>
> También puede seleccionar Reanudar en el servidor haciendo clic con el botón secundario en la VM suspendida en el panel Recursos.

Aceptar recomendaciones de optimización de equilibrio de carga

Después de ejecutar el equilibrio de carga de trabajo durante un tiempo, comienza a hacer recomendaciones sobre las formas en que puede mejorar su entorno. Por ejemplo, si su objetivo es mejorar la densidad de máquinas virtuales en los hosts, en algún momento, el equilibrio de carga de trabajo puede recomendar que consolide las máquinas virtuales en un host. Si no se ejecuta en modo automatizado, puede elegir entre aceptar esta recomendación y aplicarla o ignorarla.

> **Importante:**
>
> Después de que el equilibrio de carga de trabajo se ejecute durante un tiempo, si no recibe recomendaciones de ubicación óptimas, evalúe sus umbrales de rendimiento. Esta evaluación se describe en Comprender cuándo el equilibrio de carga de trabajo hace recomendaciones. Es fundamental establecer el equilibrio de carga de trabajo en los umbrales correctos para su entorno o es posible que sus recomendaciones no sean apropiadas.

Las recomendaciones de optimización se basan en los siguientes criterios:

- La estrategia de colocación que seleccione (es decir, el modo de optimización).

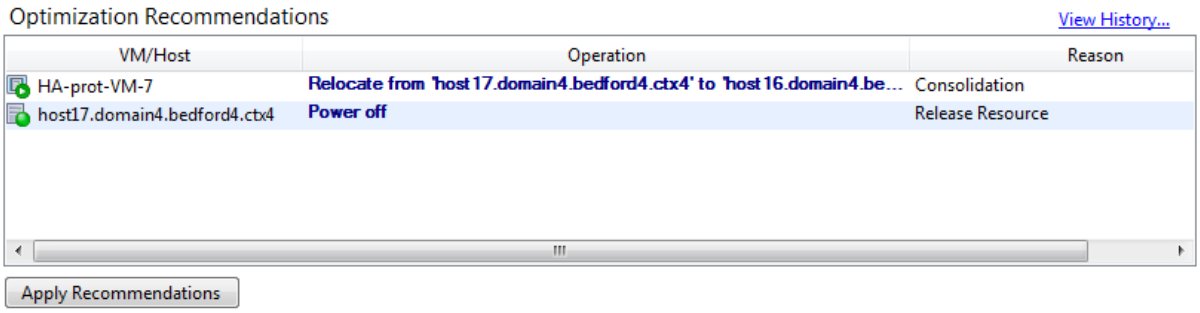
  Descubra el modo de optimización de un grupo mediante XenCenter para seleccionar el grupo. Consulte la sección Configuración de la ficha WLB para obtener información.
- Métricas de rendimiento para recursos como la utilización de la CPU, la memoria, la red y el disco de un host físico.
- La función del host en el grupo de recursos.

  Al hacer recomendaciones de ubicación, el equilibrio de carga de trabajo considera al coordinador del grupo para la colocación de VM solo si ningún otro host puede aceptar la carga de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

trabajo. Del mismo modo, cuando un grupo funciona en modo de densidad máxima, el equilibrio de carga de trabajo considera al coordinador del grupo en último lugar al determinar el orden para llenar los hosts con máquinas virtuales.

Las recomendaciones de optimización aparecen en la ficha **Optimización de WLB** en XenCenter.



Las recomendaciones de optimización muestran la siguiente información:

- El nombre de la máquina virtual que Workload Balancing recomienda reubicar
- El host en el que reside actualmente la VM
- El equilibrio de carga de trabajo del host recomienda como la nueva ubicación.

Las recomendaciones de optimización también muestran el motivo por el que Workload Balancing recomienda mover la VM. Por ejemplo, la recomendación muestra "CPU"para mejorar el uso de la CPU. Cuando la administración de energía del equilibrio de carga de trabajo está habilitada, el equilibrio de carga de trabajo también muestra recomendaciones de optimización para los hosts que recomienda encender o apagar. Específicamente, estas recomendaciones son para consolidaciones.

Puede hacer clic en **Aplicar recomendaciones**para realizar todas las operaciones enumeradas en la lista Recomendaciones de optimización.

Para aceptar una recomendación de optimización

1. En el panel Recursos de XenCenter, seleccione el grupo de recursos para el que quiere mostrar recomendaciones.
2. Haga clic en la ficha WLB. Si hay optimizaciones recomendadas para cualquier máquina virtual en el grupo de recursos seleccionado, se muestran en la sección Recomendaciones de optimización de la ficha WLB.
3. Para aceptar las recomendaciones, haga clic en Aplicar recomendaciones. XenServer comienza a realizar todas las operaciones enumeradas en la columna Operaciones de la sección Recomendaciones de optimización.

   Después de hacer clic en Aplicar recomendaciones, XenCenter muestra automáticamente la ficha Registros para que pueda ver el progreso de la migración de la máquina virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Comprender las recomendaciones de equilibrio de carga de trabajo en

Si tiene el equilibrio de carga de trabajo y la alta disponibilidad de XenServer habilitados en el mismo grupo, es útil entender cómo interactúan las dos funciones. El equilibrio de carga de trabajo está diseñado para no interferir con la alta disponibilidad. Cuando hay un conflicto entre una recomendación de equilibrio de carga de trabajo y una configuración de **alta disponibilidad, la configuración de alta disponibilidad** siempre tiene prioridad. En la práctica, esta precedencia significa que:

- Si intentar iniciar una VM en un host infringe el plan de alta disponibilidad, Equilibrio de carga de trabajo no le da calificaciones con estrellas.
- Equilibrio de carga de trabajo no apaga automáticamente ningún host que supere el número especificado en el cuadro de diálogo **Configurar alta disponibilidad**.
  - Sin embargo, el equilibrio de carga de trabajo aún puede hacer recomendaciones para apagar más hosts que la cantidad de errores de host que se deben tolerar. (Por ejemplo, Equilibrio de carga de trabajo aún recomienda apagar dos hosts cuando la alta disponibilidad solo está configurada para tolerar una falla de host). Sin embargo, cuando intenta aplicar la recomendación, XenCenter puede mostrar un mensaje de error que indica que la alta disponibilidad ya no está garantizada.
  - Cuando el equilibrio de carga de trabajo se ejecuta en modo automatizado y tiene habilitada la administración de energía, se ignoran las recomendaciones que exceden la cantidad de errores de host tolerados. En esta situación, el registro de equilibrio de carga de trabajo muestra un mensaje que indica que la recomendación de administración de energía no se aplicó porque la alta disponibilidad está habilitada.

Generar informes de carga

Equilibrio de carga de trabajo captura datos de rendimiento y puede usar estos datos para generar informes, conocidos como informes de carga de trabajo, sobre su entorno virtualizado, incluidos informes sobre hosts y máquinas virtuales. Los informes de equilibrio de carga de trabajo pueden ayudarlo a planificar la capacidad, determinar el estado del servidor virtual y evaluar la eficacia de los niveles de umbral configurados.

Puede utilizar el informe de estado del grupo para evaluar la eficacia de sus umbrales de optimización. Si bien el equilibrio de carga de trabajo proporciona una configuración de umbral predeterminada, es posible que deba ajustar estos valores predeterminados para que proporcionen valor en su entorno. Si no tiene los umbrales de optimización ajustados al nivel correcto para su entorno, es posible que las recomendaciones de equilibrio de carga de trabajo no sean adecuadas para su entorno.

Para ejecutar informes, no es necesario configurar el equilibrio de carga de trabajo para hacer recomendaciones de ubicación o mover máquinas virtuales. Sin embargo, debe configurar el compo-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

nente Equilibrio de carga de trabajo. Idealmente, debe establecer umbrales críticos en valores que reflejen el punto en el que se degrada el rendimiento de los hosts de su grupo. Idealmente, el grupo ha estado ejecutando Equilibrio de carga de trabajo durante un par de horas o el tiempo suficiente para generar los datos que se mostrarán en los informes.

Equilibrio de carga de trabajo permite generar informes sobre tres tipos de objetos: Hosts físicos, grupos de recursos y máquinas virtuales. En un nivel alto, el equilibrio de carga de trabajo proporciona dos tipos de informes:

- Informes históricos que muestran información por fecha
- Informes de estilo "Roll up", que proporcionan una visión general resumida de un área
- Informes con fines de auditoría, para que pueda determinar, por ejemplo, la cantidad de veces que se movió una VM
- Informe de devolución de cargo que muestra el uso de VM y puede ayudarle a medir y asignar costes

Generar un informe de equilibrio de carga

1. En XenCenter, en el menú **Agrupación**, seleccione **Ver informes de carga de trabajo**.

   También puede mostrar la pantalla **Informes de carga** de trabajo desde la ficha **WLB** haciendo clic en el botón **Informes**.

2. En la pantalla **Informes de carga** de trabajo, seleccione un informe en el panel **Informes**.
3. Seleccione la **fecha de inicio** y la **fecha de finalización** para el período del informe. Según el informe que seleccione, es posible que deba especificar un host en la lista **Hosts**.
4. Haga clic en **Ejecutar informe**. El informe se muestra en la ventana del informe. Para obtener información sobre el significado de los informes, consulte Glosario de informes Equilibriode carga de trabajo.

Navegar en un informe de equilibrio de carga

Después de generar un informe, puede usar los botones de la barra de herramientas del informe para navegar y realizar ciertas tareas. Para mostrar el nombre de un botón de barra de herramientas, coloque el ratón sobre el icono de la barra de herramientas.

Botones de barras	Descripción
	El mapa del documento le permite mostrar un mapa del documento que le

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Botones de barras	Descripción
	Avanzar/retroceder página le permite avanzar o retroceder una página en
	Volver al informe principal le permite volver al informe principal cuando t
	Detener generación cancela la generación del informe.
	Imprimir le permite imprimir un informe y especificar opciones de impresió
	Diseño de impresión le permite mostrar una vista previa del informe antes
	Configurar página le permite especificar opciones de impresión, como el ta
	Exportar le permite exportar el informe como archivo de Acrobat (.PDF) o c
	Buscar le permite buscar una palabra en un informe, como el nombre de un

Exportar un informe de equilibrio de carga

Puede exportar un informe en formato Microsoft Excel o Adobe Acrobat (PDF).

1. Después de generar el informe, haga clic en el siguiente botón Exportar:
2. Seleccione uno de los siguientes elementos del menú del botón Exportar:
   - Excel
   - Archivo Acrobat (PDF)

> **Nota:**
>
> Según el formato de exportación que seleccione, el informe contiene diferentes cantidades de datos. Los informes exportados a Excel incluyen todos los datos disponibles para los informes, incluidos los datos de "profundización". Los informes exportados a PDF y mostrados en XenCenter solo contienen los datos que seleccionó al generar el informe.

Glosario de informes Informe de equilibrio de carga de trabajo

En esta sección se proporciona información sobre los siguientes informes de equilibrio de carga de trabajo:

- Análisis de utilización de contracargos
- Historial de estado del anfitrión
- Historial de rendimiento de optimización de grupos

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Seguimiento de auditoría de grupos
- Estado del grupo
- Historial de estado del grupo
- Historial de optimización de grupos
- Historial de movimiento de máquinas virtuales
- Historial de rendimiento de máquinas virtuales

Análisis de utilización de contracargos

Puede usar el informe Análisis de utilización de contracargos ("informe de reversión de cargo") para determinar qué cantidad de un recurso utilizó un departamento específico de su organización. Específicamente, el informe muestra información sobre todas las máquinas virtuales del grupo, incluida su disponibilidad y el uso de recursos. Como este informe muestra el tiempo de actividad de la VM, puede ayudarlo a demostrar el cumplimiento y la disponibilidad de los acuerdos de nivel de servicio.

El informe de reversión de cargo puede ayudarlo a implementar una solución de devolución de cargo simple y facilitar la facturación. Para facturar a los clientes por un recurso específico, genera el informe, guárdalo como Excel y modifica la hoja de cálculo para incluir el precio por unidad. Como alternativa, puede importar los datos de Excel a su sistema de facturación.

Si quiere facturar a clientes internos o externos por el uso de VM, considere incorporar nombres de departamento o cliente en sus convenciones de nomenclatura de VM. Esta práctica facilita la lectura de los informes de reversión de cargo.

Los informes de recursos en el informe de reversión de cargo se basan, a veces, en la asignación de recursos físicos a las VM individuales.

Los datos de memoria promedio de este informe se basan en la cantidad de memoria asignada actualmente a la VM. XenServer le permite tener una asignación de memoria fija o una asignación de memoria que se ajuste automáticamente (Control dinámico de memoria).

El informe de reversión de cargo contiene las siguientes columnas de datos:

- **Nombre de VM**. El nombre de la máquina virtual a la que se aplican los datos de las columnas de esa fila.
- **Tiempo de actividad de VM**. La cantidad de minutos que la VM estuvo encendida (o, más específicamente, aparece con un icono verde al lado en XenCenter).
- **Asignación de vCPU**. La cantidad de CPU virtuales configuradas en la VM. Cada CPU virtual recibe una parte igual de las CPU físicas en el host. Por ejemplo, considere el caso en el que configuró ocho CPU virtuales en un host que contiene dos CPU físicas. Si la columna **Asignación de vCPU** contiene "1", este valor es igual a 2/16 de la potencia de procesamiento total del host.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Uso mínimo de CPU (%)**. El valor registrado más bajo para el uso de CPU virtual en el período del informe. Este valor se expresa como un porcentaje de la capacidad de vCPU de la VM. La capacidad se basa en la cantidad de vCPU asignadas a la VM. Por ejemplo, si asignó una vCPU a una VM, el **uso mínimo de CPU** representa el porcentaje más bajo de uso de vCPU que se registra. Si asignó dos vCPU a la VM, el valor es el uso más bajo de la capacidad combinada de ambas vCPU como porcentaje.

  En última instancia, el porcentaje de uso de CPU representa la carga de trabajo registrada más baja que manejó la CPU virtual. Por ejemplo, si asigna una vCPU a una VM y la PCPU del host es de 2,4 GHz, se asignan 0,3 GHz a la VM. Si el **uso mínimo de CPU** para la máquina virtual era del 20%, el uso más bajo de la CPU del host físico de la máquina virtual durante el período del informe fue de 60 MHz.

- **Uso máximo de CPU (%)**. El porcentaje más alto de la capacidad de CPU virtual de la VM que la VM consumió durante el período del informe. La capacidad de CPU consumida es un porcentaje de la capacidad de CPU virtual que asignó a la VM. Por ejemplo, si asignó una vCPU a la VM, el uso máximo de CPU representa el porcentaje más alto registrado de uso de vCPU durante el tiempo informado. Si asignó dos CPU virtuales a la VM, el valor de esta columna representa la mayor utilización de la capacidad combinada de ambas CPU virtuales.

- **Uso medio de CPU (%)**. La cantidad promedio, expresada como porcentaje, de la capacidad de CPU virtual de la VM que se usó durante el período del informe. La capacidad de la CPU es la capacidad de la CPU virtual que asignó a la VM. Si asignó dos CPU virtuales a la VM, el valor de esta columna representa el uso promedio de la capacidad combinada de ambas CPU virtuales.

- **Asignación total de almacenamiento (GB)**. La cantidad de espacio en disco que está asignado actualmente a la máquina virtual en el momento en que se ejecutó el informe. Con frecuencia, a menos que lo haya modificado, este espacio en disco es la cantidad de espacio en disco que asignó a la máquina virtual cuando la creó.

- **Asignación de NIC virtuales**. La cantidad de interfaces virtuales (VIF) asignadas a la VM.

- **Memoria dinámica mínima actual (MB)**.

  - **Asignación de memoria fija**. Si asignó a una máquina virtual una cantidad fija de memoria (por ejemplo, 1024 MB), la misma cantidad de memoria aparece en las siguientes columnas: memoria dinámica mínima actual (MB), memoria dinámica máxima actual (MB), memoria asignada actual (MB) y memoria asignada promedio (MB).

  - **Asignación de memoria dinámica**. Si configuró XenServer para usar el Control dinámico de memoria, la cantidad mínima de memoria especificada en el rango aparece en esta columna. Si el rango tiene 1024 MB como memoria mínima y 2048 MB como memoria máxima, la columna **Memoria dinámica mínima actual (MB)** muestra 1024 MB.

- **Memoria dinámica máxima actual (MB)**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Asignación de memoria dinámica**. Si XenServer ajusta la memoria de una máquina virtual automáticamente en función de un rango, la cantidad máxima de memoria especificada en el rango aparece en esta columna. Por ejemplo, si los valores del rango de memoria son 1024 MB como mínimo y 2048 MB como máximo, aparecerán 2.048 MB en la columna **Memoria dinámica máxima actual (MB)**.
  - **Asignación de memoria fija**. Si asigna a una máquina virtual una cantidad fija de memoria (por ejemplo, 1024 MB), la misma cantidad de memoria aparece en las siguientes columnas: memoria dinámica mínima actual (MB), memoria dinámica máxima actual (MB), memoria asignada actual (MB) y memoria asignada promedio (MB).

- **Memoria asignada actual (MB)**.
  - **Asignación de memoria dinámica**. Cuando se configura el Control dinámico de memoria, este valor indica la cantidad de memoria que XenServer asigna a la máquina virtual cuando se ejecuta el informe.
  - **Asignación de memoria fija**. Si asigna a una máquina virtual una cantidad fija de memoria (por ejemplo, 1024 MB), la misma cantidad de memoria aparece en las siguientes columnas: memoria dinámica mínima actual (MB), memoria dinámica máxima actual (MB), memoria asignada actual (MB) y memoria asignada promedio (MB).

> **Nota:**
>
> Si cambia la asignación de memoria de la máquina virtual inmediatamente antes de ejecutar este informe, el valor reflejado en esta columna refleja la nueva asignación de memoria que configuró.

- **Memoria asignada media (MB)**.
  - **Asignación de memoria dinámica**. Cuando se configura el Control dinámico de memoria, este valor indica la cantidad media de memoria que XenServer asignó a la máquina virtual durante el período del informe.
  - **Asignación de memoria fija**. Si asigna a una máquina virtual una cantidad fija de memoria (por ejemplo, 1024 MB), la misma cantidad de memoria aparece en las siguientes columnas: memoria dinámica mínima actual (MB), memoria dinámica máxima actual (MB), memoria asignada actual (MB) y memoria asignada promedio (MB).

> **Nota:**
>
> Si cambia la asignación de memoria de la máquina virtual inmediatamente antes de ejecutar este informe, es posible que el valor de esta columna no cambie con respecto al que se

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> mostraba anteriormente. El valor de esta columna refleja el promedio durante el período de tiempo.

- **Lecturas de red promedio (BPS)**. La cantidad promedio de datos (en bits por segundo) que la VM recibió durante el período del informe.
- **Escrituras de red promedio (BPS)**. La cantidad promedio de datos (en bits por segundo) que la VM envió durante el período del informe.
- **Uso medio de red (BPS)**. El total combinado (en bits por segundo) de las lecturas de red promedio y las escrituras de red promedio. Si una VM envía, en promedio, 1027 bps y recibe, en promedio, 23.831 bps durante el período del informe, el uso promedio de red es el total combinado de estos valores: 24.858 bps.
- **Uso total de red (BPS)**. El total de todas las transacciones de lectura y escritura de la red en bits por segundo durante el período del informe.

Historial de estado del anfitrión

Este informe muestra el rendimiento de los recursos (CPU, memoria, lecturas de red y escrituras de red) en un host específico en relación con los valores de umbral.

Las líneas de colores (rojo, verde, amarillo) representan los valores de umbral. Puede usar este informe junto con el informe de estado del grupo para un anfitrión para determinar cómo el rendimiento del anfitrión puede afectar al estado general del grupo. Al modificar los umbrales de rendimiento, puede utilizar este informe para obtener información sobre el rendimiento del host.

Puede mostrar la utilización de recursos como un promedio diario u horario. El promedio por hora le permite ver las horas más ocupadas del día, promediadas, para el período de tiempo.

Para ver los datos del informe agrupados por hora, en **Historial de estado del anfitrión**, expanda **Haga clic para ver los datos del informe agrupados por casa durante el período de tiempo**.

Equilibrio de carga de trabajo muestra el promedio de cada hora para el período de tiempo que establezca. El punto de datos se basa en un promedio de utilización de esa hora para todos los días del período de tiempo. Por ejemplo, en un informe del 1 de mayo de 2009 al 15 de mayo de 2009, el punto de datos Promedio de uso de CPU representa la utilización de recursos de los 15 días a las 12:00 horas. Esta información se combina como un promedio. Si la utilización de la CPU era del 82% a las 12 p.m. del 1 de mayo, del 88% a las 12 p.m. del 2 de mayo y del 75% en todos los demás días, el promedio mostrado para las 12 p.m. es del 76.3%.

> **Nota:**
>
> Equilibrio de carga de trabajo suaviza los picos y los picos para que los datos no parezcan artificialmente altos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Historial de rendimiento de optimización de grupos

El informe de rendimiento de optimización muestra los eventos de optimización en relación con el uso medio de recursos de ese grupo Estos eventos son instancias en las que optimizó un grupo de recursos. Específicamente, muestra el uso de recursos para CPU, memoria, lecturas de red y escrituras de red.

La línea de puntos representa el uso promedio en todo el grupo durante el período de días que seleccione. Una barra azul indica el día en el que optimizó el grupo.

Este informe puede ayudarlo a determinar si el equilibrio de carga de trabajo funciona correctamente en su entorno. Puede usar este informe para ver qué llevó a los eventos de optimización (es decir, el uso de recursos antes de que Equilibrio de carga de trabajo recomendara la optimización).

Este informe muestra el uso promedio de recursos para el día. No muestra la utilización máxima, como cuando el sistema está estresado. También puede usar este informe para ver el rendimiento de un grupo de recursos cuando el equilibrio de carga de trabajo no hace recomendaciones de optimización.

En general, el uso de recursos disminuye o se mantiene estable después de un evento de optimización. Si no ve un uso mejorado de los recursos después de la optimización, considere reajustar los valores de umbral. Además, tenga en cuenta si el grupo de recursos tiene demasiadas máquinas virtuales y si agregó o quitó nuevas máquinas virtuales durante el período que especificó.

Seguimiento de auditoría de grupos

Este informe muestra el contenido del registro de auditoría de XenServer. El registro de auditoría es una función de XenServer diseñada para registrar los intentos de realizar acciones no autorizadas y seleccionar acciones autorizadas. Estas acciones incluyen:

- Importación y exportación
- Backups de hosts y agrupaciones
- Acceso a la consola de invitado y host.

El informe proporciona información más significativa cuando se proporcionan a los administradores de XenServer sus propias cuentas de usuario con funciones distintas que se les asignan mediante la función RBAC.

> **Importante:**
>
> Para ejecutar el informe de registro de auditoría, debe habilitar la función Registro de auditoría. De forma predeterminada, el registro de auditoría siempre está habilitado en el dispositivo virtual del equilibrio de carga de trabajo.

La función mejorada de seguimiento de auditoría del grupo le permite especificar la granularidad del informe del registro de auditoría. También puede buscar y filtrar los registros de seguimiento

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de auditoría por usuarios y objetos específicos y por tiempo. La granularidad de la pista de auditoría del grupo está establecida en Mínima de forma predeterminada. Esta opción captura una cantidad limitada de datos para usuarios y tipos de objetos específicos. Puede modificar la configuración en cualquier momento en función del nivel de detalle que necesite en su informe. Por ejemplo, establezca la granularidad en Media para obtener un informe fácil de usar del registro de auditoría. Si necesita un informe detallado, establezca la opción en Máximo.

El informe de seguimiento de auditoría de grupos contiene la siguiente información:

- Hora . La hora en que XenServer registró la acción del usuario.
- Nombre de usuario. El nombre de la persona que creó la sesión en la que se realizó la acción. En ocasiones, este valor puede ser el seudónimo
- Objeto de evento. El objeto que fue el sujeto de la acción (por ejemplo, una VM).
- Acción del evento. La acción que se ha producido. Para obtener las definiciones de estas acciones, consulte Nombres de eventos del registro de auditoría.
- Acceso. Indica si el usuario tenía permiso para realizar la acción.
- Nombre del objeto. El nombre del objeto (por ejemplo, el nombre de la máquina virtual).
- UUID de objeto. El UUID del objeto (por ejemplo, el UUID de la VM).
- Tuvo éxito. Esta información proporciona el estado de la acción (es decir, si tuvo éxito).

Nombres de eventos del registro de auditoría El informe del registro de auditoría registra los eventos, los objetos de eventos y las acciones de XenServer, incluidas la importación y exportación, las copias de seguridad de hosts y grupos y el acceso a las consolas de invitados y hosts. En la siguiente tabla se definen algunos de los eventos típicos que aparecen con frecuencia en el informe XenServer Audit Log y Pool Audit Trail. La tabla también especifica la granularidad de estos eventos.

En el informe Pista de auditoría de grupo, los eventos enumerados en la columna `Event Action` se aplican a un grupo, máquina virtual o host. Para determinar a qué se aplican los eventos, consulte las columnas `Event Object` y `Object Name` en el informe. Para obtener más definiciones de eventos, consulte la sección de eventos de la API de administración de XenServer.

Granularidad del seguimiento de auditoría de grupos	Acción del evento	Acción del usuario
Mínimo	`pool.join`	Se le indicó al anfitrión que se uniera a un grupo nuevo
Mínimo	`pool.join_force`	Se ordenó (obligó) al anfitrión a unirse a un grupo

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Granularidad del seguimiento de auditoría de grupos	Acción del evento	Acción del usuario
Medio	SR.destroy	Destruyó el repositorio de almacenamiento
Medio	SR.create	Se creó un repositorio de almacenamiento
Medio	VDI.snapshot	Se tomó una instantánea de solo lectura de la VDI y se devolvió una referencia a la instantánea
Medio	VDI.clone	Tomó una copia exacta de la VDI y devolvió una referencia al disco nuevo
Medio	VIF.plug	Conectó en caliente la VIF especificada y la conectó dinámicamente a la VM en ejecución
Medio	VIF.unplug	Desenchufó en caliente el VIF especificado y lo desconectó dinámicamente de la VM en ejecución
Máximo	auth.get_subject_identifier	Se consultó al servicio de directorio externo para obtener el identificador de sujeto como una cadena a partir del nombre de sujeto legible por humanos
Máximo	task.cancel	Se ha solicitado que se cancele una tarea
Máximo	VBD.insert	Se insertaron nuevos medios en el dispositivo
Máximo	VIF.get_by_uuid	Se obtuvo una referencia a la instancia de VIF con el UUID especificado
Máximo	VDI.get_sharable	Se ha obtenido el campo compartible de la VDI dada
Máximo	SR.get_all	Devuelve una lista de todos los SR conocidos por el sistema

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Granularidad del seguimiento de auditoría de grupos	Acción del evento	Acción del usuario
Máximo	`pool.create_new_blob`	Se creó un marcador de posición para un dato binario con nombre que está asociado con este grupo
Máximo	`host.send_debug_keys`	Se inyectó la cadena dada como claves de depuración en Xen
Máximo	`VM.get_boot_record`	Se devolvió un registro que describe el estado dinámico de la VM, se inicializó cuando se inicia la VM y se actualiza para reflejar los cambios de configuración en tiempo de ejecución, por ejemplo, conexión en caliente de la CPU

Estado del grupo

El informe Estado del grupo muestra el porcentaje de tiempo que un grupo de recursos y sus hosts han pasado en cuatro rangos de umbral diferentes: Crítico, Alto, Medio y Bajo. Puede utilizar el informe de estado del grupo para evaluar la eficacia de sus umbrales de rendimiento.

Algunos puntos sobre la interpretación de este informe:

- La utilización de recursos en el umbral medio (azul) es la utilización óptima de recursos independientemente de la estrategia de colocación seleccionada. Del mismo modo, la sección azul del gráfico circular indica la cantidad de tiempo que el host usó los recursos de manera óptima.
- La utilización de recursos en el porcentaje de umbral bajo promedio (verde) no es necesariamente positiva. El hecho de que la baja utilización de recursos sea positiva depende de su estrategia de colocación. Si su estrategia de ubicación es Densidad máxima y el uso de recursos es verde, es posible que el equilibrio de carga de trabajo no se ajuste a la cantidad máxima de máquinas virtuales en ese host o grupo. Si es así, ajuste los valores de umbral de rendimiento hasta que la mayor parte de la utilización de los recursos caiga en el intervalo de umbral medio (azul).
- La utilización de recursos en el porcentaje de umbral crítico promedio (rojo) indica la cantidad de tiempo en que la utilización promedio de recursos alcanzó o superó el valor del umbral crítico.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si hace doble clic en un gráfico circular para el uso de recursos de un host, XenCenter muestra el informe Historial de estado del host para ese recurso en ese host. Al hacer clic en **Volver al informe principal** en la barra de herramientas, volverá al informe de historial de estado del grupo.

Si observa que la mayoría de los resultados de su informe no están en el Umbral medio promedio, ajuste el umbral crítico para este grupo. Si bien el equilibrio de carga de trabajo proporciona una configuración de umbral predeterminada, estos valores predeterminados no son efectivos en todos los entornos. Si no tiene los umbrales ajustados al nivel correcto para su entorno, es posible que las recomendaciones de ubicación y optimización del equilibrio de carga de trabajo no sean apropiadas. Para obtener más información, consulte Cambiar los umbrales críticos.

Historial de estado del grupo

Este informe proporciona un gráfico lineal de la utilización de recursos en todos los hosts físicos de un grupo a lo largo del tiempo. Le permite ver la tendencia de la utilización de recursos, si tiende a aumentar en relación con sus umbrales (Crítico, Alto, Medio y Bajo). Puede evaluar la efectividad de sus umbrales de rendimiento mediante la supervisión de las tendencias de los puntos de datos en este informe.

Equilibrio de carga de trabajo extrapola los rangos de umbrales a partir de los valores que estableció para los umbrales críticos cuando conectó el grupo al equilibrio de carga de trabajo. Aunque es similar al informe de estado de la agrupación, el informe Historial de estado de la agrupación muestra la utilización media de un recurso en una fecha específica. En lugar de la cantidad de tiempo total que el recurso pasó en un umbral.

A excepción del gráfico Memoria libre promedio, los puntos de datos nunca promedian por encima de la línea del umbral crítico (rojo). Para el gráfico Memoria libre promedio, los puntos de datos nunca promedian *por debajo* de la línea del umbral crítico (que se encuentra en la parte inferior del gráfico). Como este gráfico muestra memoria *libre*, el umbral Crítico es un valor bajo, a diferencia de los demás recursos.

Algunos puntos sobre la interpretación de este informe:

- Cuando la línea Uso promedio del gráfico se acerca a la línea Umbral medio promedio (azul), indica que la utilización de recursos del grupo es óptima. Esta indicación es independiente de la estrategia de colocación configurada.
- La utilización de recursos que se aproxima al umbral mínimo promedio (verde) no es necesariamente positiva. El hecho de que la baja utilización de recursos sea positiva depende de su estrategia de colocación. En el caso de que:
  - Su estrategia de colocación es la densidad máxima
  - La mayoría de los días, la línea de uso promedio está en la línea verde o por debajo de ella, es posible que el equilibrio de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

carga de trabajo no coloque las máquinas virtuales con la mayor densidad posible en ese grupo Si es así, ajuste los valores de umbral crítico del grupo hasta que la mayor parte de su utilización de recursos caiga en el rango de umbral medio (azul).

- Cuando la línea Uso promedio se cruza con el Umbral crítico promedio (rojo), indica cuándo la utilización promedio de recursos alcanzó o superó el valor del umbral crítico para ese recurso.

Si los puntos de datos de sus gráficos no están en el intervalo Umbral medio, pero el rendimiento es satisfactorio, puede ajustar el umbral crítico para este grupo. Para obtener más información, consulte Cambiar los umbrales críticos.

Historial de optimización de grupos

El informe Historial de optimización de grupos proporciona visibilidad cronológica de la actividad de optimización de equilibrio de carga de trabajo

La actividad de optimización se resume gráficamente y en una tabla. Al profundizar en un campo de fecha dentro de la tabla, se muestra información detallada de cada optimización de grupo realizada para ese día.

Este informe le permite ver la siguiente información:

- Nombre de VM: el nombre de la VM que optimizó Workload Balancing.
- Motivo: el motivo de la optimización.
- Método: indica si la optimización se ha realizado correctamente.
- Desde el host: el host físico en el que se alojó originalmente la máquina virtual.
- Al host: el host físico al que se migró la máquina virtual.
- Hora: el momento en que se produjo la optimización.

> **Sugerencia:**
>
> También puede generar un informe Historial de optimización de grupos desde la ficha WLB haciendo clic en el enlace Ver historial.

Historial de movimiento de máquinas virtuales

Este gráfico de líneas muestra la cantidad de veces que las máquinas virtuales migraron a un grupo de recursos durante un período. Indica si una migración fue el resultado de una recomendación de optimización y a qué host se trasladó la VM. Este informe también indica el motivo de la optimización. Puede usar este informe para auditar el número de migraciones en un grupo.

Algunos puntos sobre la interpretación de este informe:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Los números del lado izquierdo del gráfico se corresponden con el número de migraciones posibles. Este valor se basa en el número de máquinas virtuales que hay en un grupo de recursos.
- Puede ver los detalles de las migraciones en una fecha específica expandiendo el signo + en la sección Fecha del informe.

Historial de rendimiento de máquinas virtuales

Este informe muestra los datos de rendimiento de cada máquina virtual en un host específico durante un período de tiempo que especifique. Equilibrio de carga de trabajo basa los datos de rendimiento en la cantidad de recursos virtuales asignados a la VM. Por ejemplo, si el uso promedio de CPU para su VM es del 67%, su VM usa, en promedio, el 67% de su vCPU durante el período especificado.

La vista inicial del informe muestra un valor promedio para la utilización de recursos durante el período que especificó.

Al expandir el signo +, se muestran gráficos de líneas para recursos individuales. Puede utilizar estos gráficos para ver las tendencias en la utilización de los recursos a lo largo del tiempo.

Este informe muestra datos de uso de CPU, memoria libre, lecturas/escrituras de red y lecturas/escrituras de disco.

Configurar el comportamiento del equilibrio de carga

April 11, 2024

Después de conectarse al dispositivo virtual Equilibrio de carga de trabajo, puede modificar la configuración que el equilibrio de carga de trabajo utiliza para calcular la ubicación y las recomendaciones. La configuración de equilibrio de carga de trabajo se aplica de forma colectiva a todas las máquinas virtuales y hosts del grupo.

La configuración de ubicación y optimización que puede modificar incluye lo siguiente:

- Cambiar la estrategia de colocación
- Configuración de optimizaciones automáticas y administración de energía
- Edición de umbrales de rendimiento y ponderaciones de métricas
- Excluidos los anfitriones.

Siempre que los umbrales de red y disco se alineen con el hardware del entorno, considere utilizar la mayoría de los valores predeterminados en el equilibrio de carga de trabajo inicialmente. Después de habilitar Equilibrio de carga de trabajo durante un tiempo, se recomienda evaluar los umbrales de rendimiento y determinar si se deben modificar. Por ejemplo, considere los siguientes casos:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Obtener recomendaciones cuando aún no se requieren. Si es así, intente ajustar los umbrales hasta que Equilibrio de carga de trabajo comience a proporcionar recomendaciones adecuadas.
- No recibir recomendaciones cuando espera recibirlas. Por ejemplo, si su red no tiene suficiente ancho de banda y no recibe recomendaciones, puede que tenga que modificar la configuración. Si es así, intente reducir los umbrales críticos de la red hasta que el equilibrio de carga de trabajo comience a proporcionar recomendaciones

Antes de modificar los umbrales, puede generar un informe del estado de la agrupación y el informe del historial de salud de la agrupación para cada anfitrión físico de la agrupación. Para obtener más información, consulte Generar informes de carga de trabajo.

> **Notas:**
>
> - Workload Balancing está disponible para los clientes de XenServer Premium Edition. Para obtener más información sobre las licencias de XenServer, consulte Licencias. Para actualizar o comprar una licencia de XenServer, visite el sitio web de XenServer.
> - Workload Balancing 8.3.0 es compatible con XenServer 8 y Citrix Hypervisor 8.2 CU1.

En este artículo se supone que ya ha conectado el grupo a un dispositivo virtual de equilibrio de carga de trabajo. Para obtener información sobre la descarga, la importación, la configuración y la conexión a un dispositivo virtual de equilibrio de carga de trabajo, consulte Introducción.

Ajuste el modo de optimización

Equilibrio de carga de trabajo hace recomendaciones para reequilibrar u optimizar la carga de trabajo de la VM en su entorno en función de una estrategia para la ubicación que seleccione. La estrategia de colocación se conoce como modo de optimización.

Puede elegir entre los siguientes modos de optimización:

- **Maximizar el rendimiento** (predeterminado)

  El equilibrio de carga de trabajo intenta distribuir la carga de trabajo de manera uniforme entre todos los hosts físicos de un grupo de recursos. El objetivo es minimizar la presión de la CPU, la memoria y la red para todos los hosts. Si su estrategia de ubicación es maximizar el rendimiento, Workload Balancing recomienda la optimización cuando un host alcanza el umbral alto.

- **Maximizar densidad**

  El equilibrio de carga de trabajo intenta minimizar la cantidad de hosts físicos que deben estar en línea mediante la consolidación de las máquinas virtuales activas.

  Cuando selecciona Maximizar densidad como estrategia de ubicación, puede especificar parámetros similares a los de Maximizar rendimiento. Sin embargo, Workload Balancing utiliza

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

estos parámetros para determinar cómo puede empaquetar las máquinas virtuales en un host. Si Maximizar densidad es su estrategia de ubicación, Equilibrio de carga de trabajo recomienda optimizaciones de consolidación cuando una VM alcanza el umbral bajo.

Equilibrio de carga de trabajo también le permite aplicar estos modos de optimización siempre, *fijos* o cambiar entre modos durante períodos de tiempo específicos, *programados*:

Modos de optimización fijos

Los modos de optimización fijos establecen que el equilibrio de carga de trabajo siempre tenga un comportamiento de optimización específico. Este comportamiento puede ser para intentar crear el mejor rendimiento o para crear la densidad más alta.

Para establecer un modo de optimización fijo, siga los pasos siguientes:

1. En XenCenter, seleccione su grupo.
2. En el panel **Propiedades** del grupo, haga clic en la ficha **WLB**.
3. En la ficha **WLB**, haga clic en **Configuración**.
4. En el panel izquierdo, haga clic en **Modo de optimización**.
5. En la sección **Fijo** de la página **Modo de optimización**, seleccione uno de estos modos de optimización:

    - Maximizar el rendimiento (predeterminado). Intenta distribuir la carga de trabajo de manera uniforme entre todos los hosts físicos de un grupo de recursos. El objetivo es minimizar la presión de la CPU, la memoria y la red para todos los hosts.
    - Maximizar la densidad Intenta colocar tantas máquinas virtuales como sea posible en un host físico. El objetivo es minimizar la cantidad de hosts físicos que deben estar en línea.

Modos de optimización programada

Los modos de optimización programada le permiten programar el equilibrio de carga de trabajo para aplicar diferentes modos de optimización en función de la hora del día. Por ejemplo, es posible que quiera configurar el equilibrio de carga de trabajo para optimizar el rendimiento durante el día cuando tenga usuarios conectados. Para ahorrar energía, puede especificar que Equilibrio de carga de trabajo optimice la densidad máxima por la noche.

Cuando configura los modos de optimización programados, el equilibrio de carga de trabajo cambia automáticamente al modo de optimización al principio del período de tiempo que especificó. Puede configurar todos los días, días laborables, fines de semana o días individuales. Para la hora, seleccione una hora del día.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para establecer un horario para sus modos de optimización, complete los siguientes pasos:

1. En XenCenter, seleccione su grupo.
2. En el panel **Propiedades** del grupo, haga clic en la ficha **WLB**.
3. En la ficha **WLB**, haga clic en **Configuración**.
4. En el panel izquierdo, haga clic en **Modo de optimización**.
5. En el panel **Modo de optimización**, seleccione **Programado**. La sección **Programado** pasa a estar disponible.
6. Haga clic en **Agregar nuevo**.
7. En el cuadro **Cambiar a**, seleccione uno de los siguientes modos:
   - Maximice el rendimiento Intenta distribuir la carga de trabajo de manera uniforme entre todos los hosts físicos de un grupo de recursos. El objetivo es minimizar la presión de la CPU, la memoria y la red para todos los hosts.
   - Maximizar la densidad Intenta colocar tantas máquinas virtuales como sea posible en un host físico. El objetivo es minimizar la cantidad de hosts físicos que deben estar en línea.
8. Seleccione el día de la semana y la hora en la que quiere que el equilibrio de carga de trabajo comience a funcionar en este modo.
9. Repita los pasos anteriores para crear más tareas en modo programado hasta que tenga el número que necesita. Si solo planifica una tarea, Equilibrio de carga de trabajo cambia a ese modo según lo programado, pero nunca cambia de nuevo.
10. Haga clic en **Aceptar**.

Para cambiar la configuración del horario, complete los siguientes pasos.

1. En XenCenter, seleccione su grupo.
2. En el panel **Propiedades** del grupo, haga clic en la ficha **WLB**.
3. En la ficha **WLB**, haga clic en **Configuración**.
4. En el panel izquierdo, haga clic en **Modo de optimización**.
5. Seleccione la tarea que quiera eliminar o inhabilitar de la lista de **cambios de modo programados**.
6. Lleve a cabo una de las siguientes acciones:
   - **Eliminar la tarea permanentemente**: haga clic en el botón **Eliminar**.
   - **Detener la ejecución temporal de la tarea**: haga clic con el botón secundario en la tarea y **,**a

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sugerencias:

```
- También puede inhabilitar o habilitar las tareas seleccionando la tarea, haciendo clic en **Modificar** y marcando la casilla **Habilitar tarea** en el cuadro de diálogo **Programador del modo de optimización**.
```

- Para volver a habilitar una tarea, haga clic con el botón secundario en la tarea en la lista **Cambios de modo programados** y haga clic en **Habilitar**.

- **Modificar la tarea**: Haga doble clic en la tarea que quiera modificar. En el cuadro **Cambiar a**, seleccione un modo diferente o realice los cambios que quiera.

Nota:

Al hacer clic en Cancelar, antes de hacer clic en Aceptar, se deshacen los cambios realizados en la ficha Optimización, incluida la eliminación de una tarea.

Optimice y administre la energía automáticamente

Puede configurar el equilibrio de carga de trabajo para aplicar las recomendaciones automáticamente y activar o desactivar los hosts automáticamente. Para apagar los hosts automáticamente (por ejemplo, durante los períodos de bajo uso), debe configurar el equilibrio de carga de trabajo para aplicar las recomendaciones automáticamente y habilitar la administración de energía. Tanto la administración de energía como la automatización se describen en las secciones siguientes.

Aplicar recomendaciones automáticamente

Equilibrio de carga de trabajo le permite configurar para que aplique recomendaciones en su nombre y lleve a cabo las acciones de optimización que recomienda automáticamente. Puede usar esta función, que se conoce como aceptación automática de la optimización, para aplicar cualquier recomendación de forma automática, incluidas las destinadas a mejorar el rendimiento o apagar los hosts. Sin embargo, para apagar los hosts a medida que disminuye el uso de las máquinas virtuales, debe configurar la automatización, la administración de energía y el modo de máxima densidad.

De forma predeterminada, Equilibrio de carga de trabajo no aplica recomendaciones automáticamente. Si quiere que Equilibrio de carga de trabajo aplique recomendaciones automáticamente, habilite la automatización. Si no lo hace, debe aplicar las recomendaciones manualmente haciendo clic en **Aplicar recomendaciones**.

El equilibrio de carga de trabajo no aplica automáticamente las recomendaciones a los hosts o las máquinas virtuales cuando las recomendaciones entran en conflicto con la configuración de alta

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

disponibilidad. Si un grupo se vuelve demasiado comprometido al aplicar las recomendaciones de optimización del equilibrio de carga de trabajo, XenCenter le pregunta si quiere seguir aplicando la recomendación. Cuando la automatización está habilitada, Workload Balancing no aplica ninguna recomendación de administración de energía que supere la cantidad de fallas de host que se toleran en el plan de alta disponibilidad.

Cuando Equilibrio de carga de trabajo se ejecuta con la función de automatización habilitada, este comportamiento a veces se denomina ejecución en modo automatizado.

Es posible ajustar la forma en que Equilibrio de carga de trabajo aplica las recomendaciones en modo automatizado. Para obtener información, consulte Establecer recomendaciones automatizadas conservadoras o agresivas.

Para aplicar recomendaciones de optimización automáticamente

1. En XenCenter, seleccione su grupo.
2. En el panel **Propiedades** del grupo, haga clic en la ficha **WLB**.
3. En la ficha **WLB**, haga clic en **Configuración**.
4. En el panel izquierdo, haga clic en **Automatización**.
5. Seleccione una o más de las siguientes casillas de verificación:
   - **Aplica automáticamente las recomendaciones de optimización**. Al seleccionar esta opción, no necesita aceptar las recomendaciones de optimización de forma manual. Workload Balancing acepta automáticamente las recomendaciones de optimización y ubicación que hace.
   - **Aplica automáticamente las recomendaciones de administración de energía**. El comportamiento de esta opción varía en función del modo de optimización del grupo:
     - Modo de máximo rendimiento: cuando se habilita la **aplicación automática de las recomendaciones de administración de energía**, el equilibrio de carga de trabajo enciende automáticamente los hosts cuando, al hacerlo, se mejora el rendimiento del host.
     - Modo de densidad máxima: cuando la **aplicación automática de las recomendaciones de administración de energía** está habilitada, el equilibrio de carga de trabajo apaga automáticamente los hosts cuando la utilización de los recursos cae por debajo del umbral bajo. Es decir, el equilibrio de carga de trabajo apaga los hosts automáticamente durante los períodos de bajo uso.
6. (Opcional). Ajuste las recomendaciones de optimización haciendo clic en **Avanzado** en el panel izquierdo del cuadro de diálogo **Configuración** y realizando una o más de las siguientes acciones:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Especificar el número de veces que el equilibrio de carga de trabajo debe hacer una recomendación de optimización antes de que la recomendación se aplique automáticamente. El valor predeterminado es tres veces, lo que significa que la recomendación se aplica la tercera vez que se hace.
- Seleccionar el nivel más bajo de recomendación de optimización que quiere que Equilibrio de Carga de Trabajo se aplique automáticamente. El valor predeterminado es "Alta".
- Cambiar la agresividad con la que el equilibrio de carga de trabajo aplica sus recomendaciones de optimización.

  También puede especificar el número de minutos que debe esperar el equilibrio de carga de trabajo antes de aplicar una recomendación de optimización a una máquina virtual que se mudó recientemente.

  Todas estas configuraciones se explican con más profundidad en Establecer recomendaciones automatizadas conservadoras o agresivas.

7. (opcional) Si quiere configurar la administración de energía, haga clic en **Automatización/Administración de energía**

   a) En la sección **Administración de energía**, seleccione los hosts que quiere que Workload Balancing recomiende encender y apagar.

   > **Nota:**
   >
   > Al seleccionar hosts para las recomendaciones de administración de energía sin seleccionar **Aplicar automáticamente las recomendaciones de administración de energía**, Workload Balancing sugiere recomendaciones de administración de energía, pero no las aplique automáticamente.

   Si ninguno de los hosts del grupo de recursos admite la administración remota de energía, Workload Balancing muestra el mensaje "No hay hosts compatibles con la administración de energía". "

   b) Haga clic en **Aceptar**.

8. Para terminar de configurar la automatización, haga clic en **Aceptar**.

Habilitar la administración de energía de equilibrio

El término administración de energía se refiere a la capacidad de encender o apagar la alimentación de los hosts físicos. En un contexto de equilibrio de carga de trabajo, este término significa encender o apagar los hosts de un grupo en función de la carga de trabajo total del grupo.

La configuración de la administración de energía de Workload Balancing en un host requiere que

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- El hardware del host tiene capacidades de encendido/apagado remoto.
- La función de encendido del host está configurada para el host. Para configurar la función de encendido del host para el host, consulte Configurar la función de encendido del host.
- El host se seleccionó explícitamente como host para participar en la administración de energía de Workload Balancing.

Además, si quiere que el equilibrio de carga de trabajo apague los hosts automáticamente, configure el equilibrio de carga de trabajo para que realice las siguientes acciones:

- Aplicar recomendaciones automáticamente
- Aplicar recomendaciones de administración de energía automáticamente

Cuando un host está configurado para participar en la administración de energía, Workload Balancing hace recomendaciones de encendido y apagado según sea necesario.

Si ejecutas en modo Densidad máxima:

- Cuando Workload Balancing detecta recursos no utilizados en un grupo, recomienda apagar los hosts hasta eliminar todo el exceso de capacidad.
- Si no hay suficiente capacidad de host en el grupo para cerrar los hosts, Workload Balancing recomienda dejar los hosts encendidos hasta que la carga de trabajo del grupo disminuya lo suficiente.
- Al configurar el equilibrio de carga de trabajo para apagar automáticamente los hosts adicionales, aplica estas recomendaciones automáticamente y, por lo tanto, se comporta de la misma manera.

Si se ejecuta en modo de rendimiento máximo:

- Si configura el equilibrio de carga de trabajo para que encienda los hosts automáticamente, el equilibrio de carga de trabajo enciende los hosts cuando la utilización de los recursos en un host supera el umbral alto.
- Workload Balancing nunca apaga los hosts después de encenderlos.

Si activa la opción de aplicar las recomendaciones de administración de energía automáticamente, lo hace a nivel de grupo. Sin embargo, puede especificar qué hosts del grupo quiere que participen en la administración de energía.

Configurar la función Host Power On Para configurar la función Host Power On para su host, siga estos pasos:

1. **En XenCenter, seleccione su host y haga clic en Propiedades.**
2. En el panel izquierdo, haga clic **en Encender**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Para el **modo de encendido**, seleccione la controladora de **acceso remoto de Dell (DRAC)**.
4. Para las **opciones de configuración**, introduzca la dirección IP DRAC del servidor. Esta es la dirección IP del puerto de administración de BMC. Para obtener más información, consulte la Guía práctica de la tarjeta DRAC [PDF].
5. Una vez configurada la controladora de acceso remoto (DRAC) de Dell, seleccione su grupo.
6. En el panel **Propiedades** del grupo, haga clic en la ficha **WLB**.
7. En la ficha **WLB**, haga clic en **Configuración**.
8. En el panel izquierdo, haga clic en **Automatización**.
9. Para **Automatización**, active las siguientes casillas de verificación:
   - **Aplica automáticamente las recomendaciones de optimización**. Al seleccionar esta opción, no necesita aceptar las recomendaciones de optimización de forma manual. Workload Balancing acepta automáticamente las recomendaciones de optimización y ubicación que hace.
   - **Aplica automáticamente las recomendaciones de administración de energía**. El comportamiento de esta opción varía en función del modo de optimización del grupo:
     - Modo de máximo rendimiento: cuando se habilita la **aplicación automática de las recomendaciones de administración de energía**, el equilibrio de carga de trabajo enciende automáticamente los hosts cuando, al hacerlo, se mejora el rendimiento del host.
     - Modo de densidad máxima: cuando la **aplicación automática de las recomendaciones de administración de energía** está habilitada, el equilibrio de carga de trabajo apaga automáticamente los hosts cuando la utilización de los recursos cae por debajo del umbral bajo. Es decir, el equilibrio de carga de trabajo apaga los hosts automáticamente durante los períodos de bajo uso.
10. Para **Administración de energía**, seleccione el nombre del **servidor host** que está configurando actualmente.

Comprender el comportamiento de la administración

Antes de que Workload Balancing recomiende encender o apagar los hosts, selecciona los hosts a los que transferir las máquinas virtuales. Lo hace en el siguiente orden:

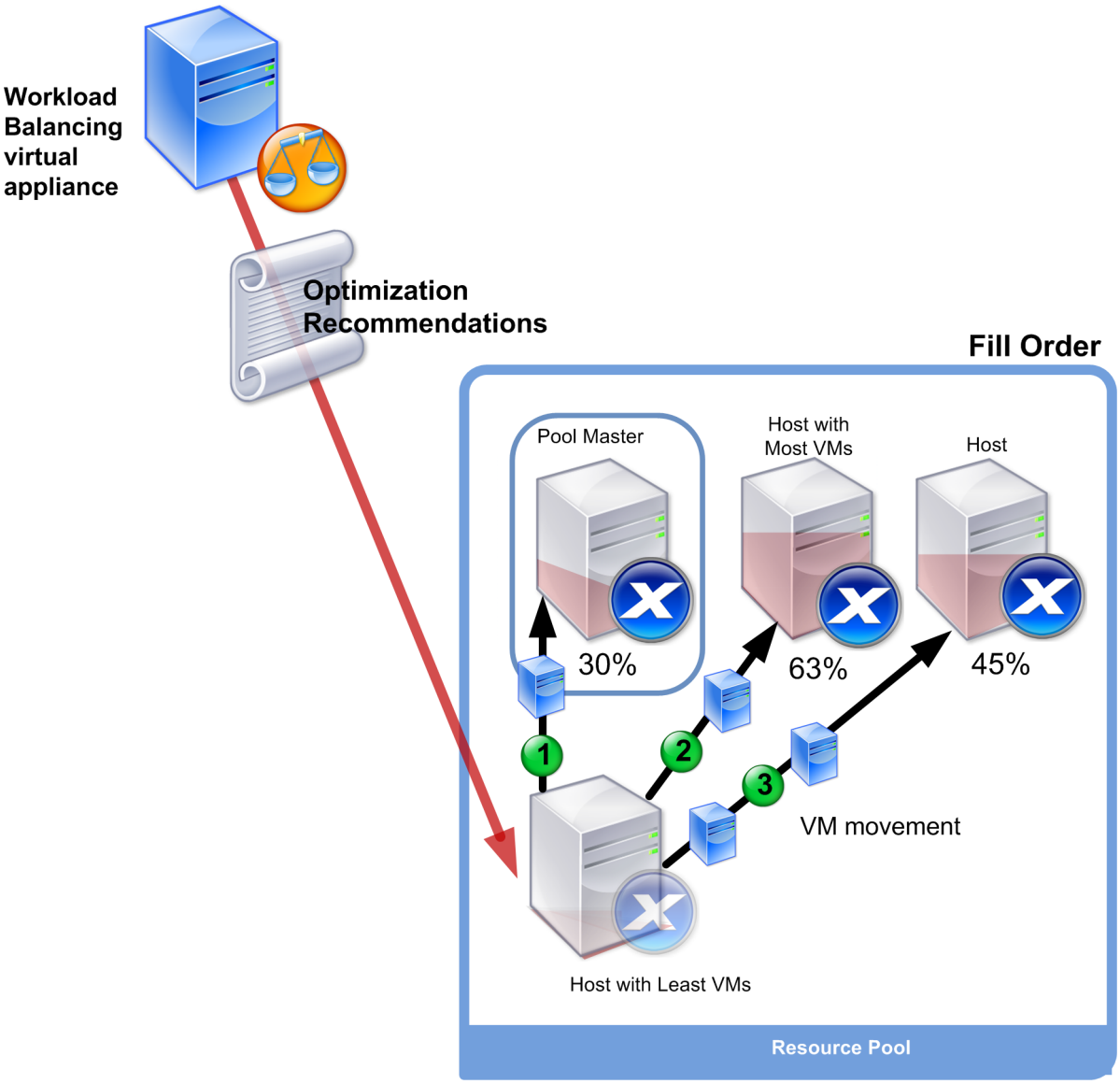
1. Llenar el coordinador de la agrupación, ya que es el host el que no se puede apagar.
2. Llenar el host con la mayor cantidad de máquinas virtuales.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Rellenar los hosts subsiguientes en función de los hosts que tienen más máquinas virtuales en ejecución.

Cuando el equilibrio de carga de trabajo ocupa al coordinador del grupo, lo hace suponiendo umbrales artificialmente bajos para el coordinador. El equilibrio de carga de trabajo utiliza estos umbrales bajos como un búfer para evitar que el coordinador del grupo se sobrecargue.

El equilibrio de carga de trabajo llena los hosts en este orden para fomentar la densidad.



Cuando Workload Balancing detecta un problema de rendimiento mientras el grupo está en modo de densidad máxima, recomienda migrar las cargas de trabajo entre los hosts encendidos. Si el equilibrio de carga de trabajo no puede resolver el problema con este método, intenta encender un host. El equilibrio de carga de trabajo determina qué hosts se deben encender aplicando los mismos criterios que si el modo de optimización estuviera configurado en Rendimiento máximo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cuando Workload Balancing se ejecuta en el modo de rendimiento máximo, Workload Balancing recomienda encender los hosts hasta que la utilización de los recursos de todos los miembros del grupo caiga por debajo del umbral alto.

Al migrar las máquinas virtuales, si Workload Balancing determina que el aumento de la capacidad beneficia al rendimiento general del grupo, enciende los hosts automáticamente o recomienda hacerlo.

> **Importante:**
>
> Equilibrio de carga de trabajo solo recomienda encender un host que esté apagado.

Diseñe entornos para administración de energía y consolidación de VM

Cuando planifique una implementación de XenServer y quiera configurar la consolidación automática de máquinas virtuales y la administración de energía, tenga en cuenta el diseño de la carga de trabajo. Por ejemplo, es posible que quiera:

- Coloque diferentes tipos de cargas de trabajo en grupos separados.

  Si tiene un entorno con distintos tipos de cargas de trabajo, considere si quiere ubicar las máquinas virtuales que alojan estas cargas de trabajo en diferentes grupos. También considere la posibilidad de dividir las máquinas virtuales que alojan tipos de aplicaciones que funcionan mejor con ciertos tipos de hardware en grupos diferentes.

  Dado que la administración de energía y la consolidación de VM se administran a nivel de grupo, diseñe los grupos de modo que contengan cargas de trabajo que quiere consolidar al mismo ritmo. Asegúrese de tener en cuenta consideraciones como las que se describen en Configurar opciones avanzadas.

- Excluya los hosts del equilibrio de carga de trabajo.

  Es posible que algunos hosts deban estar siempre activados. Para obtener más información, consulta Excluir a los anfitriones de las recomendaciones.

Comprender cuándo el equilibrio de carga de trabajo

Workload Balancing evalúa continuamente las métricas de recursos de los hosts físicos y las máquinas virtuales en los grupos que administra en función de los umbrales. Los umbrales son valores preestablecidos que funcionan como límites que un host debe superar antes de que Workload Balancing pueda hacer una recomendación de optimización. El proceso de equilibrio de carga de trabajo es el siguiente:

1. El equilibrio de carga de trabajo detecta que se infringió el umbral de un recurso.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Equilibrio de carga de trabajo evalúa si hace una recomendación de optimización.
3. El equilibrio de carga de trabajo determina qué hosts recomienda que funcionen como hosts de destino y en qué orden realizar las optimizaciones. Un host de destino es el host en el que Workload Balancing recomienda reubicar una o más máquinas virtuales.
4. Workload Balancing hace una recomendación de optimización.

Al evaluar los hosts del grupo para hacer una recomendación de optimización, Workload Balancing utiliza los siguientes umbrales y ponderaciones:

- Los**umbrales** son los valores de límite con los que Equilibrio de carga de trabajo compara las métricas de recursos de su grupo. Los umbrales se utilizan para determinar si se debe hacer una recomendación y qué hosts son candidatos adecuados para alojar máquinas virtuales reubicadas.
- Las**ponderaciones** son una forma de clasificar los recursos según cuánto quiere que sean considerados, se utilizan para determinar el orden de procesamiento. Después de que Equilibrio de carga de trabajo decide hacer una recomendación, utiliza sus especificaciones de qué recursos son importantes para determinar lo siguiente:
  - Qué rendimiento de los anfitriones abordar primero
  - Qué máquinas virtuales se recomienda migrar primero

Para cada recurso que supervisa el equilibrio de carga de trabajo, tiene cuatro niveles de umbrales: Crítico, Alto, Medio y Bajo. El equilibrio de carga de trabajo evalúa si se debe hacer una recomendación cuando una métrica de recursos de un host:

- Supera el umbral Alto cuando el grupo se ejecuta en modo de rendimiento máximo (mejora el rendimiento)
- Cae por debajo del umbral bajo cuando el grupo se ejecuta en modo de densidad máxima (consolide las máquinas virtuales en los hosts)
- Supera el umbral crítico cuando la agrupación se ejecuta en modo de densidad máxima (mejora el rendimiento)

Si el umbral alto para un grupo que se ejecuta en el modo de rendimiento máximo es del 80%, cuando el uso de la CPU en un host alcanza el 80,1%, Workload Balancing evalúa si se debe emitir una recomendación.

Cuando un recurso infringe su umbral, el equilibrio de carga de trabajo evalúa la métrica del recurso en función del rendimiento histórico para evitar hacer una recomendación de optimización basada en un pico temporal. Para ello, Equilibrio de carga de trabajo crea una métrica de utilización promediada históricamente mediante la evaluación de los datos para la utilización de recursos capturados en los siguientes momentos:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datos capturados	Peso
Inmediatamente, en el momento en que se superó el umbral. Es decir, datos en tiempo real.	70%
30 minutos antes de que se superara el umbral	25%
24 horas antes de que se superara el umbral	5%

Si la utilización de la CPU en el host supera el umbral a las 12:02 p.m., Workload Balancing comprueba la utilización a las 11:32 a.m. de ese día y a las 12:02 p.m., del día anterior. Por ejemplo, si la utilización de la CPU se encuentra en los siguientes valores, Equilibrio de carga de trabajo no hace ninguna recomendación:

- 80,1% a las 12:02 de ese día
- 50% a las 11:32 AM de ese día
- 78% a las 12:32 del día anterior

Este comportamiento se debe a que la utilización promediada históricamente es del 72,5%, por lo que el equilibrio de carga de trabajo supone que la utilización es un pico temporal. Sin embargo, si la utilización de la CPU era del 83% a las 11:32 a. m., Equilibrio de carga de trabajo hace una recomendación, ya que la utilización promediada históricamente es 80,1%.

Proceso de optimización y consolidación

El proceso de equilibrio de carga de trabajo para determinar posibles optimizaciones varía según el modo de optimización: rendimiento máximo o densidad máxima. Sin embargo, independientemente del modo de optimización, las recomendaciones de optimización y colocación se realizan mediante un proceso de dos etapas:

1. Determine las posibles optimizaciones: qué máquinas virtuales migrar de los hosts.
2. Determine las recomendaciones de ubicación: qué hosts serían candidatos adecuados para nuevas máquinas virtuales.

> **Nota:**
>
> Workload Balancing solo recomienda migrar las máquinas virtuales que cumplan con los criterios de XenServer para la migración en vivo. Uno de estos criterios es que el host de destino debe tener el almacenamiento que requiere la máquina virtual. El host de destino también debe tener recursos suficientes para admitir la adición de la máquina virtual sin superar los umbrales del modo de optimización configurado en el grupo. Por ejemplo, el umbral alto en el modo de rendimiento máximo y el umbral crítico para el modo de densidad máxima.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cuando el equilibrio de carga de trabajo se ejecuta en modo automatizado, puede ajustar la forma en que aplica las recomendaciones. Para obtener más información, consulte Establecer recomendaciones automatizadas conservadoras o agresivas.

Proceso de recomendación de optimización en el modo de rendimiento máximo Cuando se ejecuta en modo de rendimiento máximo, Equilibrio de carga de trabajo utiliza el siguiente proceso para determinar posibles optimizaciones:

1. Cada dos minutos, Workload Balancing evalúa la utilización de los recursos de cada host del grupo. Para ello, supervisa cada host y determina si la utilización de cada recurso supera su umbral alto. Para obtener más información, consulte Cambiar el umbral crítico.

   En el modo de rendimiento máximo, si la utilización de un recurso supera su umbral Alto, el equilibrio de carga de trabajo inicia el proceso para determinar si se debe hacer una recomendación de optimización. El equilibrio de carga de trabajo determina si se debe hacer una recomendación de optimización en función de si hacerlo puede aliviar las restricciones de rendimiento, como las reveladas por el umbral Alto.

   Por ejemplo, consideremos el caso en el que Workload Balancing considera que la insuficiencia de recursos de CPU afecta negativamente al rendimiento de las máquinas virtuales de un host. Si Workload Balancing puede encontrar otro host con menos uso de la CPU, se recomienda mover una o más máquinas virtuales a otro host.

2. Si la utilización de un recurso en un host supera el umbral correspondiente, Workload Balancing combina los siguientes datos para formar la utilización promediada históricamente:

   - La utilización actual del recurso
   - Datos históricos de hace 30 minutos
   - Datos históricos de hace 24 horas

   Si la utilización promediada históricamente supera el umbral de un recurso, el equilibrio de carga de trabajo determina que hace una recomendación de optimización.

3. El equilibrio de carga de trabajo utiliza ponderaciones métricas para determinar qué hosts se deben optimizar primero. El recurso al que se ha asignado más peso es el que Equilibrio de carga de trabajo intenta abordar primero. Para obtener más información, consulte Ajuste de ponderaciones de métricas.

4. El equilibrio de carga de trabajo determina qué hosts pueden admitir las máquinas virtuales que quiere migrar fuera de los hosts.

   El equilibrio de carga de trabajo realiza esta determinación calculando el efecto proyectado en la utilización de los recursos de colocar diferentes combinaciones de máquinas virtuales en los hosts. Equilibrio de carga de trabajo utiliza un método para realizar estos cálculos que en matemáticas se conoce como permutación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para ello, Workload Balancing crea una única métrica o puntuación para pronosticar el impacto de la migración de una máquina virtual al host. La puntuación indica la idoneidad de un host como hogar para más máquinas virtuales.

Para evaluar el rendimiento del host, Workload Balancing combina las siguientes métricas:

- Las métricas actuales del anfitrión
- Las métricas del anfitrión de los últimos 30 minutos
- Las métricas del anfitrión de hace 24 horas
- Las métricas de la VM.

5. Tras puntuar los hosts y las máquinas virtuales, Workload Balancing intenta crear modelos virtuales del aspecto de los hosts con diferentes combinaciones de máquinas virtuales. Workload Balancing utiliza estos modelos para determinar el mejor host para colocar la máquina virtual.

   En el modo de rendimiento máximo, el equilibrio de carga de trabajo utiliza ponderaciones métricas para determinar qué hosts se deben optimizar primero y qué máquinas virtuales de esos hosts se deben migrar primero. Equilibrio de carga de trabajo basa sus modelos en las ponderaciones métricas. Por ejemplo, si se asigna la máxima importancia al uso de la CPU, Workload Balancing ordena los hosts y las máquinas virtuales para optimizarlos según los siguientes criterios:

   a) Qué hosts se ejecutan más cerca del umbral alto de utilización de la CPU.
   b) Qué máquinas virtuales tienen la mayor utilización de CPU o se ejecutan más cerca de su umbral alto.

6. El equilibrio de carga de trabajo sigue calculando optimizaciones Considera a los hosts como candidatos a la optimización y a las máquinas virtuales como candidatas a la migración hasta que la utilización prevista de los recursos en el host que aloja la máquina virtual caiga por debajo del umbral alto. La utilización de recursos prevista es la utilización de recursos que Workload Balancing prevé que tendrá un host después de que Workload Balancing haya agregado o eliminado una máquina virtual del host.

Proceso de consolidación en modo Densidad máxima El equilibrio de carga de trabajo determina si se debe hacer una recomendación en función de si se puede migrar una máquina virtual a un host y seguir ejecutando ese host por debajo del umbral crítico.

1. Cuando la utilización de un recurso cae por debajo de su umbral bajo, Equilibrio de carga de trabajo comienza a calcular posibles casos de consolidación.
2. Cuando Workload Balancing descubre una forma de consolidar las máquinas virtuales en un host, evalúa si el host de destino es un hogar adecuado para la máquina virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Al igual que en el modo de rendimiento máximo, el equilibrio de carga de trabajo puntúa el host para determinar su idoneidad como hogar para nuevas máquinas virtuales.

   Antes de que Workload Balancing recomiende consolidar las máquinas virtuales en menos hosts, comprueba que la utilización de los recursos en esos hosts después de reubicar las máquinas virtuales en ellos esté por debajo de los umbrales críticos.

   > **Nota:**
   >
   > El equilibrio de carga de trabajo no tiene en cuenta las ponderaciones de métricas cuando hace una recomendación de consolidación. Solo tiene en cuenta las ponderaciones métricas para garantizar el rendimiento en los hosts.

4. Tras puntuar los hosts y las máquinas virtuales, Workload Balancing intenta crear modelos virtuales del aspecto de los hosts con diferentes combinaciones de máquinas virtuales. Utiliza estos modelos para determinar el mejor host para colocar la máquina virtual.
5. Workload Balancing calcula el efecto de agregar máquinas virtuales a un host hasta que prevé que agregar otra máquina virtual provoque que un recurso de host supere el umbral crítico.
6. Las recomendaciones de equilibrio de carga de trabajo siempre sugieren que primero se llene el coordinador del grupo, ya que es el host el que no se puede apagar. Sin embargo, el equilibrio de carga de trabajo aplica un búfer al coordinador del grupo para que no pueda sobreasignarse.
7. Workload Balancing sigue recomendando migrar las máquinas virtuales a los hosts hasta que todos los hosts restantes superen un umbral crítico al migrar una máquina virtual a ellos.

Cambiar los umbrales críticos

Es posible que quiera cambiar los umbrales críticos como una forma de controlar cuándo se activan las recomendaciones de optimización. En esta sección se proporciona orientación sobre:

- Cómo modificar los umbrales críticos predeterminados en los hosts del grupo
- Cómo los valores establecidos para el umbral crítico alteran los umbrales alto, medio y bajo.

El equilibrio de carga de trabajo determina si se deben producir recomendaciones en función de si la utilización histórica promedio de un recurso en un host infringe su umbral. Las recomendaciones de equilibrio de carga de trabajo se activan cuando se infringe el umbral alto en el modo de rendimiento máximo o los umbrales bajo y crítico para el modo de densidad máxima. Para obtener más información, consulte Proceso de optimización y consolidación.

Después de especificar un nuevo umbral crítico para un recurso, el equilibrio de carga de trabajo restablece los demás umbrales del recurso en relación con el nuevo umbral crítico. Para simplificar la interfaz de usuario, el umbral Crítico es el único umbral que puede cambiar a través de XenCenter.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

En la siguiente tabla se muestran los valores predeterminados para los umbrales del equilibrio de carga de trabajo:

Métrica	Grave	Alto	Medio	Bajo
Utilización de CPU	90%	76.5%	45%	22.5%
Memoria libre	51 MB	63,75 MB	510 MB	1020 MB
Lecturas de red	25 MB/seg.	21.25 MB/seg.	12.5 MB/seg.	6,25 MB/seg.
Escrituras en red	25 MB/seg.	21.25 MB/seg.	12.5 MB/seg.	6,25 MB/seg.
Lecturas de disco	25 MB/seg.	21.25 MB/seg.	12.5 MB/seg.	6,25 MB/seg.
Escrituras en disco	25 MB/seg.	21.25 MB/seg.	12.5 MB/seg.	6,25 MB/seg.

Para calcular los valores de umbral para todas las métricas, excepto la memoria, el equilibrio de carga de trabajo multiplica el nuevo valor del umbral crítico con los siguientes factores:

- **Factor de umbral alto**: 0.85
- **Factor de umbral medio**: 0.50
- **Factor de umbral bajo**: 0.25

Por ejemplo, si aumenta el umbral crítico para el uso de la CPU al 95%, el equilibrio de carga de trabajo restablece los demás umbrales de la siguiente manera:

- Alto: 80,75%
- Medio: 47,5%
- Bajo: 23,75%

Para calcular los valores de umbral para la memoria libre, Equilibrio de carga de trabajo multiplica el nuevo valor del umbral crítico por estos factores:

- **Factor de umbral alto**: 1.25
- **Factor de umbral medio**: 10.0
- **Factor de umbral bajo**: 20.0

Por ejemplo, si aumenta el umbral crítico para la memoria libre a 45 MB, el equilibrio de carga de trabajo restablece los demás umbrales de la siguiente manera:

- Alto: 56,25 MB
- Mediana: 450 MB
- Bajo: 900 MB

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para realizar este cálculo para un umbral específico, multiplique el factor del umbral por el valor que introdujo para el umbral crítico de ese recurso:

```
High, Medium, or Low Threshold = Critical Threshold * High, Medium, or
    Low Threshold Factor
```

Si bien el umbral Crítico desencadena muchas recomendaciones de optimización, otros umbrales también pueden desencadenar recomendaciones de optimización, de la siguiente manera:

- **Umbral alto**.
  - **Máximo rendimiento**. Superar el umbral alto genera recomendaciones de optimización para reubicar una máquina virtual en un host con un menor uso de recursos.
  - **Densidad máxima**. Workload Balancing no recomienda colocar una máquina virtual en el host cuando al mover esa máquina virtual al host, la utilización de los recursos del host supera un umbral alto.
- **Umbral bajo**.
  - **Máximo rendimiento**. El equilibrio de carga de trabajo no desencadena recomendaciones desde el umbral bajo.
  - **Densidad máxima**. Cuando el valor de una métrica cae por debajo del umbral bajo, Workload Balancing determina que los hosts están infrautilizados y hace una recomendación de optimización para consolidar las máquinas virtuales en un menor número de hosts. Workload Balancing sigue recomendando mover las máquinas virtuales a un host hasta que los valores de las métricas de uno de los recursos del host alcancen su umbral alto.

    Sin embargo, después de reubicar una máquina virtual, la utilización de un recurso en el nuevo host de la máquina virtual puede superar un umbral crítico. En este caso, Workload Balancing utiliza temporalmente un algoritmo similar al algoritmo de equilibrio de carga de máximo rendimiento para encontrar un nuevo host para las máquinas virtuales. Workload Balancing sigue utilizando este algoritmo para recomendar mover las máquinas virtuales hasta que la utilización de los recursos en los hosts del grupo caiga por debajo del umbral alto.

Para cambiar los umbrales críticos:

1. En XenCenter, seleccione su grupo.
2. En el panel **Propiedades** del grupo, haga clic en la ficha **WLB**.
3. En la ficha **WLB**, haga clic en **Configuración**.
4. En el panel izquierdo, seleccione **Umbrales críticos**. Estos umbrales críticos se utilizan para evaluar la utilización de los recursos del host.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. En la página **Umbrales críticos**, escriba uno o más valores nuevos en los cuadros **Umbrales críticos**. Los valores representan la utilización de los recursos en el host.

   Equilibrio de carga de trabajo utiliza estos umbrales al hacer recomendaciones de ubicación de VM y optimización de grupos. Workload Balancing se esfuerza por mantener la utilización de recursos en un host por debajo de los valores críticos establecidos.

Ajustar ponderaciones métricas

La forma en que Workload Balancing utiliza las ponderaciones métricas al determinar qué hosts y máquinas virtuales procesar primero varía según el modo de optimización: densidad máxima o rendimiento máximo. En general, las ponderaciones métricas se utilizan cuando un grupo está en modo de rendimiento máximo. Sin embargo, cuando el equilibrio de carga de trabajo está en modo de densidad máxima, utiliza ponderaciones de métricas cuando un recurso supera su umbral crítico.

Cuando el equilibrio de carga de trabajo procesa las recomendaciones de optimización, crea un orden de optimización. El equilibrio de carga de trabajo determina el orden clasificando los hosts según los hosts que tienen los valores de métrica más altos para cualquier recurso que se clasifique como el más importante en la página de ponderaciones de métricas.

Modo de rendimiento máximo

En el modo de máximo rendimiento, el equilibrio de carga de trabajo utiliza ponderaciones métricas para determinar:

- En qué hosts se abordará primero el rendimiento
- Qué máquinas virtuales se recomienda migrar primero

Por ejemplo, si las escrituras en red son el recurso más importante, Workload Balancing primero hace recomendaciones de optimización para el host con el mayor número de escrituras en red por segundo. Para hacer que las escrituras de red sean el recurso más importante, mueva el control deslizante **Ponderación métrica** hacia la derecha y todos los demás controles deslizantes hacia el medio.

Si configura todos los recursos para que sean igualmente importantes, el equilibrio de carga de trabajo aborda primero el uso de la CPU y, en segundo lugar, la memoria, ya que estos recursos suelen ser los más restringidos. Para que todos los recursos sean igualmente importantes, configure el control deslizante **Ponderación métrica** en el mismo lugar para todos los recursos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Modo de densidad máxima

En el modo de densidad máxima, el equilibrio de carga de trabajo solo utiliza ponderaciones métricas cuando un host alcanza el umbral crítico. En ese momento, Workload Balancing aplica un algoritmo similar al algoritmo para obtener el máximo rendimiento hasta que ningún host supere los umbrales críticos. Al usar este algoritmo, el equilibrio de carga de trabajo utiliza ponderaciones métricas para determinar el orden de optimización de la misma manera que lo hace para el modo de rendimiento máximo.

Si dos o más hosts tienen recursos que superan sus umbrales críticos, Workload Balancing comprueba la importancia que ha establecido para cada recurso. Aprovecha esta importancia para determinar qué host se debe optimizar primero y qué máquinas virtuales de ese host se deben reubicar primero.

Por ejemplo, su grupo contiene el host A y el host B, que se encuentran en el siguiente estado:

- La utilización de la CPU en el host A supera su umbral crítico y la ponderación métrica para la utilización de la CPU se establece en **Más importante**.
- La utilización de la memoria en el host B supera su umbral crítico y la ponderación métrica para la utilización de la memoria se establece en **Menos importante**.

Workload Balancing recomienda optimizar primero el host A porque el recurso que contiene y que alcanzó el umbral crítico es el recurso al que se le ha asignado el peso más alto. Una vez que Workload Balancing determina que debe abordar el rendimiento en el host A, Workload Balancing comienza a recomendar la ubicación de las máquinas virtuales en ese host. Comienza con la máquina virtual que tiene la mayor utilización de CPU, ya que esa utilización de CPU es el recurso con mayor peso.

Una vez que Workload Balancing ha recomendado optimizar el host A, hace recomendaciones de optimización para el host B. Cuando recomienda la ubicación de las máquinas virtuales en el host B, lo hace abordando primero la utilización de la CPU, ya que a la utilización de la CPU se le ha asignado la máxima importancia. Si hay más hosts que necesitan optimización, el equilibrio de carga de trabajo aborda el rendimiento de esos hosts de acuerdo con el host que tenga el tercer mayor uso de CPU.

De forma predeterminada, todas las ponderaciones métricas se establecen en el punto más lejano del control deslizante: Más importante.

> **Nota:**
>
> La ponderación de las métricas es relativa. Si todas las métricas se establecen en el mismo nivel, incluso si ese nivel es Menos importante, todas se ponderarán de la misma manera. La relación de las métricas entre sí es más importante que el peso real en el que se establece cada métrica.

Para modificar los factores de ponderación de métrica

1. En XenCenter, seleccione su grupo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. En el panel **Propiedades** del grupo, haga clic en la ficha **WLB**.
3. En la ficha **WLB**, haga clic en **Configuración**.
4. En el panel izquierdo, seleccione **Ponderación métrica**.
5. En la página **Ponderación de métricas**, si lo quiere, ajuste los controles deslizantes junto a los recursos individuales.

   Mueva el control deslizante hacia **Menos importante** para indicar que garantizar que las VM siempre tengan la mayor cantidad disponible de este recurso no es tan vital para este grupo.

Excluir a los anfitriones de las recomendaciones

Al configurar el equilibrio de carga de trabajo, puede especificar que los hosts físicos específicos se excluyan de las recomendaciones de optimización y colocación del equilibrio de carga de trabajo, incluidas las recomendaciones de ubicación de inicio.

Las situaciones en las que es posible que quiera excluir hosts de las recomendaciones incluyen las siguientes:

- Desea ejecutar el grupo en modo de densidad máxima y consolidar y cerrar los hosts, pero quiere excluir hosts específicos de este comportamiento.
- Tiene dos cargas de trabajo de máquinas virtuales que siempre deben ejecutarse en el mismo host. Por ejemplo, si las VM tienen aplicaciones o cargas de trabajo complementarias.
- Tiene cargas de trabajo que no quiere mover: por ejemplo, un controlador de dominio o un servidor de base de datos.
- Desea realizar el mantenimiento en un host y no quiere que las máquinas virtuales se coloquen en el host.
- El rendimiento de la carga de trabajo es tan crítico que el coste del hardware dedicado es irrelevante.
- Los hosts específicos ejecutan cargas de trabajo de alta prioridad y no quiere utilizar la función de alta disponibilidad para priorizar estas máquinas virtuales.
- El hardware del host no es el óptimo para las demás cargas de trabajo del grupo.

Independientemente de si especifica un modo de optimización fijo o programado, los hosts excluidos permanecen excluidos incluso cuando cambia el modo de optimización. Por lo tanto, si solo quiere evitar que el equilibrio de carga de trabajo apague un host automáticamente, considere la posibilidad de inhabilitar la administración de energía para ese host. Para obtener más información, consulte Optimizar y administrar la energía automáticamente.

Al excluir un host de las recomendaciones, está especificando que Workload Balancing no administre ese host en absoluto. Esta configuración significa que Workload Balancing no hace ninguna recomendación de optimización para un host excluido. Por el contrario, si no selecciona un host para que

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

participe en la administración de energía, Workload Balancing administra el host, pero no hace recomendaciones de administración de energía para él.

Para excluir los hosts del equilibrio de carga de trabajo

Utilice este procedimiento para excluir un host de un grupo que Workload Balancing administra de las recomendaciones de administración de energía, evacuación, ubicación y optimización del host.

1. En XenCenter, seleccione su grupo.
2. En el panel **Propiedades** del grupo, haga clic en la ficha **WLB**.
3. En la ficha **WLB**, haga clic en **Configuración**.
4. En el panel izquierdo, seleccione **Hosts excluidos**.
5. En la página **Hosts excluidos**, seleccione los hosts para los que no quiere que Workload Balancing recomiende ubicaciones y optimizaciones alternativas.

Configurar ajustes avanzados

Equilibrio de carga de trabajo proporciona algunos ajustes avanzados que le permiten controlar cómo el equilibrio de carga de trabajo aplica las recomendaciones Esta configuración aparece en la página **Avanzado** del cuadro de diálogo Configuración de equilibrio de carga de trabajo. Para llegar a la página **Avanzado**, siga los pasos que se indican a continuación:

1. En XenCenter, seleccione su grupo.
2. En el panel **Propiedades** del grupo, haga clic en la ficha **WLB**.
3. En la ficha **WLB**, haga clic en **Configuración**.
4. En el panel izquierdo, seleccione **Avanzado**.

En las siguientes secciones se describen los comportamientos que se pueden configurar en la configuración **avanzada**.

Establecer recomendaciones automatizadas conservadoras o agresivas

Cuando se ejecuta en modo automatizado, la frecuencia de las recomendaciones de optimización y consolidación y la rapidez con la que se aplican automáticamente son producto de varios factores, que incluyen:

- Cuánto tiempo especifica que el equilibrio de carga de trabajo espera después de mover una VM antes de hacer otra recomendación

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- El número de recomendaciones que debe hacer el equilibrio de carga de trabajo antes de aplicar una recomendación automáticamente
- El nivel de gravedad que debe alcanzar una recomendación antes de que la optimización se aplique automáticamente
- El nivel de coherencia en las recomendaciones (máquinas virtuales recomendadas para mover, hosts de destino) que requiere el equilibrio de carga de trabajo antes de aplicar las recomendaciones automáticamente

En general, solo ajuste la configuración para estos factores en los siguientes casos:

- Cuenta con las instrucciones del soporte técnico de XenServer
- Ha realizado observaciones y pruebas importantes del comportamiento de su grupo con el equilibrio de carga de trabajo habilitado

La configuración incorrecta de estos ajustes puede provocar que Equilibrio de carga de trabajo no haga ninguna recomendación.

Intervalo de migración VM

Puede especificar el número de minutos que espera el equilibrio de carga de trabajo después de la última vez que se movió una máquina virtual, antes de que el equilibrio de carga de trabajo pueda hacer otra recomendación para esa máquina virtual. El intervalo de recomendación está diseñado para evitar que el equilibrio de carga de trabajo genere recomendaciones por motivos artificiales, por ejemplo, si hubo un pico de utilización temporal.

Cuando se configura la automatización, es especialmente importante tener cuidado al modificar el intervalo de recomendación. Si se produce un problema que provoca picos continuos y recurrentes, la disminución del intervalo puede generar muchas recomendaciones y, por lo tanto, reubicaciones.

> **Nota:**
>
> Establecer un intervalo de recomendación no afecta al tiempo de espera de Workload Balancing para incluir los hosts reequilibrados recientemente en las recomendaciones de ubicación inicial, reanudación y modo de mantenimiento.

Recuento de recomendaciones

Cada dos minutos, el equilibrio de carga de trabajo comprueba si puede generar recomendaciones para el grupo que está supervisando. Cuando habilita la automatización, puede especificar el número de veces que se debe hacer una recomendación coherente antes de que Equilibrio de carga de trabajo aplique la recomendación automáticamente. Para hacerlo, configure un ajuste conocido como **Recuento de recomendaciones**, como se especifica en el campo **Recomendaciones**. La configuración

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Recuento de recomendaciones y **Agresividad de optimización** le permiten ajustar la aplicación automatizada de recomendaciones en su entorno.

Equilibrio de carga de trabajo utiliza la similitud de recomendaciones para realizar las siguientes comprobaciones

1. Si la recomendación es realmente necesaria
2. Si el host de destino tiene un rendimiento lo suficientemente estable durante un período prolongado como para aceptar una máquina virtual reubicada sin necesidad de volver a moverla del host en breve

Equilibrio de carga de trabajo utiliza el valor Recuento de recomendaciones para determinar si una recomendación debe repetirse antes de que el equilibrio de carga de trabajo aplique la recomendación Equilibrio de carga de trabajo usa esta configuración de la

1. Cada vez que el equilibrio de carga de trabajo genera una recomendación que cumple con sus requisitos de consistencia, como se indica en la configuración Agresividad de Optimización, el equilibrio de carga de trabajo incrementa el Recuento de Recomendaciones. Si la recomendación no cumple con los requisitos de coherencia, el equilibrio de carga de trabajo puede restablecer el recuento de recomendaciones a cero. Este comportamiento depende de los factores descritos en Agresividad de optimización.
2. Cuando el equilibrio de carga de trabajo genera suficientes recomendaciones coherentes para cumplir con el valor del recuento de recomendaciones, como se especifica en el campo **Recomendaciones**, aplica automáticamente la recomendación.

Si decide modificar esta configuración, el valor que quiere establecer varía según el entorno. Considere estos casos:

- Si la carga y la actividad de los hosts aumentan rápidamente en su entorno, es posible que quiera aumentar el valor del recuento de recomendaciones. El equilibrio de carga de trabajo genera recomendaciones cada dos minutos. Por ejemplo, si establece este intervalo en **3**, seis minutos después, el equilibrio de carga de trabajo aplica la recomendación automáticamente.
- Si la carga y la actividad de los hosts aumentan gradualmente en su entorno, es posible que quiera reducir el valor del recuento de recomendaciones.

La aceptación de recomendaciones utiliza recursos del sistema y afecta al rendimiento cuando Equilibrio de carga de trabajo está reubicando las VM. Aumentar el recuento de recomendaciones aumenta el número de recomendaciones coincidentes que deben producirse antes de que el equilibrio de carga de trabajo aplique la recomendación. Esta configuración anima a Equilibrio de carga de trabajo a aplicar recomendaciones más conservadoras y estables y puede reducir la posibilidad de movimientos de VM espurios. El recuento de recomendaciones se establece en un valor conservador de forma predeterminada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Debido al impacto potencial que puede tener el ajuste de esta configuración en su entorno, solo cámbielo con extrema precaución. Preferiblemente, realice estos ajustes probando y cambiando el valor de forma iterativa o siguiendo las instrucciones del soporte técnico de XenServer.

Gravedad de recomendaciones

Todas las recomendaciones de optimización incluyen una calificación de gravedad (crítica, alta, media, baja) que indica la importancia de la recomendación. Equilibrio de carga de trabajo basa esta calificación en una combinación de factores, incluidos los siguientes:

- Opciones de configuración que establezca, como umbrales y ajustes de métricas
- Recursos disponibles para la carga de trabajo
- Historial de uso de recursos.

La clasificación de gravedad de una recomendación aparece en el panel **Recomendaciones de optimización** de la ficha **WLB**.

Cuando configura Equilibrio de carga de trabajo para aplicar recomendaciones automáticamente, puede establecer el nivel de gravedad mínimo para asociarlo a una recomendación antes de que Equilibrio de carga de trabajo lo aplique automáticamente.

Agresividad de optimización

Para proporcionar seguridad adicional cuando se ejecuta en modo automatizado, Equilibrio de carga de trabajo tiene criterios de coherencia para aceptar optimizaciones automáticamente. Este criterio puede ayudar a evitar que las VM se muevan debido a picos y anomalías. En el modo automatizado, el equilibrio de carga de trabajo no acepta la primera recomendación que produce. En cambio, Workload Balancing espera a aplicar una recomendación automáticamente hasta que un host o una máquina virtual muestre un comportamiento coherente a lo largo del tiempo. El comportamiento coherente a lo largo del tiempo incluye factores como si un host sigue activando recomendaciones y si las mismas máquinas virtuales de ese host siguen activando recomendaciones.

Equilibrio de carga de trabajo determina si el comportamiento es coherente mediante el uso de criterios de coherencia y teniendo criterios para el número de veces que se hace la misma recomendación. Puede configurar hasta qué punto quiere que Equilibrio de carga de trabajo aplique los criterios de coherencia mediante la configuración **Agresividad de optimización**. Puede usar esta configuración para controlar la cantidad de estabilidad que quiere en su entorno antes de que Equilibrio de carga de trabajo aplique una recomendación de optimización. La configuración más estable, Baja agresividad, se configura de forma predeterminada. En este contexto, el término estable significa la similitud de los cambios recomendados a lo largo del tiempo, como se explica a lo largo de esta sección. La agresividad no es deseable en la mayoría de los entornos. Por lo tanto, Low es la configuración predeterminada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Equilibrio de carga de trabajo utiliza hasta cuatro criterios para determinar la coherencia. El número de criterios que deben cumplirse varía según el nivel que establezca en la configuración **Agresividad de optimización**. Cuanto más bajo sea el nivel (por ejemplo, bajo o medio), menos agresivo será el equilibrio de carga de trabajo al aceptar una recomendación. En otras palabras, Equilibrio de carga de trabajo es más estricto en cuanto a requerir que los criterios coincidan cuando la agresividad se establece en Baja.

Por ejemplo, si el nivel de agresividad se establece en Bajo, cada criterio de Bajo debe cumplirse el número de veces especificado por el valor Recuento de recomendaciones antes de aplicar automáticamente la recomendación.

Si establece el Recuento de recomendaciones en **3**, Equilibrio de carga de trabajo espera hasta que se cumplan todos los criterios enumerados para Bajo y se repitan en tres recomendaciones consecutivas. Esta configuración ayuda a garantizar que realmente sea necesario mover la máquina virtual y que el host de destino recomendado tenga un uso estable de los recursos durante un período más prolongado. Reduce la posibilidad de que una máquina virtual trasladada recientemente se traslade de un host debido a cambios en el rendimiento del host tras el traslado. De forma predeterminada, este ajuste se establece en Bajo para fomentar la estabilidad.

No recomendamos aumentar la configuración de **agresividad de la optimización** para aumentar la frecuencia con la que se optimizan los hosts. Si cree que sus hosts no se optimizan con la suficiente rapidez o frecuencia, intente ajustar los umbrales críticos. Compare los umbrales con el informe de estado de la agrupación.

Los criterios de consistencia asociados a los diferentes niveles de agresividad son los siguientes:

Bajo:

- Todas las VM en las recomendaciones posteriores deben ser iguales (como se demuestra al hacer coincidir los UUID en cada recomendación).
- Todos los anfitriones de destino deben ser iguales en las recomendaciones posteriores
- La recomendación que sigue inmediatamente a la recomendación inicial debe coincidir o, de lo contrario, el recuento de recomendaciones vuelve a 1

Mediano:

- Todas las máquinas virtuales de las recomendaciones posteriores deben ser del mismo host; sin embargo, pueden ser máquinas virtuales diferentes de las de la primera recomendación.
- Todos los anfitriones de destino deben ser iguales en las recomendaciones posteriores
- Una de las dos recomendaciones siguientes que siguen inmediatamente a la primera recomendación debe coincidir o, de lo contrario, el recuento de recomendaciones vuelve a 1.

Alto:

- Todas las máquinas virtuales de las recomendaciones deben provenir del mismo host. Sin embargo, las recomendaciones no tienen que seguirse de inmediato.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- El host desde el que Workload Balancing recomendó que el movimiento de la máquina virtual fuera el mismo en cada recomendación
- El recuento de recomendaciones permanece en el mismo valor incluso cuando las dos recomendaciones que siguen a la primera recomendación no coinciden.

Ejemplo de agresividad de optimización El siguiente ejemplo ilustra cómo Equilibrio de carga de trabajo utiliza la configuración **Agresividad de optimización** y el recuento de recomendaciones para determinar si se debe aceptar una recomendación automáticamente.

Cada recomendación de optimización emitida por Workload Balancing propone tres ubicaciones de VM. Después de estas ubicaciones propuestas, el recuento de recomendaciones asociado con cada nivel de agresividad es el número de veces que ha habido recomendaciones consecutivas en esa configuración de Agresividad de optimización.

En los siguientes ejemplos, cuando la configuración **Agresividad de optimización** se establece en Alta, el recuento de recomendaciones sigue aumentando después de las recomendaciones 1, 2 y 3. Este aumento se produce a pesar de que no se recomiendan las mismas VM para las nuevas ubicaciones en cada recomendación. Workload Balancing aplica la recomendación de ubicación junto con la recomendación 3 porque ha observado el mismo comportamiento en ese host durante tres recomendaciones consecutivas.

Por el contrario, cuando se establece en Agresividad baja, el recuento de recomendaciones consecutivas no aumenta para las cuatro primeras recomendaciones. El recuento de recomendaciones se restablece a 1 con cada recomendación porque no se recomendaron las mismas VM para las ubicaciones. El recuento de recomendaciones no comienza a aumentar hasta que se hace la misma recomendación en la Recomendación #5. Por último, Equilibrio de carga de trabajo aplica automáticamente la recomendación hecha en la Recomendación #6 después de la tercera vez que emite las mismas recomendaciones de ubicación.

Recomendación 1:

Emplazamientos propuestos:

- Mover la VM1 del host A al host B
- Mover la VM3 del host A al host B
- Mover la VM5 del host A al host C

La recomendación cuenta:

- Recuento de recomendaciones de alta agresividad: 1
- Recuento de recomendaciones de agresividad media: 1
- Recuento de recomendaciones de baja agresividad: 1

Recomendación 2:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Emplazamientos propuestos:

- Mover la VM1 del host A al host B
- Mover la VM3 del host A al host C
- Mover la VM7 del host A al host C

La recomendación cuenta:

- Recuento de recomendaciones de alta agresividad: 2
- Recuento de recomendaciones de agresividad media: 1
- Recuento de recomendaciones de baja agresividad: 1

Recomendación 3:

Emplazamientos propuestos:

- Mover la VM1 del host A al host B
- Mover la VM3 del host A al host C
- Mover la VM5 del host A al host C

La recomendación cuenta:

- Recuento de recomendaciones de alta agresividad: 3 (Aplicar)
- Recuento de recomendaciones de agresividad media: 1
- Recuento de recomendaciones de baja agresividad: 1

Recomendación 4:

Emplazamientos propuestos:

- Mover la VM1 del host A al host B
- Mover la VM3 del host A al host B
- Mover la VM5 del host A al host C

La recomendación cuenta:

- Recuento de recomendaciones de agresividad media: 2
- Recuento de recomendaciones de baja agresividad: 1

Recomendación 5:

Emplazamientos propuestos:

- Mover la VM1 del host A al host B
- Mover la VM3 del host A al host B
- Mover la VM5 del host A al host C

La recomendación cuenta:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Recuento de recomendaciones de agresividad media: 3 (Aplicar)
- Recuento de recomendaciones de baja agresividad: 2

Recomendación 6:

Emplazamientos propuestos:

- Mover la VM1 del host A al host B
- Mover la VM3 del host A al host B
- Mover la VM5 del host A al host C

La recomendación cuenta:

- Recuento de recomendaciones de baja agresividad: 3 (Aplicar)

Para configurar los intervalos de recomendación de VM

1. En XenCenter, seleccione su grupo.
2. En el panel **Propiedades** del grupo, haga clic en la ficha **WLB**.
3. En la ficha **WLB**, haga clic en **Configuración**.
4. En el panel izquierdo, haga clic en **Avanzado**.
5. En la sección **Intervalo de recomendación de VM**, lleve a cabo una o varias de las siguientes acciones:

    - En el cuadro **Minutos**, escriba un valor para el número de minutos que espera Workload Balancing antes de realizar otra recomendación de optimización en un host recién reequilibrado.
    - En el cuadro **Recomendaciones**, escriba un valor para el número de recomendaciones que quiere que haga Equilibrio de carga de trabajo antes de que aplique una recomendación automáticamente.
    - Seleccione un nivel de gravedad mínimo antes de que las optimizaciones se apliquen automáticamente.
    - Modifique la forma en que Equilibrio de carga de trabajo aplica las recomendaciones de optimización cuando se ejecuta en modo automatizado. El aumento del nivel de agresividad reduce las restricciones en la coherencia de las recomendaciones antes de aplicarlas automáticamente. La configuración **Agresividad de optimización** complementa directamente la configuración de **Recomendaciones**; es decir, las recomendaciones cuentan.

        > **Nota:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Si escribe “1”para el valor en la configuración **Recomendaciones**, la configuración **Agresividad de optimización** no es relevante.

Ajustar la configuración de granularidad del registro de auditoría de

Siga este procedimiento para modificar la configuración de granularidad:

1. En XenCenter, seleccione su grupo.
2. En el panel **Propiedades** del grupo, haga clic en la ficha **WLB**.
3. En la ficha **WLB**, haga clic en **Configuración**.
4. En el panel izquierdo, haga clic en **Avanzado**.
5. En la página **Avanzado**, haga clic en la lista **Granularidad del informe de seguimiento de auditoría de grupo** y seleccione una opción de la lista.

   > **Importante:**
   >
   > Seleccione la granularidad en función de sus requisitos de registro de auditoría. Por ejemplo, si establece la granularidad del informe del registro de auditoría en Mínimo, el informe solo captura una cantidad limitada de datos para usuarios y tipos de objetos específicos. Si establece la granularidad en Media, el informe proporciona un informe fácil de usar del registro de auditoría. Si elige establecer la granularidad en Máximo, el informe contiene información detallada sobre el informe de registro de auditoría. Establecer el informe de registro de auditoría en Máximo puede provocar que el servidor Equilibrio de carga de trabajo utilice más espacio en disco y memoria.

6. Para confirmar los cambios, haga clic en **Aceptar**.

Vea los informes de Pool Audit Trail basados en objetos en XenCenter

Siga este procedimiento para ejecutar y ver informes de la pista de auditoría de agrupaciones en función del objeto seleccionado:

1. Tras configurar la configuración de granularidad de Pool Audit Trail, haga clic en **Informes**. Aparece la página Informes de carga de trabajo
2. Seleccione **Pool Audit Trail** en el panel izquierdo.
3. Puede ejecutar y ver los informes en función de un objeto específico seleccionándolo en la lista **Objeto**. Por ejemplo, elija **Anfitrión** de la lista para obtener los informes basados únicamente en el anfitrión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Personalice los objetos y las acciones del evento capturados por el registro de auditoría de agrupaciones

Para personalizar los objetos de eventos y las acciones capturados por el registro de auditoría del grupo, debe iniciar sesión en la base de datos de PostgreSQL del dispositivo virtual de equilibrio de carga de trabajo, realizar los cambios pertinentes en la lista de objetos o acciones de eventos y, a continuación, reiniciar el dispositivo virtual de equilibrio de carga de trabajo.

Inicie sesión en la base de datos de PostgreSQL

1. Inicie sesión en la consola del dispositivo virtual Workload Balancing.
2. Ejecute este comando:

```
psql -Upostgres -dWorkloadBalancing
<!--NeedCopy-->
```

3. Introduzca la contraseña de la base de datos. Estableció la contraseña de la base de datos al ejecutar el asistente de configuración de equilibrio de carga de trabajo después de importar el dispositivo virtual.

Personalizar objetos de eventos

> **Nota:**
>
> En la sintaxis del comando siguiente, `event_object` representa el nombre del objeto de evento que quiere agregar, actualizar o inhabilitar.

Habilitar un objeto de evento:

```
select * from update_audit_log_objects('event_object', true);
<!--NeedCopy-->
```

Desactivar un objeto de evento:

```
select * from update_audit_log_objects('event_object', false);
<!--NeedCopy-->
```

Obtenga una lista de los objetos de eventos que están inhabilitados actualmente:

```
select * from hv_audit_log_get_event_objects(false);
<!--NeedCopy-->
```

Obtenga una lista de los objetos de eventos que están habilitados actualmente:

```
select * from hv_audit_log_get_event_objects(true);
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Personaliza las acciones del evento

> **Nota:**
>
> En la sintaxis del comando siguiente, `event_action` representa el nombre de la acción de evento que quiere agregar, actualizar o inhabilitar.

Habilitar una acción de evento:

```
select * from update_audit_log_actions('event_action', true);
<!--NeedCopy-->
```

Desactivar una acción de evento:

```
select * from update_audit_log_actions('event_action', false);
<!--NeedCopy-->
```

Obtenga una lista de las acciones del evento que están inhabilitadas actualmente:

```
select * from hv_audit_log_get_event_actions(false);
<!--NeedCopy-->
```

Obtenga una lista de las acciones de eventos que están habilitadas actualmente:

```
select * from hv_audit_log_get_event_actions(true);
<!--NeedCopy-->
```

Reinicie el dispositivo virtual de equilibrio de carga de trabajo Ejecute los siguientes comandos para salir de PostgreSQL y reiniciar el dispositivo virtual de equilibrio de carga de trabajo.

```
\q
<!--NeedCopy-->
```

```
systemctl restart workloadbalancing
<!--NeedCopy-->
```

Establecer el nivel de alerta para las alertas de equilibrio de carga de trabajo en XenCenter

Puede establecer el nivel de alerta para las alertas de Workload Balancing en XenCenter mediante la API de administración.

Siga estos pasos:

1. Ejecute el siguiente comando en el coordinador del grupo para establecer el nivel de alerta de cada código de alerta:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe pool-send-wlb-configuration config:<wlb-alert-code>=<alert-
    level>
<!--NeedCopy-->
```

Los 4 `wlb-alert-code` tipos son:

- MESSAGE_PRIORITY_WLB_OPTIMIZATION_ALERT: si el equilibrio de carga de trabajo ofrece una recomendación de optimización, se genera esta alerta.
- MESSAGE_PRIORITY_WLB_VM_RELOCATION: si el equilibrio de carga de trabajo reubica una máquina virtual en otro host, se genera esta alerta.
- MESSAGE_PRIORITY_WLB_HOST_POWER_OFF: si se ha configurado el modo de optimización del equilibrio de carga de trabajo en `Maximize Density` y un host está apagado porque no hay máquinas virtuales ejecutándose en el host, se genera esta alerta.
- MESSAGE_PRIORITY_WLB_HOST_POWER_ON: si el modo de optimización del equilibrio de carga de trabajo se ha configurado en `Maximize Performance` y un host está encendido porque al hacerlo mejora el rendimiento del host, se genera esta alerta.

Los 6 `alert-level` tipos son:

- 0 - Silencia la alerta
- 1 - Crítica
- 2 - Importante
- 3 - Advertencia
- 4 - Menor
- 5 - Informativa

2. Ejecute el siguiente comando en el coordinador del grupo para ver los niveles de alerta establecidos para los códigos de alerta:

```
xe pool-retrieve-wlb-configuration
<!--NeedCopy-->
```

3. Para probar las alertas, genere una alerta de equilibrio de carga de trabajo y, a continuación, haga clic en el panel `Notifications` para ver la alerta.

Administrar el equilibrio de carga

November 8, 2023

Después de que el equilibrio de carga de trabajo se haya ejecutado durante un tiempo, hay tareas rutinarias que puede que deba realizar para que el equilibrio de carga de trabajo se ejecute de manera

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

óptima. Es posible que deba realizar estas tareas debido a cambios en su entorno (como diferentes direcciones IP o credenciales), actualizaciones de hardware o mantenimiento rutinario.

Conectarse al dispositivo virtual de equilibrio de carga de trabajo

Después de la configuración de Equilibrio de carga de trabajo, conecte el grupo que quiere administrar al dispositivo virtual Equilibrio de carga de trabajo mediante la CLI o XenCenter. Del mismo modo, es posible que deba volver a conectarse al mismo dispositivo virtual en algún momento.

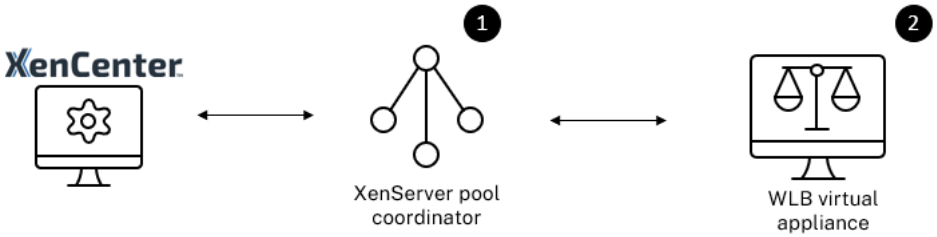
Para conectar un grupo a su dispositivo virtual de equilibrio de carga de trabajo, necesita la siguiente información:

- Dirección IP o FQDN del dispositivo virtual de Workload Balancing
  - Para obtener la dirección IP del dispositivo virtual de Workload Balancing:
    1. En XenCenter, vaya a la ficha **Consola** del dispositivo virtual de Workload Balancing.
    2. Inicie sesión como `root` con la contraseña raíz que creó al importar el dispositivo.
    3. Ejecute el siguiente comando: `ifconfig`.
  - Para especificar el FQDN de equilibrio de carga de trabajo al conectarse al servidor de equilibrio de carga de trabajo, primero agregue su nombre de host y dirección IP a su servidor DNS.
- El número de puerto del dispositivo virtual de Workload Balancing. De forma predeterminada, XenServer se conecta al equilibrio de carga de trabajo en el puerto 8012.

  Modifique únicamente el número de puerto cuando lo haya cambiado durante la configuración de equilibrio de carga de trabajo. El número de puerto especificado durante la configuración de equilibrio de carga de trabajo, en cualquier regla de firewall y en el cuadro de diálogo Conectar al servidor WLB debe coincidir.
- Credenciales de la agrupación de recursos que quiere que supervise Equilibrio de carga de trabajo.
- Credenciales para la cuenta de equilibrio de carga de trabajo que creó durante la configuración de equilibrio de

  Esta cuenta se conoce a menudo como cuenta de usuario de equilibrio de carga de trabajo. XenServer usa esta cuenta para comunicarse con Workload Balancing. Creó esta cuenta en el dispositivo virtual de Workload Balancing durante la configuración de equilibrio de carga

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Cuando se conecta por primera vez al equilibrio de carga de trabajo, utiliza los umbrales y la configuración predeterminados para equilibrar cargas de trabajo. Las funciones automáticas, como el modo de optimización automatizada, la administración de energía y la automatización, están inhabilitadas de forma predeterminada.

Trabajar con certificados

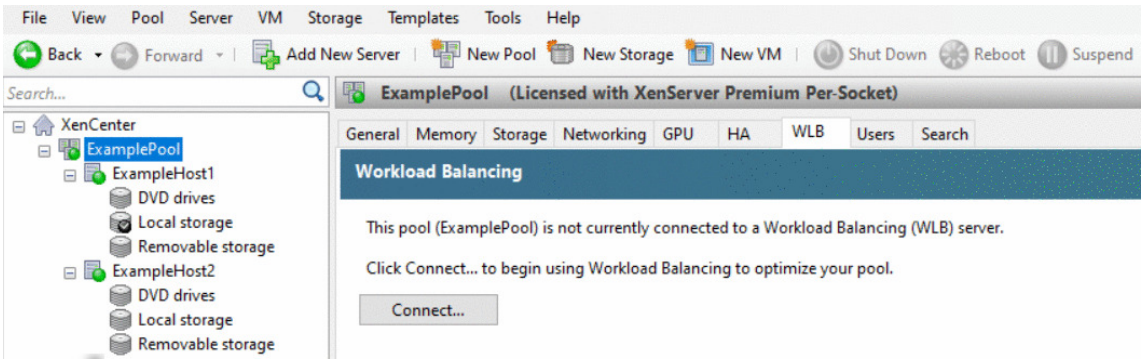
Si quiere cargar un certificado diferente (de confianza) o configurar la verificación de certificados, tenga en cuenta lo siguiente antes de conectar el grupo a Workload Balancing:

- Si quiere que XenServer verifique el certificado de equilibrio de carga de trabajo autofirmado, debe usar la dirección IP de equilibrio de carga de trabajo para conectarse a equilibrio de carga de trabajo. El certificado autofirmado se emite para Workload Balancing en función de su dirección IP.
- Si quiere utilizar un certificado de una entidad de certificación, es más fácil especificar el FQDN al conectarse a Workload Balancing. Sin embargo, puede especificar una dirección IP estática en el cuadro de diálogo **Conectar al servidor WLB**. Use esta dirección IP como el nombre alternativo del firmante (SAN) en el certificado.

Para obtener más información, consulte Certificados.

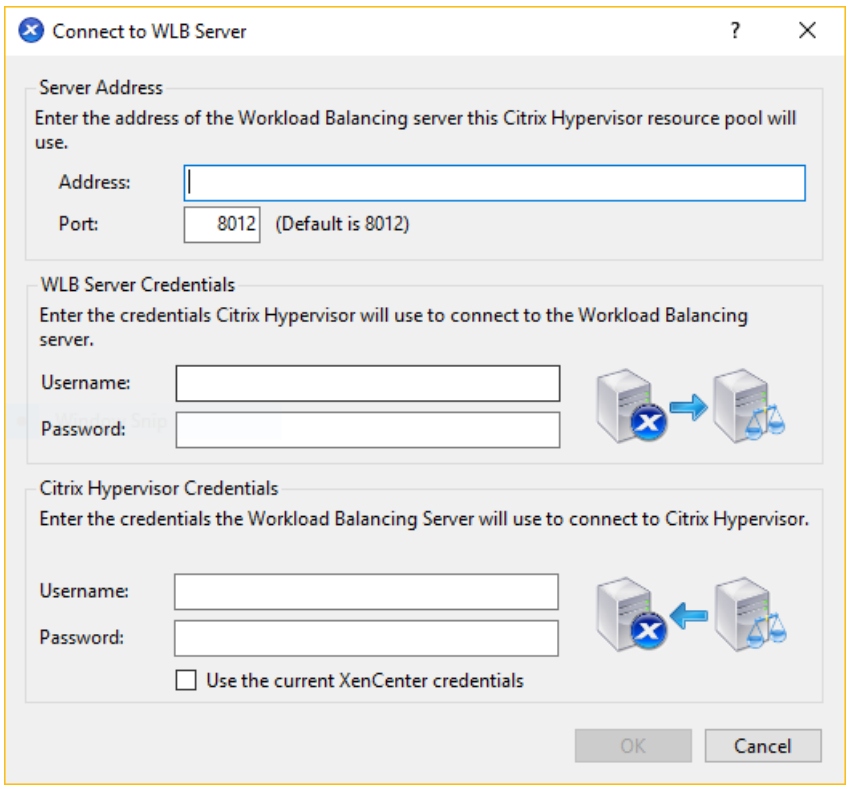
Para conectar su grupo al dispositivo virtual de Workload Balancing

1. En XenCenter, seleccione el grupo de recursos y, en su panel **Propiedades**, haga clic en la ficha **WLB**. La ficha **WLB** muestra el botón **Conectar**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. En la ficha **WLB**, haga clic en **Conectar**. Aparece el cuadro de diálogo **Conectarse al servidor WLB**.



3. En la sección **Dirección del servidor**, introduzca lo siguiente:

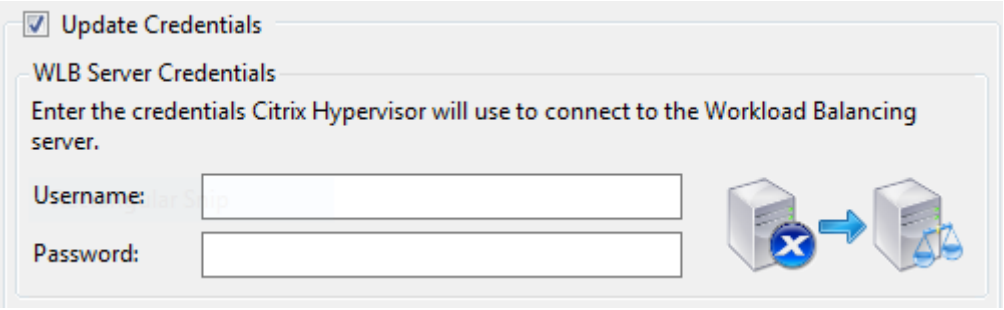
   a) En el cuadro **Dirección**, escriba la dirección IP o el FQDN del dispositivo virtual de Workload Balancing. Por ejemplo: `WLB-appliance-computername.yourdomain.net` .

   b) (Opcional) Si cambió el puerto de equilibrio de carga de trabajo durante la configuración de equilibrio de carga de trabajo, introduzca el número de puerto en el cuadro **Puerto**. XenServer usa este puerto para comunicarse con Workload Balancing.

      De forma predeterminada, XenServer se conecta al equilibrio de carga de trabajo en el puerto 8012.

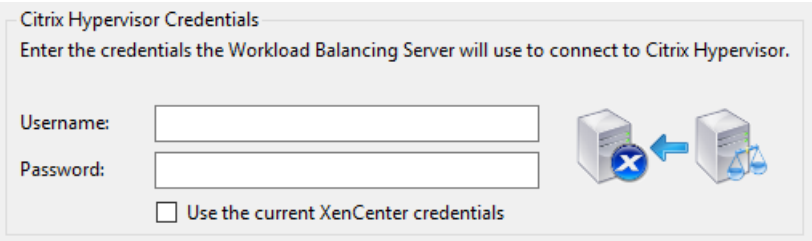
4. En la sección **Credenciales del servidor WLB**, introduzca el nombre de usuario y la contraseña que el grupo utiliza para conectarse al dispositivo virtual de Workload Balancing.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Estas credenciales deben ser para la cuenta que creó durante la configuración del equilibrio de carga de trabajo. De forma predeterminada, el nombre de usuario de esta cuenta es `wlbuser`.

5. En la sección **Credenciales de Citrix Hypervisor**, introduzca el nombre de usuario y la contraseña del grupo que está configurando. Workload Balancing usa estas credenciales para conectarse a los hosts de ese grupo.



Para usar las credenciales con las que ha iniciado sesión actualmente en XenServer, seleccione **Usar las credenciales actuales de XenCenter**. Si asignó una función a esta cuenta mediante la función de control de acceso basado en funciones (RBAC), asegúrese de que la función tenga permisos suficientes para configurar el equilibrio de carga de trabajo. Para obtener más información, consulte Permisos de control de acceso de equilibrio de cargade

Después de conectar el grupo al dispositivo virtual de Workload Balancing, el equilibrio de carga de trabajo comienza a supervisar automáticamente el grupo con la configuración de optimización predeterminada. Si quiere modificar esta configuración o cambiar la prioridad asignada a los recursos, espere hasta que el registro de XenCenter muestre que la detección ha finalizado antes de continuar.

> **Importante:**
>
> Después de que el equilibrio de carga de trabajo se ejecute durante un tiempo, si no recibe recomendaciones óptimas, evalúe los umbrales de rendimiento como se describe en Configurar el comportamiento del equilibrio de cargade trabajo. Es fundamental establecer el equilibrio de carga de trabajo en los umbrales correctos para su entorno o es posible que sus recomendaciones no sean apropiadas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Permisos de control de acceso de equilibrio

Cuando se implementa el control de acceso basado en roles (RBAC) en su entorno, todos los roles de usuario pueden mostrar la ficha **WLB**. Sin embargo, no todos los roles pueden realizar todas las operaciones. En la siguiente tabla se enumeran las funciones mínimas que los administradores deben utilizar las funciones de equilibrio de carga de trabajo

Permiso	Función mínima requerida
Configurar, inicializar, habilitar, inhabilitar WLB	Operador de grupo
Aplicar recomendaciones de optimización de WLB en la ficha WLB	Operador de grupo
Modificar suscripciones a informes de WLB	Operador de grupo
Aceptar recomendaciones de ubicación de WLB	Administrador de energía de VM
Generar informes de WLB, incluido el informe de seguimiento de auditoría de grupos	Solo lectura
Mostrar configuración de WLB	Solo lectura

En la siguiente tabla se proporcionan más detalles sobre los permisos.

Permiso	Permite a la persona asignada
Configurar, inicializar, habilitar, inhabilitar WLB	Configurar WLB Inicializar WLB y cambiar los servidores WLB Habilitar WLB Inhabilitar WLB
Aplicar recomendaciones de optimización de WLB en la ficha WLB	Aplicar las recomendaciones de optimización que aparecen en la ficha **WLB**
Modificar suscripciones a informes de WLB	Cambiar el informe de WLB generado o su destinatario
Aceptar recomendaciones de ubicación de WLB	Seleccione uno de los hosts que Workload Balancing recomienda para su ubicación
Generar informes de WLB, incluido el informe de seguimiento de auditoría de grupos	Ver y generar informes de WLB, incluido el informe de seguimiento de auditoría de grupos
Mostrar configuración de WLB	Ver la configuración de WLB para un grupo como se muestra en la ficha WLB

Si un usuario intenta usar Equilibrio de carga de trabajo y ese usuario no tiene suficientes permisos,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

aparece un cuadro de diálogo de elevación de roles. Para obtener más información sobre RBAC, consulte Control de acceso basado en roles.

Reconfigurar un grupo para usar otro dispositivo virtual de equilibrio de carga de trabajo

Puede volver a configurar una agrupación de recursos para utilizar un dispositivo virtual de Equilibrio de carga de trabajo diferente.

Si va a pasar de una versión anterior del dispositivo virtual Equilibrio de carga de trabajo a la versión más reciente, antes de desconectar el dispositivo virtual anterior, puede migrar sus datos a la nueva versión del dispositivo virtual. Para obtener más información, consulte Migrar datos de un dispositivo virtual existente.

Después de desconectar un grupo del antiguo dispositivo virtual de equilibrio de carga de trabajo, puede conectar el grupo especificando el nombre del nuevo dispositivo virtual de equilibrio de carga de trabajo.

Para usar un dispositivo virtual de equilibrio de carga de trabajo diferente:

1. (Opcional) Migre los datos de una versión anterior del dispositivo virtual. Para obtener más información, consulte Migrar datos de un dispositivo virtual existente.
2. En XenCenter, en el menú **Agrupación**, seleccione **Disconnect Workload Balancing Server** y haga clic en **Desconectar** cuando se le solicite.
3. En la ficha **WLB**, haga clic en **Conectar**. Aparecerá el cuadro de diálogo **Conectarse a WLB Server**.
4. Conéctese al nuevo dispositivo virtual. Para obtener más información, consulte Conectarse al dispositivo virtual Equilibrio de cargade trabajo

Cambio de las credenciales de equilibrio de carga

Tras la configuración inicial, si quiere actualizar las credenciales que XenServer y el dispositivo Workload Balancing utilizan para comunicarse, siga el siguiente proceso:

1. Para detener el equilibrio de carga de trabajo, vaya a la ficha **WLB** y haga clic en **Pausar**.
2. Cambie las credenciales de equilibrio de carga de trabajo ejecutando el comando `wlbconfig`. Para obtener más información, consulte Comandos de equilibrio de cargade trabajo
3. Vuelva a habilitar el equilibrio de carga de trabajo y especifique las nuevas credenciales
4. Cuando se complete la barra de progreso, haga clic en **Conectar**.

   Aparece el cuadro de diálogo **Conectarse al servidor WLB**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Haga clic en **Actualizar credenciales**.
6. En la sección **Dirección del servidor**, modifique la siguiente configuración según corresponda:

   - En el cuadro **Dirección**, escriba la dirección IP o FQDN del dispositivo del equilibrio de carga de trabajo.
   - (Opcional). Si cambió el número de puerto durante la configuración de equilibrio de carga de trabajo, introduzca ese número de puerto. El número de puerto que especifique en este cuadro y durante la configuración del equilibrio de carga de trabajo es el número de puerto que XenServer utiliza para conectarse al equilibrio de carga de trabajo.

     De forma predeterminada, XenServer se conecta al equilibrio de carga de trabajo en el puerto 8012.

     > **Nota:**
     >
     > Modifique este número de puerto solo si lo cambió cuando ejecutó el Asistente de configuración de equilibrio de carga de trabajo. El valor del número de puerto especificado al ejecutar el Asistente de configuración de equilibrio de carga de trabajo y el cuadro de diálogo Conectar al servidor WLB deben coincidir.

7. En la sección **Credenciales del servidor WLB**, introduzca el nombre de usuario (por ejemplo `wlbuser`) y la contraseña que utilizan los equipos que ejecutan XenServer para conectarse al servidor de equilibrio de carga de trabajo.
8. En la sección **Credenciales de Citrix Hypervisor**, introduzca el nombre de usuario y la contraseña del grupo que va a configurar (normalmente, la contraseña del coordinador del grupo). Workload Balancing usa estas credenciales para conectarse a los equipos que ejecutan XenServer en ese grupo.
9. En la sección **Credenciales de Citrix Hypervisor**, introduzca el nombre de usuario y la contraseña del grupo que está configurando. Workload Balancing usa estas credenciales para conectarse a los equipos que ejecutan XenServer en ese grupo.

   Para usar las credenciales con las que ha iniciado sesión actualmente en XenServer, seleccione **Usar las credenciales actuales de XenCenter**.

Cambio de la dirección IP de equilibrio de carga

Para cambiar la dirección IP de equilibrio de carga de trabajo, complete lo siguiente:

1. Para ver la dirección IP de equilibrio de carga de trabajo actual, ejecute el comando `ifconfig` en el dispositivo virtual.
2. Abra el archivo `/etc/sysconfig/network-scripts/ifcfg-eth0` con una herramienta de edición como vi.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Para cambiar el protocolo de dhcp a estático, cambie `BOOTPROTO=dhcp` a `BOOTPROTO=static`.
4. En la parte inferior del archivo, establece la dirección IP, la máscara de red, la puerta de enlace y las direcciones DNS. Por ejemplo:

```
IPADDR=192.168.1.100
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
DNS1=1.1.1.1
DNS2=8.8.8.8
<!--NeedCopy-->
```

> **Nota:**
>
> Agregue tantas entradas de DNS como necesite.

5. Guarde el archivo y ciérrelo.
6. Para que los cambios surtan efecto, debe reiniciar el sistema de red ejecutándolo `systemctl restart network`.
7. Una vez que se haya reiniciado el sistema de red, vuelva a ejecutar el comando `ifconfig` para ver la nueva dirección IP de equilibrio de carga de trabajo.
8. Para comprobar que el servicio de equilibrio de carga de trabajo se ejecuta con normalidad, ejecute el comando `systemctl status workloadbalancing`.

   Si el resultado devuelto contiene `Active: active (running)`, el servicio de equilibrio de carga de trabajo se ejecuta con normalidad. Si el resultado contiene `Active: inactive (dead)` o cualquier otro estado, el equilibrio de carga de trabajo podría cerrarse de forma anormal.

Cambiar la configuración del dispositivo virtual Equilibrio de carga

Cuando instala por primera vez el dispositivo virtual Equilibrio de carga de trabajo, tiene la siguiente configuración predeterminada:

Configuración	Valor
Cantidad de vCPU	2
Memoria (RAM)	2 GB
Espacio en disco	30 GB

Estos valores son adecuados para la mayoría de los entornos. Si supervisa grupos muy grandes, puede considerar aumentar estos valores.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cambiar la cantidad de CPU virtuales asignadas al dispositivo virtual

De forma predeterminada, al dispositivo virtual de Workload Balancing se le asignan 2 vCPU. Este valor es suficiente para grupos que alojan 1000 VM. Por lo general, no es necesario aumentarlo. Reduzca la cantidad de CPU virtuales asignadas al dispositivo virtual solo si tiene un entorno pequeño.

En este procedimiento se explica cómo cambiar la cantidad de CPU virtuales asignadas al dispositivo virtual Equilibrio de carga de trabajo. Apague el dispositivo virtual antes de llevar a cabo estos pasos. El equilibrio de carga de trabajo no está disponible durante aproximadamente cinco minutos.

1. Cierre el dispositivo virtual Equilibrio de carga de trabajo.
2. En el panel de recursos de XenCenter, seleccione el dispositivo virtual Equilibrio de carga de trabajo.
3. En la ficha **General** del dispositivo virtual, haga clic en **Propiedades**. Se abre el cuadro de diálogo **Propiedades**.
4. En la ficha **CPU** del cuadro de diálogo **Propiedades**, modifique la configuración de la CPU a los valores requeridos.
5. Haga clic en **Aceptar**.
6. Inicie el dispositivo virtual de equilibrio de carga de trabajo.

La nueva configuración de vCPU se aplica cuando se inicia el dispositivo virtual.

Cambiar el tamaño de la memoria del dispositivo virtual

De forma predeterminada, al dispositivo virtual Equilibrio de carga de trabajo se le asignan 2 GB de memoria.

Para grupos grandes, configure el dispositivo virtual Equilibrio de carga de trabajo para que consuma la cantidad máxima de memoria que puede poner a su disposición (incluso hasta 16 GB). No se preocupe por la alta utilización de la memoria. La utilización elevada de la memoria es normal para el dispositivo virtual porque la base de datos siempre consume la mayor cantidad de memoria que puede obtener.

> **Nota:**
>
> El dispositivo virtual Equilibrio de carga de trabajo no admite el control de memoria dinámica. Establezca un valor fijo para la memoria máxima que se asignará al dispositivo virtual.

En este procedimiento se explica cómo cambiar el tamaño de la memoria del dispositivo virtual Equilibrio de carga de trabajo. Apague el dispositivo virtual antes de llevar a cabo estos pasos. El equilibrio de carga de trabajo no está disponible durante aproximadamente cinco minutos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Cierre el dispositivo virtual Equilibrio de carga de trabajo.
2. En el panel de recursos de XenCenter, seleccione el dispositivo virtual Equilibrio de carga de trabajo.
3. En la ficha **Memoria** del dispositivo virtual, haga clic en **Modificar**. Se abre el diálogo **Configuración de memoria**.
4. Modifique la configuración de la memoria a los valores requeridos.
5. Haga clic en **Aceptar**.
6. Inicie el dispositivo virtual de equilibrio de carga de trabajo.

La nueva configuración de memoria se aplica cuando se inicia el dispositivo virtual.

Amplíe el disco del dispositivo virtual

> **Advertencia:**
>
> Solo puede ampliar el espacio en disco disponible en las versiones 8.3.0 y posteriores, ya que LVM no es compatible con versiones anteriores a la 8.3.0.
>
> El equilibrio de carga de trabajo no permite reducir el espacio disponible en disco.

De forma predeterminada, al dispositivo virtual Equilibrio de carga de trabajo se le asignan 30 GB de espacio en disco.

Cuanto mayor sea la cantidad de máquinas virtuales que supervisa el dispositivo virtual Equilibrio de carga de trabajo, más espacio en disco consume por día.

Puede estimar la cantidad de tamaño de disco que necesita el dispositivo virtual mediante la siguiente fórmula:

```
Total estimated disk size = ( ( number of days * average disk usage ) +
    base disk usage ) * grooming multiplier
```

- *número de días* es el número de días de datos que se deben conservar
- El *uso promedio del disco* depende de la cantidad de VM que se supervisan. Los siguientes valores proporcionan una aproximación para ciertos números de máquinas virtuales:
  - Para 200 VM: 0,246 GB/día
  - Para 400 VM: 0,505 GB/día
  - Para 600 VM: 0,724 GB/día
  - Para 800 VM: 0,887 GB/día
- el*uso del disco base* es de 2,4 GB

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- El*multiplicador de aseo* es de 1,25. Este multiplicador explica la cantidad de espacio en disco requerido por la limpieza. Se supone que la limpieza requiere un 25% adicional del espacio total en disco calculado.

Para las versiones 8.2.2 y anteriores Este procedimiento explica cómo extender el disco virtual del dispositivo virtual de Workload Balancing para las versiones 8.2.2 y anteriores.

> **Advertencia:**
>
> Recomendamos tomar una instantánea de sus datos antes de realizar este procedimiento. La ejecución incorrecta de estos pasos puede provocar la corrupción del dispositivo virtual Equilibrio de carga de trabajo.

1. Cierre el dispositivo virtual Equilibrio de carga de trabajo.
2. En el panel de recursos de XenCenter, seleccione el dispositivo virtual Equilibrio de carga de trabajo.
3. Haga clic en la ficha **Almacenamiento**.
4. Seleccione el disco `vdi_xvda` y haga clic en el botón **Propiedades**.
5. En el cuadro de diálogo `vdi_xvda` **Propiedades**, seleccione **Tamaño y ubicación**.
6. Aumente el tamaño del disco según sea necesario y haga clic en **Aceptar**.
7. Inicie el dispositivo virtual Equilibrio de carga de trabajo e inicie sesión en él.
8. Ejecute el siguiente comando en el dispositivo virtual Equilibrio de carga de trabajo:

```
resize2fs /dev/xvda
<!--NeedCopy-->
```

9. Ejecute el comando `df –h` para confirmar el nuevo tamaño del disco.

Instalación `resize2fs` Si la herramienta `resize2fs` no está instalada en el dispositivo virtual Equilibrio de carga de trabajo, puede instalarla mediante los siguientes pasos.

Si está conectado a Internet, ejecute el siguiente comando en el dispositivo virtual Equilibrio de carga de trabajo:

```
yum install -y --enablerepo=base,updates --disablerepo=citrix-*
   e2fsprogs
<!--NeedCopy-->
```

Si no hay acceso a internet:

1. Descargue lo siguiente desde https://centos.pkgs.org/7/centos-x86_64/.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- libss-1.42.9-7.el7.i686.rpm
- e2fsprogs-libs-1.42.9-7.el7.x86_64.rpm
- e2fsprogs-1.42.9-7.el7.x86_64.rpm

2. Cárguelos en Workload Balancing VM mediante SCP o cualquier otra herramienta adecuada.
3. Ejecute el siguiente comando desde el dispositivo virtual Workload Balancing:

```
rpm -ivh libss-\*.rpm e2fsprogs-\*.rpm
<!--NeedCopy-->
```

La herramienta `resize2fs` ya está instalada.

Para las versiones 8.3.0 y posteriores Este procedimiento explica cómo extender el disco virtual del dispositivo virtual de equilibrio de carga de trabajo para las versiones 8.3.0 y posteriores de Workload Balancing, mediante Linux Volume Manager (LVM).

> **Advertencia:**
>
> Este procedimiento solo lo deben seguir los administradores de sistemas Linux con experiencia, ya que si se realizan estos pasos de forma incorrecta, se puede dañar el dispositivo virtual de equilibrio de carga de trabajo. No podemos garantizar que se puedan resolver los problemas derivados del uso incorrecto del Editor del Registro. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo y de apagar el dispositivo virtual antes de realizar estos pasos. El equilibrio de carga de trabajo no está disponible durante aproximadamente cinco minutos.

Para crear nuevas particiones, manipular volúmenes físicos y cambiar el tamaño del sistema de archivos, realice las siguientes acciones con la sesión iniciada como superusuario (root):

1. Vea las particiones actuales:

```
fdisk -l
<!--NeedCopy-->
```

Las particiones predeterminadas podrían tener este aspecto:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
-bash-4.2# fdisk -l

Disk /dev/xvda: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000008b2

   Device Boot      Start         End      Blocks   Id  System
/dev/xvda1   *        2048     1026047      512000   83  Linux
/dev/xvda2         1026048    16777215     7875584   8e  Linux LVM

Disk /dev/mapper/centos-root: 7159 MB, 7159676928 bytes, 13983744 sectors
Units = sectors of 1 * 512 = 512 bytes
```

2. Vea el estilo de partición del disco:

```
parted <disk>
<!--NeedCopy-->
```

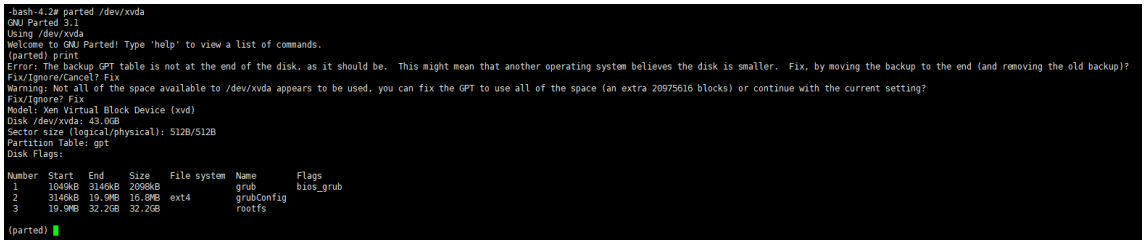
   Por ejemplo, para ver el estilo de partición de `/dev/xvda`:

```
parted /dev/xvda
<!--NeedCopy-->
```

3. Escriba `p`.

   Si aparecen los siguientes mensajes de error, introduzca `Fix` para resolver cada uno de ellos:

   - "Error: la tabla GPT de respaldo no está al final del disco, como debería estar. Esto puede significar que otro sistema operativo cree que el disco es más pequeño. ¿Arreglar, moviendo la copia de seguridad hasta el final (y quitando la copia de seguridad anterior)?"
   - "Advertencia: No parece que se esté utilizando todo el espacio disponible de <disk>. ¿Puede arreglar el GPT para usar todo el espacio (<block number> bloques adicionales) o continuar con la configuración actual?"



4. Introduzca `q` y presione **Entrar** para salir de parted.

5. Modifique las particiones:

```
fdisk <disk>
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Por ejemplo, para modificar las particiones en los dispositivos de equilibrio de carga de trabajo:

```
fdisk /dev/xvda
<!--NeedCopy-->
```

6. Escriba `n` y presione **Entrar** para crear una nueva partición, escriba `p` y presione **Entrar** para convertirla en una partición primaria y presione **Entrar** para usar la partición predeterminada, que es la siguiente partición disponible (en este caso, como se indicó anteriormente, será la partición número 3).

   > **Nota:**
   >
   > Si aún no se ha asignado ningún espacio adicional, aparecerá un mensaje que indica que no hay sectores libres disponibles. Escriba `q` y presione **Entrar** para salir de fdisk. Asigne primero el espacio deseado a través de XenCenter y, a continuación, vuelva a este paso.

7. Presione **Entrar** dos veces para utilizar el primer y el último sector predeterminados de la partición disponible (o indicar manualmente los sectores deseados). Escriba `t` para especificar un tipo de partición, elija la partición deseada (en este caso, 3) `8e`, escriba y presione **Entrar** para convertirla en una partición de tipo LVM.

   Ejemplo de salida:

   ```
   Command (m for help): n
   Partition type:
      p   primary (2 primary, 0 extended, 2 free)
      e   extended
   Select (default p): p
   Partition number (3,4, default 3):
   First sector (16777216-41943039, default 16777216):
   Using default value 16777216
   Last sector, +sectors or +size{K,M,G} (16777216-41943039, default 41943039):
   Using default value 41943039
   Partition 3 of type Linux and of size 12 GiB is set

   Command (m for help): t
   Partition number (1-3, default 3):
   Hex code (type L to list all codes): 8e
   Changed type of partition 'Linux' to 'Linux LVM'
   ```

8. Escriba `p` y presione **Entrar** para imprimir los detalles de la partición. El resultado debería ser similar al siguiente (ten en cuenta que los valores de los bloques inicial y final pueden variar según la cantidad de espacio que hayas asignado):

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
Command (m for help): p

Disk /dev/xvda: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000008b2

   Device Boot      Start         End      Blocks   Id  System
/dev/xvda1   *        2048     1026047      512000   83  Linux
/dev/xvda2         1026048    16777215     7875584   8e  Linux LVM
/dev/xvda3        16777216    41943039    12582912   8e  Linux LVM
```

9. Si algo es incorrecto, escriba `q` y presione **Entrar** para salir sin guardar y evitar que las particiones existentes se vean afectadas. Vuelva a empezar desde el paso 1. De lo contrario, si todo se ve bien, escriba `w` y presione **Entrar** para escribir los cambios.

   Después de escribir estos cambios, es posible que reciba una advertencia que indique que el dispositivo estaba ocupado y que el núcleo sigue utilizando la tabla anterior. Si ese es el caso, ejecute este comando que actualizará la tabla de particiones antes de continuar con el siguiente paso: `partprobe`.

   Asegúrese de que la nueva partición del dispositivo (en este caso `/dev/xvda4`) aparezca ahora en la lista. Para ello, ejecute: `fdisk -l`.

   El dispositivo recién creado debería aparecer ahora en la lista:

```
   Device Boot      Start         End      Blocks   Id  System
/dev/xvda1   *        2048     1026047      512000   83  Linux
/dev/xvda2         1026048    16777215     7875584   8e  Linux LVM
/dev/xvda3        16777216    41943039    12582912   8e  Linux LVM
```

10. Si la salida parece correcta, cree un volumen físico:

```
pvcreate <new partition>
<!--NeedCopy-->
```

    Por ejemplo:

```
pvcreate /dev/xvda4
<!--NeedCopy-->
```

11. Compruebe que el volumen físico creado anteriormente aparezca ahora en la lista:

```
pvs
<!--NeedCopy-->
```

    En este ejemplo, el espacio adicional agregado fue de 12G. Ejemplo de salida:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
-bash-4.2# pvcreate /dev/xvda3
  Physical volume "/dev/xvda3" successfully created.
-bash-4.2# pvs
  PV         VG     Fmt  Attr PSize  PFree
  /dev/xvda2 centos lvm2 a--  <7.51g 40.00m
  /dev/xvda3        lvm2 ---  12.00g 12.00g
```

12. Según el resultado del comando anterior, se debe ampliar el grupo de volúmenes denominado centos:

```
vgextend <volume group> <new partition>
<!--NeedCopy-->
```

Por ejemplo:

```
vgextend centos /dev/xvda4
<!--NeedCopy-->
```

13. Compruebe los grupos de volúmenes actuales:

```
vgs
<!--NeedCopy-->
```

14. Ejecute este comando:

```
pvscan
<!--NeedCopy-->
```

Esto debería mostrarse `/dev/xvda4` como parte del grupo de volúmenes de centos. Ejemplo de salida:

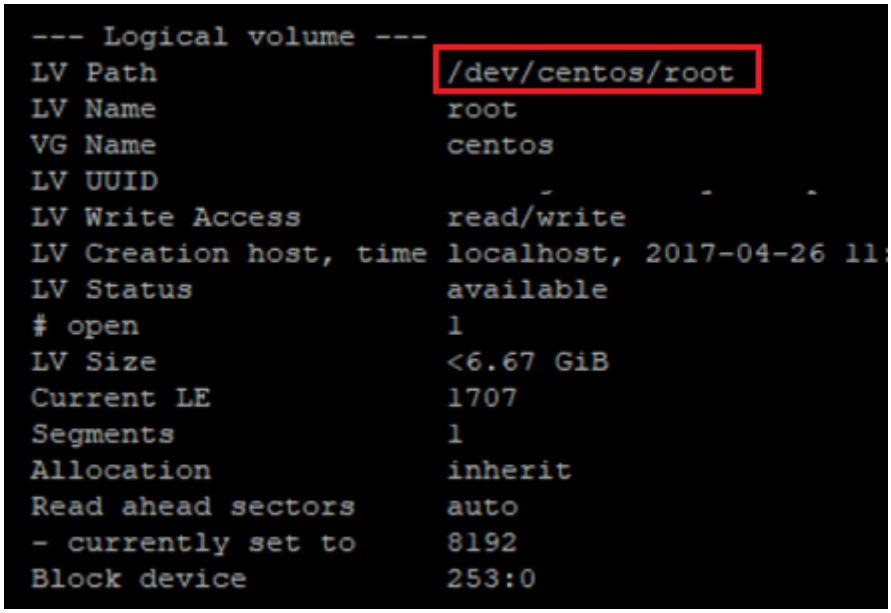
```
-bash-4.2# vgextend centos /dev/xvda3
  Volume group "centos" successfully extended
-bash-4.2# vgs
  VG     #PV #LV #SN Attr   VSize  VFree
  centos   2   2   0 wz--n- 19.50g <12.04g
-bash-4.2# pvscan
  PV /dev/xvda2   VG centos          lvm2 [<7.51 GiB / 40.00 MiB free]
  PV /dev/xvda3   VG centos          lvm2 [<12.00 GiB / <12.00 GiB free]
  Total: 2 [19.50 GiB] / in use: 2 [19.50 GiB] / in no VG: 0 [0   ]
```

15. Si la información que se muestra en los pasos anteriores parece correcta, ejecute este comando para ver la ruta del volumen lógico para ampliar el volumen lógico:

```
lvdisplay
<!--NeedCopy-->
```

En este ejemplo, la ruta es `/dev/centos/root`:

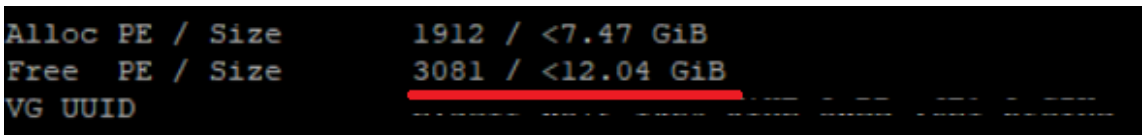
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



16. Ejecute el siguiente comando para ver el PE/Size libre (esto indica el valor exacto que se debe utilizar al extender la partición):

```
vgdisplay
<!--NeedCopy-->
```

Ejemplo de salida:



17. Utilizando el valor PE/Size libre y la ruta del volumen lógico que se muestra en el paso 11, amplíe el volumen lógico:

```
lvextend -l +100%FREE /dev/centos/root
<!--NeedCopy-->
```

Si esto se ejecuta correctamente, amplíe el sistema de archivos:

```
resize2fs /dev/centos/root
<!--NeedCopy-->
```

Ejemplo de salida:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
-bash-4.2# lvextend -l +3081 /dev/centos/root
  Size of logical volume centos/root changed from <6.67 GiB (1707 extents) to 18
.70 GiB (4788 extents).
  Logical volume centos/root successfully resized.
-bash-4.2# xfs_growfs /dev/centos/root
meta-data=/dev/mapper/centos-root isize=256    agcount=4, agsize=436992 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=0        finobt=0 spinodes=0
data     =                       bsize=4096   blocks=1747968, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal               bsize=4096   blocks=2560, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
data blocks changed from 1747968 to 4902912
```

18. Compruebe que el tamaño del sistema de archivos sea el esperado:

```
1 df -h /*
2 <!--NeedCopy-->
```

```
-bash-4.2# df -h /*
Filesystem               Size  Used Avail Use% Mounted on
/dev/mapper/centos-root   19G  4.1G   15G  22% /
/dev/xvda1               497M  111M  387M  23% /boot
devtmpfs                 990M     0  990M   0% /dev
```

Si ves los números esperados, significa que has asignado correctamente el espacio deseado y has extendido la partición correctamente. Para obtener más ayuda, póngase en contacto con el soporte de XenServer.

Detener equilibrio de carga

Como el equilibrio de carga de trabajo se configura en el nivel de grupo, cuando quiera que deje de administrar un grupo, debe realizar una de las siguientes acciones:

Poner en**pausa el equilibrio de carga** La pausa del equilibrio de carga de trabajo impide que XenCenter muestre recomendaciones para el grupo de recursos especificado y administre el grupo. La pausa está diseñada para un período breve y le permite reanudar la supervisión sin tener que volver a configurar. Al pausar Equilibrio de carga de trabajo, la recopilación de datos se detiene para esa agrupación de recursos hasta que vuelva a habilitar Equilibrio de carga de trabajo.

1. En XenCenter, seleccione el grupo de recursos para el que quiere inhabilitar el equilibrio de carga de trabajo.
2. En la ficha **WLB**, haga clic en **Pausar**. Aparece un mensaje en la ficha **WLB** que indica que el equilibrio de carga de trabajo está en pausa.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Sugerencia:**
>
> Para reanudar la supervisión, haga clic en el botón **Reanudar** en la ficha **WLB**.

Desconecte el grupo del equilibrio de carga de trabajo. La desconexión del dispositivo virtual Equilibrio de carga de trabajo interrumpe la conexión entre el grupo y, si es posible, elimina los datos del grupo de la base de datos de equilibrio de carga de trabajo. Cuando se desconecta del equilibrio de carga de trabajo, el equilibrio de carga de trabajo deja de recopilar datos del grupo.

1. En XenCenter, seleccione el grupo de recursos en el que quiere detener el equilibrio de carga de trabajo.
2. En el menú **Infraestructura**, seleccione **Desconectar servidor de equilibrio de carga**de trabajo. Aparece el cuadro de diálogo **Desconectar el servidor el equilibrio de carga de trabajo**.
3. Haga clic en **Desconectar** para detener el equilibrio de carga de trabajo de supervisar el grupo permanentemente

> **Sugerencia:**
>
> Si desconectó el grupo del dispositivo virtual Equilibrio de carga de trabajo, para volver a habilitar el equilibrio de carga de trabajo en ese grupo, debe volver a conectarse a un dispositivo de equilibrio de carga de trabajo. Para obtener información, consulte Conectarse al dispositivo virtual de equilibrio de cargade trabajo.

Entre en el modo de mantenimiento con el equilibrio de carga

Con el equilibrio de carga de trabajo habilitado, si coloca un host en modo de mantenimiento, XenServer migra las máquinas virtuales que se ejecutan en ese host a sus hosts óptimos cuando estén disponibles. XenServer utiliza las recomendaciones de equilibrio de carga de trabajo que se basan en los datos de rendimiento, la estrategia de ubicación y los umbrales de rendimiento para seleccionar el host óptimo.

Si no hay un host óptimo disponible, aparecen las palabras **Haga clic aquí para suspender la máquina virtual** en el asistente **Entrar en el modo de mantenimiento**. En este caso, dado que no hay un host con recursos suficientes para ejecutar la máquina virtual, Workload Balancing no recomienda una ubicación. Puede suspender esta máquina virtual o salir del modo de mantenimiento y suspender una máquina virtual en otro host del mismo grupo. A continuación, si vuelve a entrar en el cuadro de diálogo **Entrar en modo de mantenimiento**, es posible que Equilibrio de carga de trabajo pueda mostrar un host que sea candidato adecuado para la migración.

> **Nota:**
>
> Cuando se desconecta un host por mantenimiento y se habilita el equilibrio de carga de trabajo,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> aparecen las palabras “Equilibrio de carga de trabajo”en el asistente de **entrada al modo de mantenimiento** .

Para entrar en el modo de mantenimiento con el equilibrio de carga de trabajo habilitado:

1. En el panel **Recursos** de XenCenter, seleccione el servidor físico que quiere desconectar.
2. En el menú **Servidor**, seleccione **Entrar en modo de mantenimiento**.
3. En el asistente **Entrar en modo de mantenimiento**, haga clic en **Entrar en modo de mantenimiento**.

   Las máquinas virtuales que se ejecutan en el host se migran automáticamente al host óptimo en función de los datos de rendimiento de Workload Balancing, su estrategia de ubicación y los umbrales de rendimiento.

Para sacar el servidor del modo de mantenimiento:

1. Haga clic con el botón derecho en el anfitrión y seleccione **Salir del modo de mantenimiento**.

   Al eliminar un host del modo de mantenimiento, XenServer restaura automáticamente las máquinas virtuales originales de ese host en ese host.

Eliminar el dispositivo virtual Equilibrio de carga

Para quitar el dispositivo virtual Equilibrio de carga de trabajo, le recomendamos que utilice el procedimiento estándar para eliminar las máquinas virtuales de XenCenter.

Cuando elimina el dispositivo virtual Equilibrio de carga de trabajo, se elimina la base de datos PostgreSQL que contiene el equilibrio de carga de trabajo. Para guardar estos datos, debe migrarlos de la base de datos antes de eliminar el dispositivo virtual Equilibrio de carga de trabajo.

Administrar la base de datos de equilibrio de carga de trabajo

La base de datos de equilibrio de carga de trabajo es una base de datos de PostgreSQL. PostgreSQL es una base de datos relacional de código abierto. Puede encontrar documentación para PostgreSQL buscando en la web.

La siguiente información está dirigida a administradores de bases de datos y usuarios avanzados de PostgreSQL que se sienten cómodos con las tareas de administración de bases de datos. Si no tiene experiencia con PostgreSQL, le recomendamos que se familiarice con él antes de intentar las tareas de la base de datos en las secciones siguientes.

De forma predeterminada, el nombre de usuario de PostgreSQL es `postgres`. Establezca la contraseña para esta cuenta durante la configuración del equilibrio de carga de trabajo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La cantidad de datos históricos que puede almacenar se basa en el tamaño del disco virtual asignado a Equilibrio de carga de trabajo y en el espacio mínimo requerido. De forma predeterminada, el tamaño del disco virtual asignado a Equilibrio de carga de trabajo es de 30 GB. En términos de administración de la base de datos, puede controlar el espacio que consumen los datos de la base de datos configurando la limpieza de la base de datos. Para obtener más información, consulte Parámetros de limpieza de basesde datos.

Para almacenar una gran cantidad de datos históricos, por ejemplo, si quiere habilitar el Informe de pista de auditoría de grupo, puede realizar una de las siguientes acciones:

- Aumentar el tamaño del disco vDisk asignado al dispositivo virtual Equilibrio de carga de trabajo. Para ello, importe el dispositivo virtual y aumente el tamaño del disco virtual siguiendo los pasos de Extender el disco del dispositivo virtual.
- Cree copias de seguridad duplicadas periódicas de los datos habilitando el acceso remoto del cliente a la base de datos y mediante una herramienta de administración de bases de datos de terceros.

Acceder a la base

El dispositivo virtual Equilibrio de carga de trabajo tiene configurado un firewall. Antes de poder acceder a la base de datos, debe agregar el puerto del servidor postgreSQL a iptables.

1. En la consola del dispositivo virtual Equilibrio de carga de trabajo, ejecute el siguiente comando:

```
iptables -A INPUT -i eth0 -p tcp -m tcp --dport 5432 -m \
state --state NEW,ESTABLISHED -j ACCEPT
<!--NeedCopy-->
```

2. (Opcional) Para que esta configuración se mantenga después de reiniciar el dispositivo virtual, ejecute el siguiente comando:

```
iptables-save > /etc/sysconfig/potables
<!--NeedCopy-->
```

Controlar el aseo de las bases

La base de datos de equilibrio de carga de trabajo elimina automáticamente los datos más antiguos siempre que el dispositivo virtual alcanza la cantidad mínima de espacio en disco que el equilibrio de carga de trabajo requiere para ejecutarse. De forma predeterminada, la cantidad mínima de espacio en disco requerido se establece en 1024 MB.

Las opciones de limpieza de la base de datos de Equilibrio de carga de trabajo se controlan `wlb.conf`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cuando no queda suficiente espacio en disco en el dispositivo virtual Equilibrio de carga de trabajo, el equilibrio de carga de trabajo comienza a limpiar automáticamente los datos históricos. El proceso es el siguiente:

1. En un intervalo de limpieza predefinido, el recopilador de datos Equilibrio de carga de trabajo comprueba si se requiere limpieza. La limpieza es necesaria si los datos de la base de datos han crecido hasta el punto en que el único espacio que permanece sin usar es el espacio en disco mínimo requerido. Use `GroomingRequiredMinimumDiskSizeInMB` para establecer el espacio en disco mínimo requerido.

   Puede cambiar el intervalo de aseo si quiere con `GroomingIntervalInHour`. Sin embargo, de forma predeterminada, el equilibrio de carga de trabajo comprueba si se requiere limpieza una vez por hora.

2. Si se requiere limpieza, Equilibrio de carga de trabajo comienza con la limpieza de los datos del día más antiguo. A continuación, Equilibrio de carga de trabajo comprueba si hay suficiente espacio en disco para cumplir con el requisito mínimo de espacio en disco.

3. Si la primera limpieza no liberó suficiente espacio en disco, Equilibrio de carga de trabajo repite la limpieza hasta las veces indicadas en `GroomingRetryCounter` sin esperar las horas indicadas en `GroomingIntervalInHour`.

4. Si la primera limpieza o la limpieza repetida liberaron suficiente espacio en disco, Equilibrio de carga de trabajo espera las horas indicadas en `GroomingIntervalInHour` y vuelve al paso 1.

5. Si la limpieza iniciada por `GroomingRetryCounter` no liberó suficiente espacio en disco, el equilibrio de carga de trabajo espera las horas indicadas en `GroomingIntervalInHour` y vuelve al paso 1.

Parámetros de limpieza de bases de datos

Hay cinco parámetros en el archivo `wlb.conf` que controlan varios aspectos de la limpieza de la base de datos. Son las siguientes:

- `GroomingIntervalInHour`. Controla el número de horas que transcurren antes de que se realice la siguiente revisión de aseo. Por ejemplo, si introduce **1**, Equilibrio de carga de trabajo comprueba el espacio en disco cada hora. Si introduce **2**, Equilibrio de carga de trabajo verifica el espacio en disco cada dos horas para determinar si debe producirse una limpieza.
- `GroomingRetryCounter`. Controla el número de veces que Equilibrio de carga de trabajo intenta volver a ejecutar la consulta de la base de datos
- `GroomingDBDataTrimDays`. Controla el número de días de datos que Equilibrio de carga

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de trabajo elimina de la base de datos cada vez que intenta arreglar los datos. El valor predeterminado es de un día.

- `GroomingDBTimeoutInMinute`. Controla el número de minutos que tarda la limpieza de la base de datos antes de que se agote y se cancele. Si la consulta de limpieza tarda más de lo esperado y no termina de ejecutarse dentro del período de tiempo de espera, la tarea de limpieza se cancela. El valor predeterminado es 0 minutos, lo que significa que la limpieza de la base de datos nunca se agota.
- `GroomingRequiredMinimumDiskSizeInMB`. Controla la cantidad mínima de espacio libre que queda en el disco virtual asignado al dispositivo virtual Equilibrio de carga de trabajo. Cuando los datos del disco virtual crecen hasta que solo queda un tamaño de disco mínimo en el disco virtual, el equilibrio de carga de trabajo desencadena la limpieza de la base de datos. El valor predeterminado es 2,048 MB.

Para modificar estos valores, consulte Modificar el archivo de configuración de equilibrio de cargade trabajo.

Cambiar la contraseña de base de datos

Se recomienda utilizar el comando `wlbconfig` para cambiar la contraseña de la base de datos. Para obtener más información, consulte Modificar las opciones de configuración del equilibrio de cargade trabajo No cambie la contraseña modificando el archivo`wlb.conf`.

Archivar datos de bases

Para evitar que se eliminen datos históricos más antiguos, puede copiar datos de la base de datos para archivarlos. Para hacerlo, debe realizar las siguientes tareas:

1. Active la autenticación de clientes en la base de datos.
2. Configure el archivado con la herramienta de administración de bases de datos PostgreSQL de su elección.

Habilitar la autenticación de clientes en la base

Si bien puede conectarse directamente a la base de datos a través de la consola Equilibrio de carga de trabajo, también puede usar una herramienta de administración de base de datos PostgreSQL. Después de descargar una herramienta de administración de bases de datos, instálela en el sistema desde el que quiere conectarse a la base de datos. Por ejemplo, puede instalar la herramienta en el mismo equipo portátil en el que ejecuta XenCenter.

Antes de poder habilitar la autenticación de clientes remotos en la base de datos, debe:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Modifique los archivos de configuración de la base de datos, incluidos el archivo pg_hba.conf y postgresql.conf, para permitir las conexiones.
2. Detenga los servicios de equilibrio de carga de trabajo, reinicie la base de datos y, a continuación, reinicie los servicios
3. En la herramienta de administración de bases de datos, configure la dirección IP de la base de datos (es decir, la dirección IP del dispositivo virtual de equilibrio de carga de trabajo) y la contraseña de la base de datos.

Modificar los archivos de configuración de base

Para habilitar la autenticación de clientes en la base de datos, debe modificar los siguientes archivos en el dispositivo virtual Equilibrio de carga de trabajo: el archivo `pg_hba.conf` y el archivo `postgresql.conf`.

Para modificar el archivo `pg_hba.conf`:

1. Modifica el archivo `pg_hba.conf`. En la consola del dispositivo virtual Equilibrio de carga de trabajo, abra el archivo `pg_hba.conf` con un editor, como VI. Por ejemplo:

```
vi /var/lib/pgsql/9.0/data/pg_hba.conf
<!--NeedCopy-->
```

2. Si su red usa IPv4, agregue la dirección IP del equipo que se conecta a este archivo. Por ejemplo:

   En la sección de configuración, introduzca lo siguiente en `#IPv4 local connections`:

   - **TYPE:** host
   - **DATABASE:** all
   - **USER:** all
   - **CIDR-ADDRESS:** 0.0.0.0/0
   - **METHOD:** trust

3. Introduzca su dirección IP en el campo `CIDR-ADDRESS`.

   > **Nota:**
   >
   > En lugar de introducir 0.0.0.0/0, puede introducir su dirección IP y reemplazar los últimos tres dígitos por 0/24. El "24"posterior a / define la máscara de subred y solo permite conexiones desde direcciones IP dentro de esa máscara de subred.

   Cuando se introduce `trust` para el campo `Method`, permite que la conexión se autentique sin necesidad de una contraseña. Si introduce `password` para el campo `Method`, debe proporcionar una contraseña al conectarse a la base de datos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Si su red usa IPv6, agregue la dirección IP del equipo que se conecta a este archivo. Por ejemplo:

   Introduzca lo siguiente en `#IPv6 local connections`:

   - **TYPE:** host
   - **DATABASE:** all
   - **USER:** all
   - **CIDR-ADDRESS:** `::0/0`
   - **METHOD:** trust

   Introduzca las direcciones IPv6 en el campo `CIDR-ADDRESS`. En este ejemplo, `::0/0` abre la base de datos hasta las conexiones desde cualquier dirección IPv6.

5. Guarde el archivo y salga del editor.

6. Después de cambiar cualquier configuración de base de datos, debe reiniciar la base de datos para aplicar los cambios. Ejecute este comando:

```
service postgresql-9.0 restart
<!--NeedCopy-->
```

Para modificar el archivo `postgresql.conf`:

1. Modifica el archivo `postgresql.conf`. En la consola del dispositivo virtual Equilibrio de carga de trabajo, abra el archivo `postgresql.conf` con un editor, como VI. Por ejemplo:

```
vi /var/lib/pgsql/9.0/data/postgresql.conf
<!--NeedCopy-->
```

2. Modifique el archivo para que escuche en cualquier puerto y no solo en el host local. Por ejemplo:

   a) Busque la siguiente línea:

```
# listen_addresses='localhost'
<!--NeedCopy-->
```

   b) Quite el símbolo de comentario (#) y modifique la línea para que diga lo siguiente:

```
listen_addresses='*'
<!--NeedCopy-->
```

3. Guarde el archivo y salga del editor.

4. Después de cambiar cualquier configuración de base de datos, debe reiniciar la base de datos para aplicar los cambios. Ejecute este comando:

```
service postgresql-9.0 restart
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cambiar la ventana de mantenimiento de la base

Equilibrio de carga de trabajo realiza automáticamente el mantenimiento rutinario de la base de datos a las 12:05 a. m. GMT (00:05) Durante este período de mantenimiento, se produce la recopilación de datos, pero el registro de datos puede retrasarse. Sin embargo, los controles de la interfaz de usuario de Equilibrio de carga de trabajo están disponibles durante este período y Equilibrio de carga de trabajo

> **Nota:**
>
> Para evitar una pérdida de equilibrio de carga de trabajo:
>
> - Durante el período de mantenimiento, el servidor de equilibrio de carga de trabajo se reinicia. Asegúrese de no reiniciar las máquinas virtuales al mismo tiempo.
> - En otras ocasiones, al reiniciar todas las máquinas virtuales del grupo, no reinicie el servidor de equilibrio de carga de trabajo.

El mantenimiento de la base de datos incluye liberar el espacio en disco no utilizado asignado y reindexar la base El mantenimiento dura aproximadamente de 6 a 8 minutos. En grupos más grandes, el mantenimiento puede durar más, según el tiempo que tarde Equilibrio de carga de trabajo en realizar la detección.

Dependiendo de su zona horaria, es posible que quiera cambiar la hora en que se produce el mantenimiento. Por ejemplo, en la zona horaria de la hora estándar de Japón (JST), el mantenimiento del equilibrio de carga de trabajo se produce a las 9:05 a.m. (09:05), lo que puede entrar en conflicto con el uso máximo en algunas organizaciones. Si quiere especificar un cambio de horario estacional, como el horario de verano o el horario de verano, debe incluir el cambio en el valor que introduzca.

Para cambiar el tiempo de mantenimiento:

1. En la consola Equilibrio de carga de trabajo, ejecute el siguiente comando desde cualquier directorio:

   ```
   crontab -e
   <!--NeedCopy-->
   ```

   El equilibrio de carga de trabajo muestra lo siguiente

   ```
   05 0 * * * /opt/vpx/wlb/wlbmaintenance.sh
   <!--NeedCopy-->
   ```

   El valor `05 0` representa el tiempo predeterminado para que Equilibrio de carga de trabajo realice el mantenimiento en minutos (05) y, a continuación, en horas (0). (Los asteriscos representan el día, el mes y el año en que se ejecuta la tarea; no modifique estos campos). La entrada `05 0` indica que el mantenimiento de la base de datos se realiza a las 12:05 AM, o a las 00:05, hora del meridiano de Greenwich (GMT) todas las noches. Esta configuración significa que si

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

vives en Nueva York, el mantenimiento se ejecuta a las 7:05 p.m. (19:05) durante los meses de invierno y a las 8:05 p.m. en los meses de verano.

> **Importante:**
>
> No modifique el día, el mes y el año en que se ejecuta la tarea (representados por asteriscos). El mantenimiento de la base de datos debe realizarse

2. Introduzca la hora a la que quiere que se realice el mantenimiento en GMT.
3. Guarde el archivo y salga del editor.

Personalizar equilibrio de carga

El equilibrio de carga de trabajo proporciona varios métodos de personalización:

- **Líneas de comando para scripts**. Para obtener más información, consulte Comandos de equilibrio de cargade trabajo
- **Compatibilidad con scripts de encendido del host**. También puede personalizar Equilibrio de carga de trabajo (indirectamente) mediante scripts de encendido del host. Para obtener más información, consulte Hosts y grupos de recursos.

Actualización del equilibrio de carga

La actualización en línea del equilibrio de carga de trabajo ha quedado obsoleta por motivos de seguridad. Los clientes ya no pueden actualizar usando el repositorio de yum. Los clientes pueden actualizar Workload Balancing a la versión más reciente importando el último dispositivo virtual de Workload Balancing que se puede descargar en la página de descargas de XenServer.

Comandos de Equilibrio de carga de trabajo

En esta sección se proporciona una referencia para los comandos de equilibrio de carga de trabajo. Puede ejecutar estos comandos desde el host o la consola de XenServer para controlar el equilibrio de carga de trabajo o configurar los ajustes de equilibrio de carga de trabajo en el host de XenServer. Este apéndice incluye comandos xe y comandos de servicio.

Ejecute los siguientes comandos de servicio en el dispositivo de equilibrio de carga de trabajo. Para hacerlo, debe iniciar sesión en el dispositivo virtual Equilibrio de carga de trabajo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Inicie sesión en el dispositivo virtual de equilibrio de carga de trabajo

Antes de poder ejecutar cualquier comando de servicio o modificar el archivo `wlb.conf`, debe iniciar sesión en el dispositivo virtual Equilibrio de carga de trabajo. Para hacerlo, debe introducir un nombre de usuario y una contraseña. A menos que haya creado cuentas de usuario adicionales en el dispositivo virtual, inicie sesión con la cuenta de usuario raíz. Especificó esta cuenta cuando ejecutó el Asistente de configuración de equilibrio de carga de trabajo (antes de conectar su grupo al equilibrio de carga de trabajo). De manera opcional, puede usar la ficha **Consola** en XenCenter para iniciar sesión en el dispositivo.

Para iniciar sesión en el dispositivo virtual Equilibrio de carga de trabajo:

1. En el mensaje de inicio de sesión, introduzca el nombre de usuario de la cuenta.
2. En la solicitud de contraseña, introduzca la contraseña de la cuenta:

> **Nota:**
>
> Para cerrar sesión en el dispositivo virtual Equilibrio de carga de trabajo, simplemente escriba `logout` en el símbolo del sistema.

`wlb restart`

Ejecute el comando `wlb restart` desde cualquier lugar del dispositivo Equilibrio de carga de trabajo para detener y, a continuación, reiniciar los servicios Recopilación de datos de Equilibrio de carga de trabajo, Servicio web y Análisis de datos.

`wlb start`

Ejecute el comando `wlb start` desde cualquier parte del dispositivo de equilibrio de carga de trabajo para iniciar los servicios de recopilación de datos, servicio web y análisis de datos de equilibrio de carga de trabajo.

`wlb stop`

Ejecute el comando `wlb stop` desde cualquier parte del dispositivo de equilibrio de carga de trabajo para detener los servicios de recopilación de datos, servicio web y análisis de datos de equilibrio de carga de trabajo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

`wlb status`

Ejecute el comando `wlb status` desde cualquier lugar del dispositivo Equilibrio de carga de trabajo para determinar el estado del servidor Equilibrio de carga de trabajo. Después de ejecutar este comando, se muestra el estado de los tres servicios de equilibrio de carga de trabajo (el servicio web, el servicio de recopilación de datos y el servicio de análisis de datos).

Modificación de las opciones de configuración del equilibrio

Muchas configuraciones de equilibrio de carga de trabajo, como las opciones de configuración de la base de datos y el servicio web, se almacenan en el archivo `wlb.conf`. El archivo `wlb.conf` es un archivo de configuración en el dispositivo virtual Equilibrio de carga de trabajo.

Para modificar las opciones más utilizadas, use el comando `wlb config`. La ejecución del comando `wlb config` en el dispositivo virtual Equilibrio de carga de trabajo permite cambiar el nombre de la cuenta de usuario Equilibrio de carga de trabajo, cambiar su contraseña o cambiar la contraseña de PostgreSQL. Después de ejecutar este comando, se reinician los servicios de equilibrio de carga de trabajo.

Ejecute el siguiente comando en el dispositivo virtual Equilibrio de carga de trabajo:

```
wlb config
<!--NeedCopy-->
```

La pantalla muestra una serie de preguntas que lo guían para cambiar el nombre de usuario y la contraseña de Equilibrio de carga de trabajo y la contraseña de PostgreSQL. Siga las preguntas en pantalla para cambiar estos elementos.

> **Importante:**
>
> Compruebe dos veces los valores que introduzca en el archivo `wlb.conf`: Equilibrio de carga de trabajo no valida los valores del archivo `wlb.conf`. Por lo tanto, si los parámetros de configuración que especifica no están dentro del rango requerido, Equilibrio de carga de trabajo no genera un registro de errores.

Modificar el archivo de configuración de Equilibrio de carga de trabajo

Puede modificar las opciones de configuración del equilibrio de carga de trabajo modificando el archivo `wlb.conf`, que se almacena en el directorio `/opt/vpx/wlb` del dispositivo virtual de equilibrio de carga de trabajo. En general, solo cambie la configuración de este archivo siguiendo las instrucciones de XenServer. Sin embargo, hay tres categorías de ajustes que puede cambiar si quiere:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Nombre y contraseña de cuenta de Workload Balancing**. Es más fácil modificar estas credenciales ejecutando el comando `wlb config`.
- **contraseña de base**de datos Este valor se puede modificar mediante el archivo wlb.conf. Sin embargo, recomendamos modificarla mediante el comando `wlb config`, ya que este comando modifica el archivo wlb.conf y actualiza automáticamente la contraseña en la base de datos. Si decide modificar el archivo wlb.conf, debe ejecutar una consulta para actualizar la base de datos con la nueva contraseña.
- **Parámetros de limpieza de bases**de datos. Puede modificar los parámetros de limpieza de la base de datos, como el intervalo de limpieza de la base de datos, utilizando este archivo siguiendo las instrucciones de la sección de administración de la base de datos. Sin embargo, si lo hace, le recomendamos que actúe con precaución.

Para todos los demás ajustes del `wlb.conf` archivo, le recomendamos que los deje como predeterminados, a menos que se le haya indicado que los modifique.

Para modificar el archivo `wlb.conf`:

1. Ejecute lo siguiente desde el símbolo del sistema en el dispositivo virtual Equilibrio de carga de trabajo (mediante VI como ejemplo):

   ```
   vi /opt/vpx/wlb/wlb.conf
   <!--NeedCopy-->
   ```

   La pantalla muestra varias secciones diferentes de opciones de configuración.

2. Modifique las opciones de configuración y salga del editor.

No necesita reiniciar los servicios de equilibrio de carga de trabajo después de modificar el archivo `wlb.conf`. Los cambios entran en vigor inmediatamente después de salir del editor.

> **Importante:**
>
> Compruebe dos veces los valores que introduzca en el archivo `wlb.conf`: Equilibrio de carga de trabajo no valida los valores del archivo `wlb.conf`. Por lo tanto, si los parámetros de configuración que especifica no están dentro del rango requerido, Equilibrio de carga de trabajo no genera un registro de errores.

Aumente los detalles en el registro de equilibrio de carga de

El registro de equilibrio de carga de trabajo proporciona una lista de eventos en el dispositivo virtual de equilibrio de carga de trabajo, incluidas las acciones del motor de análisis, la base de datos y el registro de auditoría. Este archivo de registro se encuentra en esta ubicación: `/var/log/wlb/LogFile.log`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si lo quiere, puede aumentar el nivel de detalle que proporciona el registro de equilibrio de carga de trabajo. Para ello, modifique la sección `Trace flags` del archivo de configuración de equilibrio de carga de trabajo (`wlb.conf`), que se encuentra en la siguiente ubicación: `/opt/vpx/wlb/wlb.conf`. Escriba 1 o true para habilitar el registro para un seguimiento específico y 0 o false para inhabilitar el registro. Por ejemplo, para habilitar el registro para el seguimiento de Analysis Engine, introduzca:

```
AnalEngTrace=1
<!--NeedCopy-->
```

Es posible que desee aumentar los detalles del registro antes de informar de un problema al soporte técnico de XenServer o al solucionar problemas.

Opción de registro	Bandera de traza	Beneficio o propósito
Seguimiento del motor de análisis	`AnalEngTrace`	Registra los detalles de los cálculos del motor de análisis. Muestra detalles de las decisiones que toma el motor de análisis y, potencialmente, obtiene información sobre las razones por las que el equilibrio de carga de trabajo no hace recomendaciones.
Rastreo de bases	`DatabaseTrace`	Registra detalles sobre las lecturas/escrituras de bases Sin embargo, dejar este seguimiento activado aumenta el tamaño del archivo de registro rápidamente.
Seguimiento de recopilación de datos	`DataCollectionTrace`	Registra las acciones de recuperación de métricas. Este valor le permite ver las métricas que el equilibrio de carga de trabajo está recuperando e insertando en el data store de equilibrio de carga de trabajo. Sin embargo, dejar este seguimiento activado aumenta el tamaño del archivo de registro rápidamente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Opción de registro	Bandera de traza	Beneficio o propósito
Rastreo de compactación de datos	`DataCompactionTrace`	Registra detalles sobre cuántos milisegundos tardaron en compactar los datos de métricas.
Seguimiento de eventos de datos	`DataEventTrace`	Este seguimiento proporciona detalles sobre los eventos que Workload Balancing detecta de XenServer.
Rastreo de limpieza de datos	`DataGroomingTrace`	Este seguimiento proporciona detalles sobre la limpieza de la base de datos.
Seguimiento de métricas de datos	`DataMetricsTrace`	Registra los detalles sobre el análisis de los datos de métricas. Si se deja este rastro activado, el tamaño del archivo de registro se incrementa rápidamente.
Seguimiento de administración de colas	`QueueManagementTrace`	Registra detalles sobre el procesamiento de administración de colas de recopilación de datos (Esta opción es para uso interno).
Seguimiento de guardado de datos	`DataSaveTrace`	Registra los detalles sobre el grupo que se guarda en la base de datos.
Servidor de partituras Trace	`ScoreHostTrace`	Registra detalles sobre cómo el equilibrio de carga de trabajo llega a una puntuación para un host. Este seguimiento muestra las puntuaciones detalladas generadas por Workload Balancing al calcular las clasificaciones por estrellas para seleccionar los hosts óptimos para la ubicación de las máquinas virtuales.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Opción de registro	Bandera de traza	Beneficio o propósito
Seguimiento del registro de auditoría	`AuditLogTrace`	Muestra la acción de los datos de registro de auditoría que se capturan y escriben. (Esta opción es solo para uso interno y no proporciona información que se captura en el registro de auditoría). Sin embargo, dejar este seguimiento activado aumenta el tamaño del archivo de registro rápidamente.
Seguimiento de tareas programadas	`ScheduledTaskTrace`	Registra detalles sobre las tareas programadas. Por ejemplo, si los cambios de modo programados no funcionan, es posible que quiera habilitar este seguimiento para investigar la causa.
Rastreo de servicios web	`WlbWebServiceTrace`	Registra los detalles sobre la comunicación con la interfaz del servicio web.

Certificados para el equilibrio de carga

November 8, 2023

XenServer y Workload Balancing se comunican a través de HTTPS. Durante la configuración de equilibrio de carga de trabajo, el asistente crea automáticamente un certificado de prueba autofirmado. Este certificado de prueba autofirmado permite a Workload Balancing establecer una conexión TLS con XenServer. De forma predeterminada, Workload Balancing crea automáticamente esta conexión TLS con XenServer. No necesita realizar ninguna configuración de certificado durante o después de la configuración para que Equilibrio de carga de trabajo cree esta conexión TLS.

> **Nota:**
>
> El certificado autofirmado es un marcador de posición para facilitar la comunicación HTTPS y

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

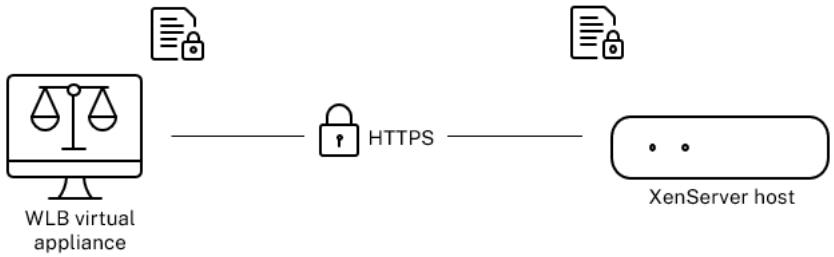
> no proviene de una entidad de certificación de confianza. Para mayor seguridad, se recomienda utilizar un certificado firmado por una entidad de certificación de confianza.

Para usar un certificado de otra entidad de certificación, como uno firmado por una autoridad comercial, debe configurar Workload Balancing y XenServer para usarlo.

De forma predeterminada, XenServer no valida la identidad del certificado antes de establecer la conexión con Workload Balancing. Para configurar XenServer para que busque un certificado específico, exporte el certificado raíz que se utilizó para firmar el certificado. Copie el certificado en XenServer y configure XenServer para que lo compruebe cuando se establezca una conexión a Workload Balancing. XenServer actúa como cliente en este caso y Workload Balancing actúa como servidor.

En función de sus objetivos de seguridad, puede:

- Configure XenServer para comprobar el certificado autofirmado.
- Configure XenServer para verificar un certificado de una entidad emisora de certificados.



> **Nota:**
>
> La verificación de certificados es una medida de seguridad diseñada para evitar conexiones no deseadas. Los certificados de equilibrio de carga de trabajo deben cumplir requisitos estrictos o la verificación del certificado no se realizará correctamente. Cuando se produce un error en la verificación del certificado, XenServer no permite la conexión.
>
> Para que la verificación de los certificados se realice correctamente, debe almacenar los certificados en las ubicaciones específicas en las que XenServer espera encontrarlos.

Configurar XenServer para verificar el certificado autofirmado

Puede configurar XenServer para comprobar que el certificado autofirmado de equilibrio de carga de trabajo de XenServer es auténtico antes de que XenServer permita la conexión de equilibrio de carga de trabajo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Importante:**
>
> Para verificar el certificado autofirmado de Equilibrio de carga de trabajo de XenServer, debe conectarse a Equilibrio de carga de trabajo con su nombre de host. Para encontrar el nombre de host de equilibrio de carga de trabajo, ejecute el comando `hostname` en el dispositivo virtual.

Para configurar XenServer para que verifique el certificado autofirmado, complete los siguientes pasos:

1. Copie el certificado autofirmado del dispositivo virtual Equilibrio de carga de trabajo al coordinador del grupo. El certificado autofirmado de equilibrio de carga de trabajo de XenServer se almacena en. `/etc/ssl/certs/server.pem` Ejecute el siguiente comando en el coordinador del grupo:

   ```
   scp root@<wlb-ip>:/etc/ssl/certs/server.pem .
   <!--NeedCopy-->
   ```

2. Si recibe un mensaje que indica que `wlb-ip` no se puede establecer la autenticidad de, escriba `yes` para continuar.

3. Introduzca la contraseña raíz del dispositivo virtual Workload Balancing cuando se le solicite El certificado se copia en el directorio actual.

4. Instale el certificado. Ejecute el siguiente comando en el directorio donde copió el certificado:

   ```
   xe pool-certificate-install filename=server.pem
   <!--NeedCopy-->
   ```

5. Verifique que el certificado se haya instalado correctamente ejecutando el siguiente comando en el coordinador del grupo:

   ```
   xe pool-certificate-list
   <!--NeedCopy-->
   ```

   Si instaló el certificado correctamente, el resultado de este comando incluye el certificado raíz exportado. Al ejecutar este comando, se enumeran todos los certificados TLS instalados, incluido el certificado que instaló.

6. Para sincronizar el certificado del coordinador con todos los hosts del grupo, ejecute el siguiente comando en el coordinador del grupo:

   ```
   xe pool-certificate-sync
   <!--NeedCopy-->
   ```

   Al ejecutar el comando `pool-certificate-sync` en el coordinador, se sincronizan las listas de certificados y revocaciones de certificados de todos los hosts del grupo con el coordinador. Esta acción garantiza que todos los hosts del grupo usen los mismos certificados.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

No hay ningún resultado de este comando. Sin embargo, el siguiente paso no funciona si este no funcionó correctamente.

7. Indique a XenServer que verifique el certificado antes de conectarse al dispositivo virtual Workload Balancing. Ejecute el siguiente comando en el coordinador del grupo:

```
xe pool-param-set wlb-verify-cert=true uuid=uuid_of_pool
<!--NeedCopy-->
```

> **Sugerencia:**
>
> Al pulsar la tecla **Tab**, se rellena automáticamente el UUID del grupo.

8. (Opcional) Para verificar que este procedimiento funcionó correctamente, lleve a cabo los siguientes pasos:

   a) Para comprobar si el certificado está sincronizado con los demás hosts del grupo, ejecute el comando `pool-certificate-list` en esos hosts.

   b) Para comprobar si XenServer estaba configurado para verificar el certificado, ejecute el comando `pool-param-get` con el parámetro `param-name`=wlb-verify-cert. Por ejemplo:

```
xe pool-param-get param-name=wlb-verify-cert uuid=uuid_of_pool
<!--NeedCopy-->
```

Configurar XenServer para verificar un certificado de una entidad emisora de certificados

Puede configurar XenServer para verificar un certificado firmado por una entidad de certificación de confianza.

Para los certificados de una autoridad de confianza, XenServer requiere un certificado o una cadena de certificados exportados (los certificados intermedio y raíz) en un `.pem` formato que contenga la clave pública.

Si quiere que Equilibrio de carga de trabajo use un certificado de autoridad de confianza, lleve a cabo las siguientes tareas:

1. Obtenga un certificado firmado de la entidad de certificación.
2. Especifique y aplique el nuevo certificado.
3. Importe la cadena de certificados en el grupo.

Antes de comenzar estas tareas, asegúrese de que:

- Conoce la dirección IP del coordinador del grupo de XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- XenServer puede resolver el nombre de host de equilibrio de carga de trabajo. (Por ejemplo, puede intentar hacer ping al FQDN de equilibrio de carga de trabajo desde la consola de XenServer para el coordinador del grupo).

Obtenga un certificado firmado de la entidad de certificación

Para obtener un certificado de una entidad de certificación, debe generar una solicitud de firma de certificado (CSR). En el dispositivo virtual Equilibrio de carga de trabajo, cree una clave privada y use esa clave privada para generar la CSR.

Pautas para especificar el nombre común El nombre común (CN) que especifique al crear una CSR debe coincidir exactamente con el FQDN de su dispositivo virtual de equilibrio de carga de trabajo. También debe coincidir con el FQDN o la dirección IP que especificó en el cuadro **Dirección** del cuadro de diálogo **Conectarse al servidor WLB**.

Para asegurarse de que el nombre coincida, especifique el nombre común siguiendo una de estas pautas:

- Especifique la misma información para el nombre común del certificado que especificó en el cuadro de diálogo **Conectar al servidor WLB**.

  Por ejemplo, si el dispositivo virtual Equilibrio de carga de trabajo se denomina `wlb-vpx.yourdomain`, especifique `wlb-vpx.yourdomain` en el cuadro de diálogo **Conectarse al servidor WLB** y proporcione `wlb-vpx.yourdomain` como Nombre común al crear la CSR.
- Si conectó su grupo a Equilibrio de carga de trabajo por dirección IP, utilice el FQDN como nombre común y la dirección IP como nombre alternativo del sujeto (SAN). Sin embargo, este enfoque puede no funcionar en todas las situaciones.

Crea un archivo de clave privada En el dispositivo virtual Equilibrio de carga de trabajo, complete los siguientes pasos:

1. Crea un archivo de clave privada:

```
openssl genrsa -des3 -out privatekey.pem 2048
<!--NeedCopy-->
```

2. Elimine la contraseña:

```
openssl rsa -in privatekey.pem -out privatekey.nop.pem
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Si escribe la contraseña de forma incorrecta o incoherente, es posible que reciba algunos mensajes que indican que hay un error en la interfaz de usuario. Puede ignorar el mensaje y volver a ejecutar el comando para crear el archivo de clave privada.

Generar la solicitud de firma de certificado En el dispositivo virtual Equilibrio de carga de trabajo, complete los siguientes pasos:

1. Cree la solicitud de firma de certificado (CSR) con la clave privada:

```
openssl req -new -key privatekey.nop.pem -out csr
<!--NeedCopy-->
```

2. Siga las instrucciones para proporcionar la información necesaria para generar la CSR:

   Nombre del país. Introduzca los códigos de país del certificado TLS para su país. Por ejemplo, CA para Canadá o JM para Jamaica. Puede encontrar una lista de códigos de países de certificados TLS en la web.

   Nombre del**estado o provincia (nombre completo)**. Introduzca el estado o la provincia donde se encuentra la agrupación. Por ejemplo, Massachusetts o Alberta.

   Nombre de la localidad. Nombre de la ciudad donde se encuentra la agrupación.

   Nombre de la organización. El nombre de su empresa u organización.

   Nombre de la unidad organizativa. Introduzca el nombre del departamento. Este campo es opcional.

   Nombre común. Introduzca el FQDN de su servidor de equilibrio de carga de trabajo. Este valor debe coincidir con el nombre que usa el grupo para conectarse a Equilibrio de carga de trabajo. Para obtener más información, consulte Pautas para especificar el nombre común.

   Dirección de correo. Esta dirección de correo electrónico se incluye en el certificado cuando lo genera.

3. Proporcione atributos opcionales o haga clic en Entrar para omitir esta información.

   La solicitud de CSR se guarda en el directorio actual y se denomina `csr`.

4. Muestre la CSR en la ventana de la consola ejecutando los siguientes comandos en la consola del dispositivo Equilibrio de carga de trabajo:

```
cat csr
<!--NeedCopy-->
```

5. Copie la CSR completa y utilícela para solicitar el certificado a la entidad de certificación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Especificar y aplicar el nuevo certificado

Use este procedimiento para especificar que Equilibrio de carga de trabajo use un certificado de una entidad de certificación. Este procedimiento instala los certificados raíz y (si están disponibles) intermedios.

Para especificar un certificado nuevo, lleve a cabo los siguientes pasos:

1. Descargue el certificado firmado, el certificado raíz y, si la entidad de certificación tiene uno, el certificado intermedio de la entidad de certificación.
2. Si no descargó los certificados directamente en el dispositivo virtual Equilibrio de carga de trabajo, cópielos mediante uno de los siguientes métodos:
   - Desde un equipo Windows, use WinSCP u otra utilidad de copia.

     Para el nombre del host, puede introducir la dirección IP y dejar el puerto en el valor predeterminado. El nombre de usuario y la contraseña suelen ser root y cualquier contraseña que establezca durante la configuración.
   - Desde un equipo Linux hasta el dispositivo Equilibrio de carga de trabajo, use SCP u otra utilidad de copia. Por ejemplo:

     ```
     scp root_ca.pem root@wlb-ip:/path_on_your_WLB
     <!--NeedCopy-->
     ```
3. En el dispositivo virtual Equilibrio de carga de trabajo, combine el contenido de todos los certificados (certificado raíz, certificado intermedio, si existe, y certificado firmado) en un archivo. Puede usar el siguiente comando:

   ```
   cat signed_cert.pem intermediate_ca.pem root_ca.pem > server.pem
   <!--NeedCopy-->
   ```
4. Cambie el nombre del certificado y la clave existentes mediante el comando move:

   ```
   mv /etc/ssl/certs/server.pem /etc/ssl/certs/server.pem_orig
   mv /etc/ssl/certs/server.key /etc/ssl/certs/server.key_orig
   <!--NeedCopy-->
   ```
5. Copie el certificado combinado:

   ```
   mv server.pem /etc/ssl/certs/server.pem
   <!--NeedCopy-->
   ```
6. Copie la clave privada creada anteriormente:

   ```
   mv privatekey.nop.pem /etc/ssl/certs/server.key
   <!--NeedCopy-->
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

7. Haga que la clave privada sea legible solo por root. Use el comando `chmod` para corregir los permisos.

```
chmod 600 /etc/ssl/certs/server.key
<!--NeedCopy-->
```

8. Reinicio `stunnel`:

```
killall stunnel
stunnel
<!--NeedCopy-->
```

Importe la cadena de certificados en el grupo

Después de obtener los certificados, impórtelos al coordinador de grupos de XenServer. Sincronice los hosts del grupo para usar esos certificados. A continuación, puede configurar XenServer para comprobar la identidad y la validez del certificado cada vez que Workload Balancing se conecte a un host.

1. Copie el certificado firmado, el certificado raíz y, si la entidad de certificación tiene uno, el certificado intermedio de la entidad de certificación en el coordinador del grupo de XenServer.
2. Instale el certificado raíz en el coordinador del grupo:

```
xe pool-install-ca-certificate filename=root_ca.pem
<!--NeedCopy-->
```

3. Si corresponde, instale el certificado intermedio en el coordinador del grupo:

```
xe pool-install-ca-certificate filename=intermediate_ca.pem
<!--NeedCopy-->
```

4. Verifique que ambos certificados estén instalados correctamente ejecutando este comando en el coordinador del grupo:

```
xe pool-certificate-list
<!--NeedCopy-->
```

   La ejecución de este comando muestra todos los certificados TLS instalados. Si los certificados se instalaron correctamente, aparecerán en esta lista.

5. Sincronice el certificado del coordinador del grupo con todos los hosts del grupo:

```
xe pool-certificate-sync
<!--NeedCopy-->
```

   Al ejecutar el comando `pool-certificate-sync` en el coordinador, se sincronizan los certificados y las listas de revocación de certificados de todos los hosts del grupo con el coordi-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

nador del grupo. Esta acción garantiza que todos los hosts del grupo usen los mismos certificados.

6. Indique a XenServer que verifique un certificado antes de conectarse al dispositivo virtual Workload Balancing. Ejecute el siguiente comando en el coordinador del grupo:

```
xe pool-param-set wlb-verify-cert=true uuid=uuid_of_pool
<!--NeedCopy-->
```

> **Sugerencia:**
>
> Al pulsar la tecla Tab, se rellena automáticamente el UUID del grupo.

7. Si especificó una dirección IP en el cuadro de diálogo **Conectarse a WLB** antes de habilitar la verificación de certificados, es posible que se le pida que vuelva a conectar el grupo a Equilibrio de carga de trabajo.

   Especifique el FQDN para el dispositivo de equilibrio de carga de trabajo en **Dirección** en el cuadro de diálogo **Conectar a WLB** exactamente como aparece en el nombre común del certificado. Introduzca el FQDN para asegurarse de que el nombre común coincide con el nombre que utiliza XenServer para conectarse.

Solución de problemas

- Si el grupo no puede conectarse al equilibrio de carga de trabajo después de configurar la verificación de certificados, compruebe si el grupo se puede conectar si desactiva la verificación de certificados. Puede usar el comando `xe pool-param-set wlb-verify-cert=false uuid=uuid_of_pool` para inhabilitar la verificación de certificados. Si se puede conectar con la verificación desactivada, el problema está en la configuración de su certificado. Si no se puede conectar, el problema está en las credenciales de equilibrio de carga de trabajo o en la conexión de red.
- Algunas autoridades de certificación comercial proporcionan herramientas para verificar que el certificado esté instalado correctamente. Considere la posibilidad de ejecutar estas herramientas si estos procedimientos no ayudan a aislar el problema. Si estas herramientas requieren la especificación de un puerto TLS, especifique el puerto 8012 o el puerto que haya configurado durante la configuración del equilibrio de carga de trabajo.
- Si la ficha **WLB** muestra un error de conexión, puede haber un conflicto entre el nombre común del certificado y el nombre del dispositivo virtual Equilibrio de carga de trabajo. El nombre del dispositivo virtual de equilibrio de carga de trabajo y el nombre común del certificado deben coincidir exactamente.

Para obtener más información, consulte Solucionar problemas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

---

layout: doc
description: Diagnose and gather information about issues that might arise when using Workload Balancing.—

Solucionar problemas de equilibrio de carga de

Si bien el equilibrio de carga de trabajo suele funcionar sin problemas, esta serie de secciones proporciona orientación en caso de que encuentre problemas.

> **Notas:**
>
> - Workload Balancing está disponible para los clientes de XenServer Premium Edition. Para obtener más información sobre las licencias de XenServer, consulte Licencias. Para actualizar o comprar una licencia de XenServer, visite el sitio web de XenServer.
> - Workload Balancing 8.3.0 y las versiones posteriores son compatibles con XenServer 8 y Citrix Hypervisor 8.2 CU 1.

Determinar el estado del dispositivo virtual Equilibrio de carga de trabajo

Ejecute el comando `systemctl status workloadbalancing`. Para obtener más información, consulte Comandos de equilibrio de cargade trabajo

Consejos generales para solucionar problemas

- Comience a solucionar problemas revisando los archivos de registro de equilibrio de carga de trabajo (`LogFile.log` y `wlb_install_log.log`) Puede encontrar estos registros en el dispositivo virtual Equilibrio de carga de trabajo en esta ubicación (de forma predeterminada):

  `/var/log/wlb`

  El nivel de detalle de estos archivos de registro se puede configurar mediante el archivo `wlb.conf`. Para obtener más información, consulte Aumentar los detalles en el registro de equilibrio de cargade trabajo.
- Consulte los registros en la ficha **Registros** de XenCenter para obtener más información.
- Para comprobar el número de compilación del dispositivo virtual de equilibrio de carga de trabajo, ejecute el siguiente comando en un host de un grupo que supervise el dispositivo virtual:

```
1  xe pool-retrieve-wlb-diagnostics | more
2  <!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El número de versión del equilibrio de carga de trabajo aparece en la parte superior de la salida.

- El dispositivo virtual Equilibrio de carga de trabajo se basa en el sistema operativo CentOS. Si experimenta problemas relacionados con la CPU, la memoria o el disco en el dispositivo virtual, puede utilizar los inicios de sesión estándar de Linux en `/var/log/*` para analizar el problema.
- Utilice los comandos estándar de depuración y ajuste del rendimiento de Linux para comprender el comportamiento del dispositivo virtual. Por ejemplo, `topps`, `free`, `sar`, y `netstat`.

Mensajes de error

Equilibrio de carga de trabajo muestra los errores en pantalla como cuadros de diálogo y como mensajes de error en la ficha **Registros** de XenCenter.

Si aparece un mensaje de error, revise el registro de eventos de XenCenter para obtener información adicional. Para obtener más información, consulte la documentación del producto XenCenter.

Problemas al introducir credenciales de equilibrio de carga

Si no puede introducir correctamente la cuenta de usuario y la contraseña del dispositivo virtual mientras configura el cuadro de diálogo **Conectarse al servidor WLB**, intente lo siguiente:

- Asegúrese de que el dispositivo virtual Equilibrio de carga de trabajo se haya importado y configurado correctamente y que todos sus servicios estén en ejecución
- Compruebe que está introduciendo las credenciales correctas. El cuadro de diálogo **Conectar al servidor WLB** solicita dos credenciales diferentes:
  - **Credenciales del servidor WLB**: XenServer usa esta cuenta para comunicarse con Workload Balancing. Creó esta cuenta en el dispositivo virtual de Workload Balancing durante la configuración de equilibrio de carga De forma predeterminada, el nombre de usuario de esta cuenta es `wlbuser`.
  - **Credenciales de Citrix Hypervisor**: El dispositivo virtual Workload Balancing utiliza esta cuenta para conectarse al grupo de XenServer. Esta cuenta se crea en el coordinador del grupo de XenServer y tiene la función `pool-admin` or `pool-operator` .
- Puede escribir un nombre de host en el cuadro **Dirección**, pero debe ser el nombre de dominio completo (FQDN) del dispositivo virtual Equilibrio de carga de trabajo. No introduzca el nombre de host del servidor físico que aloja el dispositivo. Si tiene problemas para escribir el nombre de un equipo, intente usar la dirección IP del dispositivo Equilibrio de carga de trabajo en su lugar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Compruebe que el host utiliza el servidor DNS correcto y que el host XenServer puede ponerse en contacto con el servidor Workload Balancing mediante su FQDN. Para realizar esta comprobación, haga ping al dispositivo de equilibrio de carga de trabajo mediante su FQDN desde el host de XenServer. Por ejemplo, introduzca lo siguiente en la consola host de XenServer:

```
ping wlb-vpx-1.mydomain.net
<!--NeedCopy-->
```

Problemas con los firewalls

Aparece el siguiente error si el dispositivo virtual Equilibrio de carga de trabajo está detrás de un firewall de hardware y no configuró la configuración de firewall adecuada: "Se produjo un error al conectarse al servidor de equilibrio de carga de trabajo: <nombre de agrupación> Haga clic en **Inicializar WLB** para reinicializar la configuración de conexión". Este error también puede aparecer si no se puede acceder al dispositivo Equilibrio de carga de trabajo.

Si el dispositivo virtual Equilibrio de carga de trabajo está detrás de un firewall, abra el puerto 8012.

Del mismo modo, el puerto que XenServer utiliza para contactar con Workload Balancing (8012 de forma predeterminada) debe coincidir con el número de puerto especificado al ejecutar el asistente de configuración de Workload Balancing.

Errores de conexión de equilibrio

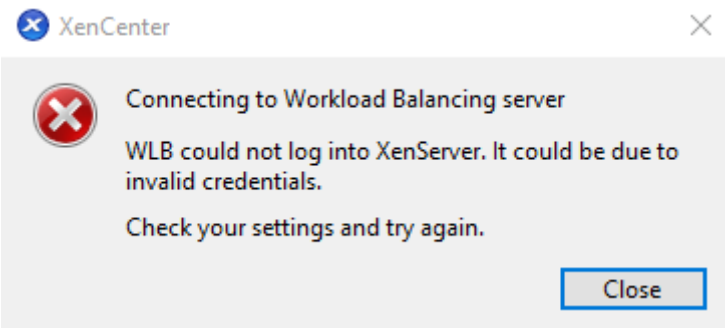
Si recibe un error de conexión después de configurar y conectarse a Equilibrio de carga de trabajo, es posible que las credenciales ya no sean válidas. Para aislar este problema:

1. Compruebe que las credenciales introducidas en el cuadro de diálogo **Conectarse al servidor WLB** son correctas. Para obtener más información, consulte los casos 1 y 2.
2. Compruebe que la dirección IP o el FQDN del dispositivo virtual de equilibrio de carga de trabajo que introdujo en el cuadro de diálogo **Conectarse al servidor WLB** sean correctos.
3. Compruebe que el nombre de usuario que creó durante la configuración del equilibrio de carga de trabajo coincida con las credenciales que introdujo en el cuadro de diálogo **Conectarse al servidor WLB** .
4. Si recibe un error de conexión en la línea Estado de equilibrio de carga de trabajo en la ficha **WLB**, es posible que deba volver a configurar el equilibrio de carga de trabajo en ese grupo. Haga clic en el botón **Conectar** de la ficha **WLB** y vuelva a introducir las credenciales del host.

Puede encontrarse con uno de los siguientes casos al intentar establecer una conexión desde XenCenter al dispositivo virtual de equilibrio de carga de trabajo.

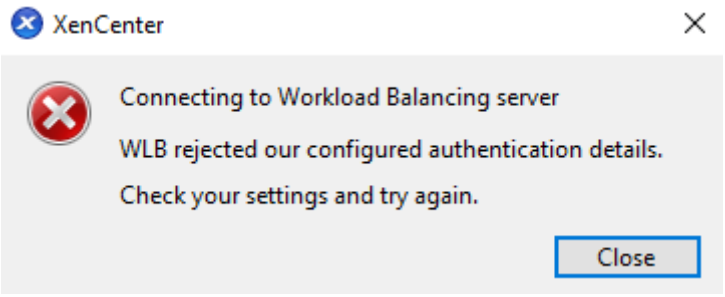
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Caso 1



Esto significa que las credenciales introducidas en el campo **Credenciales de Citrix Hypervisor** del cuadro de diálogo **Conectarse al servidor WLB** son incorrectas. Para solucionarlo, vuelva a marcar las credenciales o active la casilla **Usar las credenciales actuales de XenCenter**.

Caso 2



Esto significa que hay un problema con las credenciales introducidas en el campo Credenciales **del servidor WLB del** cuadro de diálogo **Conectarse al servidor WLB** al intentar conectarse al dispositivo virtual de equilibrio de carga de trabajo (el nombre de usuario o la contraseña son incorrectos). Sin embargo, también puede significar que el servicio de equilibrio de carga de trabajo no se está ejecutando o que hay un problema con el archivo de configuración de la base de datos.

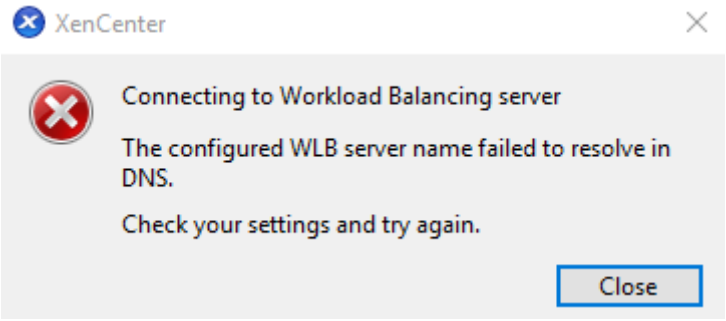
Para solucionar problemas con las credenciales, asegúrate de utilizar el nombre de usuario y la contraseña correctos. El nombre de usuario predeterminado para el campo de **credenciales del servidor WLB** es `wlbuser` (no root). Root es el nombre de usuario predeterminado del administrador. Tenga en cuenta que `wlbuser` no es un usuario real con privilegios de inicio de sesión en el dispositivo (no existe `/etc/passwd`) y, por lo tanto, estas credenciales solo se utilizan para conectarse al propio Workload Balancing. Como tal, se pueden restablecer fácilmente ejecutando el comando `wlbconfig`. Para cambiar sus credenciales, consulte Cambiar las credenciales de equilibrio de carga de trabajo. Para ejecutar el comando `wlbconfig`, debe poder iniciar sesión en el dispositivo como usuario root. Si se desconoce la contraseña raíz, se puede restablecer mediante el procedimiento normal de recuperación de contraseñas de CentOS/RHEL.

Si has restablecido sus credenciales pero el error persiste:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Compruebe si el proceso de equilibrio de carga de trabajo se está ejecutando mediante el comando `systemctl status workloadbalancing`.
2. Asegúrese de que el archivo `wlb.conf` existe y se encuentra en el directorio correcto ejecutando este comando: `cat /opt/vpx/wlb/wlb.conf`

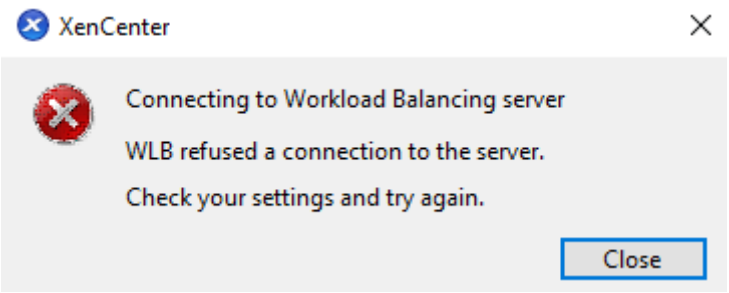
Caso 3



Esto indica que hay un problema al conectarse al puerto especificado en las opciones de dirección del servidor al conectarse a Workload Balancing desde XenCenter (se introdujo un puerto incorrecto o el puerto no escucha). Para solucionar este problema:

1. Asegúrese de que el dispositivo de destino esté en funcionamiento.
2. Vuelva a comprobar el puerto introducido en la ventana de detalles de conexión de Workload Balancing (el valor predeterminado es 8012).
3. Asegúrese de que este puerto esté activado en el dispositivo y escuchando. Utilice comandos como `telnet <port>` o `iptables -L` para ayudar a determinar si el puerto está escuchando o si se está denegando el tráfico en este puerto.

Caso 4



Este error se produce cuando hay un problema con stunnel (o bien no se está ejecutando o el par certificado/clave es incorrecto). Para solucionar este problema, primero compruebe el certificado y la clave:

1. Confirme que el certificado no ha caducado ejecutando el siguiente comando:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
openssl x509 -dates -in $(grep cert\ = /etc/stunnel/stunnel.conf |
   cut -d '=' -f2) -noout
<!--NeedCopy-->
```

2. Compare el hexadecimal en la salida de los dos comandos siguientes. Si la salida no coincide, se está utilizando la clave incorrecta.

```
openssl x509 -modulus -in $(grep cert\ = /etc/stunnel/stunnel.conf
    |cut -d '=' -f2) -noout | openssl md5
<!--NeedCopy-->
```

y

```
 openssl rsa -modulus -in $(grep key\ = /etc/stunnel/stunnel.conf
   | cut -d '=' -f2) -noout | openssl md5
<!--NeedCopy-->
```

Si no hay problemas con el certificado y la clave, asegúrese de que stunnel se esté ejecutando y esté enlazado al puerto 8012 (o al puerto configurado):

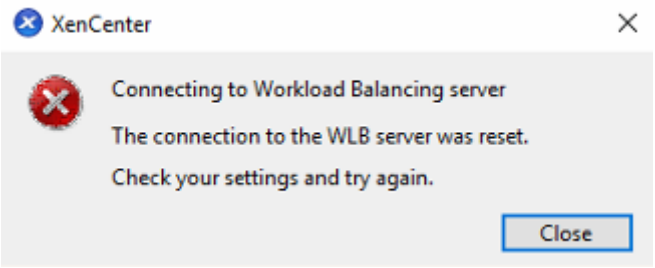
1. Ejecute el siguiente comando en la CLI del dispositivo WLB:

```
netstat -tulpn
<!--NeedCopy-->
```

   En la salida, 8012 (o el puerto personalizado) debe mostrar `status: LISTEN`.

2. Si el dispositivo se quedó sin espacio, stunnel no funcionará. Utilice comandos como `df -h` o `du -hs /*` para comprobar si tiene suficiente espacio disponible en el dispositivo. Para aumentar el espacio en disco, consulte Ampliar el disco del dispositivo virtual.

Caso 5



Este error puede producirse porque se ha finalizado el proceso de stunnel. Si al reiniciar el proceso se obtienen los mismos resultados, reinicie el dispositivo virtual de equilibrio de carga de trabajo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cualquier otro error

Si encuentra algún otro error al intentar conectarse a Workload Balancing o necesita más ayuda para realizar los pasos anteriores, recopile los registros de equilibrio de carga de trabajo que se encuentran en el directorio `/var/log/wlb` del dispositivo de equilibrio de carga de trabajo.

Ponte en contacto con el equipo de soporte para obtener más ayuda.

Workload Balancing deja de funcionar

Si el equilibrio de carga de trabajo no funciona (por ejemplo, no le permite guardar los cambios en la configuración), consulte el archivo de registro de equilibrio de carga de trabajo para ver el siguiente mensaje de error:

```
dwmdatacolsvc.exe: Don't have a valid pool. Trying again in 10 minutes.
<!--NeedCopy-->
```

Este error suele producirse en grupos que tienen una o más máquinas virtuales problemáticas. Cuando las VM son problemáticas, es posible que veas el siguiente comportamiento:

- **Windows**. La máquina virtual de Windows se bloquea debido a un error de detención ("pantalla azul").
- **Linux**. Es posible que la VM Linux no responda en la consola y, por lo general, no se apaga.

Como solución temporal para este problema:

1. Obligue a la VM a apagarse. Para hacerlo, puede realizar una de las siguientes acciones en el host con la máquina virtual problemática:

   - En XenCenter, seleccione la máquina virtual y, a continuación, en el menú VM, haga clic en Forzar **el apagado**.
   - Ejecute el comando `vm-shutdown` xe con el parámetro force establecido en **`true`**. Por ejemplo:

     ```
     xe vm-shutdown force=true uuid=vm_uuid
     <!--NeedCopy-->
     ```

     Puede encontrar el UUID del host en la ficha **General** de ese host (en XenCenter) o ejecutando el comando `host-list` xe. Puede encontrar el UUID de la máquina virtual en la ficha **General** de la máquina virtual o ejecutando el comando xe `vm-list`. Para obtener más información, consulte Interfaz de línea de comandos.

2. En `xsconsole` de XenServer que sirve a la máquina virtual bloqueada o en XenCenter, migre todas las máquinas virtuales a otro host y, a continuación, ejecute el comando `xe-toolstack`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

`-restart`. (No reinicie la pila de herramientas mientras la alta disponibilidad esté habilitada. Si es posible, desactive temporalmente HA antes de reiniciar la pila de herramientas).

Problemas al cambiar los servidores del equilibrio de carga de trabajo

Si conecta un grupo a un servidor de equilibrio de carga de trabajo diferente sin desconectarse del equilibrio de carga de trabajo, los servidores de equilibrio de carga de trabajo antiguos y nuevos supervisan el grupo.

Para resolver este problema, puede realizar una de las siguientes acciones:

- Apague y elimine el antiguo dispositivo virtual Equilibrio de carga de trabajo.
- Detener manualmente los servicios de equilibrio de carga de trabajo Estos servicios son análisis, recopilador de datos y servicio web.

> **Nota:**
>
> No utilice el comando `pool-deconfigure-wlb` xe para desconectar un grupo del dispositivo virtual Equilibrio de carga de trabajo ni use el comando `pool-initialize-wlb` xe para especificar un dispositivo diferente.

---

layout: doc
description: Convert VMware ESXi/vCenter VMs to XenServer VMs that have networking and storage configured and are ready to run in your environment.—

XenServer Conversion Manager

Utilice el dispositivo virtual XenServer Conversion Manager para migrar sus máquinas virtuales VMware ESXi/vCenter a XenServer de forma rápida y eficaz. Puede convertir hasta 10 máquinas virtuales VMware ESXi/vCenter en paralelo al mismo tiempo. Tras convertir las máquinas virtuales, Conversion Manager se apaga automáticamente por sí solo, lo que ahorra recursos en el host.

Como parte de la migración, XenCenter le ayuda a preparar las máquinas virtuales para la conectividad de redes y almacenamiento. Tras convertir sus máquinas virtuales en un entorno XenServer, están casi listas para ejecutarse.

Información general

XenServer le permite:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Convertir hasta 10 máquinas virtuales VMware ESXi/vCenter en paralelo con un sencillo asistente
- Asigne la configuración de red entre VMware y XenServer para que las máquinas virtuales convertidas puedan funcionar con la configuración de red adecuada
- Seleccione una ubicación de almacenamiento en la que desee que se ejecuten las nuevas máquinas virtuales de XenServer

> **Notas:**
>
> - XenCenter no elimina ni cambia el entorno de VMware existente. Las máquinas virtuales se duplican en el entorno de XenServer y no se eliminan de VMware.
> - El dispositivo virtual XenServer Conversion Manager admite la conversión de máquinas virtuales VMware ESXi/vCenter con diferentes tipos de almacenamiento, como aprovisionamiento ligero, aprovisionamiento grueso, IDE y SCSI.
> - El dispositivo virtual XenServer Conversion Manager no requiere que las máquinas virtuales de origen tengan VMware Tools instalado. Puede realizar la conversión en máquinas virtuales VMware ESXi/vCenter independientemente de si tienen instalado VMware Tools.
> - El dispositivo virtual XenServer Conversion Manager no puede convertir máquinas virtuales VMware ESXi/vCenter con cuatro o más discos en máquinas virtuales de XenServer. Las máquinas virtuales VMware ESXi/vCenter deben tener tres discos o menos.

Conozca XenServer

Antes de poder convertir su entorno, le recomendamos que se familiarice con los conceptos de XenServer. Para obtener más información, consulte Descripción general técnica.

Para convertir correctamente las máquinas virtuales VMware ESXi/vCenter en XenServer, realice las siguientes tareas:

- Configure un entorno de XenServer básico, incluida la instalación de XenServer. Para obtener más información, consulte Inicio e [instalación](/es-es/xenserver/8/install.html) rápidos.
- Cree una red en XenServer y asigne una dirección IP a una NIC. Para obtener más información, consulte Inicio rápido.
- Conéctese al almacenamiento. Para obtener más información, consulte Inicio rápido.

Compare la terminología de VMware y XenServer La siguiente tabla muestra el equivalente aproximado de XenServer para las funciones, conceptos y componentes comunes de VMware:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Plazo de VMware	Equivalente a XenServer
Cliente de VMware vSphere	XenCenter (la consola de administración de XenServer)
Clúster o grupo de recursos	Grupo de recursos
Almacén de datos	repositorio de almacenamiento
vMotion	Migración en vivo
Programación de recursos distribuidos (DRS)	Balance de carga
Alta disponibilidad (HA)	Alta disponibilidad (HA)
Convertidor de vCenter	Dispositivo virtual XenServer Conversion Manager
Control de acceso basado en roles (RBAC)	Control de acceso basado en roles (RBAC)

Resumen de conversiones

El dispositivo virtual XenCenter y XenServer Conversion Manager crean una copia de cada máquina virtual de destino. Tras convertir la máquina virtual de destino en una máquina virtual de XenServer con una conectividad de red y almacenamiento comparable, XenCenter importa la máquina virtual al grupo o host de XenServer. Puede convertir tan solo una o dos máquinas virtuales o realizar conversiones por lotes de un entorno completo de hasta 10 máquinas virtuales VMware ESXi/vCenter en paralelo y al mismo tiempo.

> **Nota:**
>
> Antes de convertir las máquinas virtuales de vSphere, debe apagar las máquinas virtuales (destinadas a la conversión) en vSphere. El dispositivo virtual XenServer Conversion Manager no admite la conversión de una máquina virtual en ejecución mediante la memoria copiada de vSphere a XenServer.
>
> Además, antes de realizar la conversión, asegúrese de que existan una red y un controlador de almacenamiento en su VM de VMware.

El proceso de conversión requiere cuatro elementos:

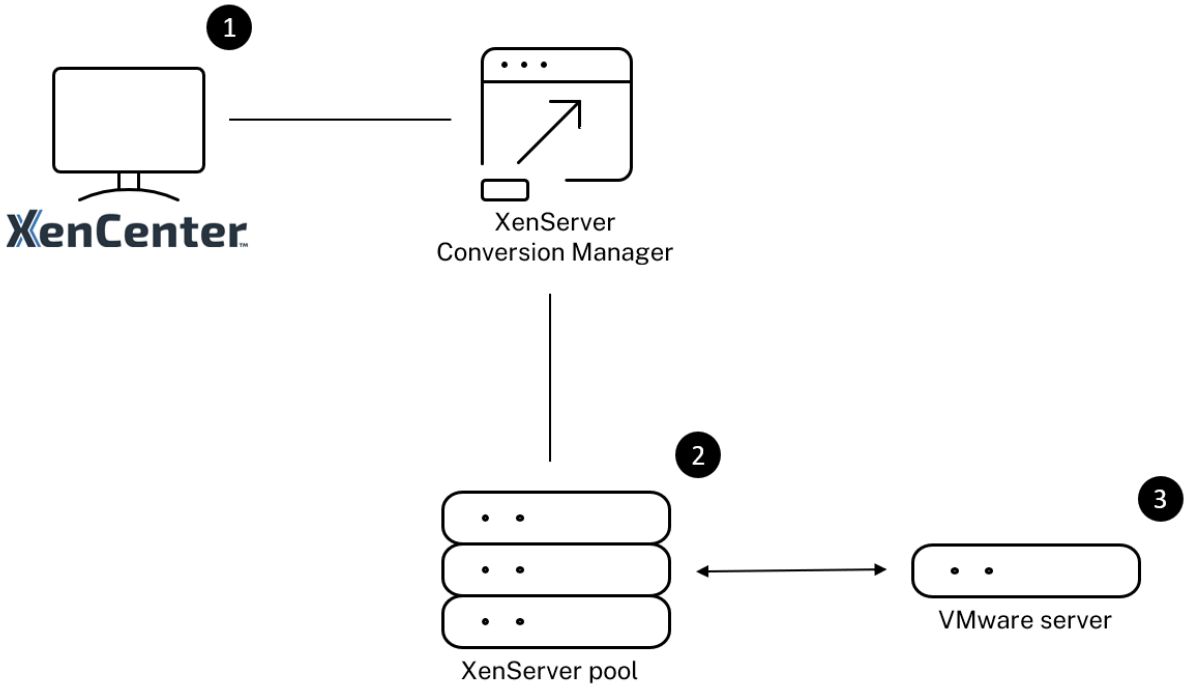
- **XenCenter** : la interfaz de administración de XenServer incluye un asistente de conversión en el que puede configurar las opciones de conversión y controlar la conversión. Puede instalar XenCenter en el escritorio de Windows. XenCenter debe poder conectarse a XenServer y al dispositivo virtual XenServer Conversion Manager.
- Dispositivo**virtual de XenServer Conversion Manager: una máquina virtual** preempaquetada que se importa al host o grupo de XenServer en el que desea ejecutar las máquinas vir-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

tuales convertidas. El dispositivo virtual convierte las copias de las máquinas virtuales VMware ESXi/vCenter al formato de máquina virtual de XenServer. Tras la conversión, importa estas copias al grupo o host de XenServer.

- **Host o grupo independiente de XenServer** : el entorno de XenServer en el que desea ejecutar las máquinas virtuales convertidas.
- **Servidor VMware**: XenServer Conversion Manager requiere una conexión a un servidor VMware que administre las máquinas virtuales que quiere convertir. Esta conexión puede ser a vCenter Server, ESXi Server o ESX Server. Las máquinas virtuales no se eliminan del servidor de VMware. En su lugar, el dispositivo virtual XenServer Conversion Manager hace una copia de estas máquinas virtuales y las convierte al formato de máquina virtual XenServer.

En la siguiente ilustración se muestran las relaciones entre estos componentes:



> En esta ilustración se muestra:
>
> 1. Cómo se comunica XenCenter con el dispositivo virtual XenServer Conversion Manager.
> 2. Cómo se autentica el dispositivo virtual XenServer Conversion Manager con el servidor VMware.
> 3. Cómo responde el servidor VMware al dispositivo virtual XenServer Conversion Manager durante la conversión.

El servidor VMware se comunica con el dispositivo virtual XenServer Conversion Manager solo cuando el dispositivo consulta al servidor VMware información del entorno y datos de disco durante la conversión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Resumen de cómo convertir máquinas virtuales Puede configurar el dispositivo virtual XenServer Conversion Manager y empezar a convertir las máquinas virtuales en tan solo unos sencillos pasos:

1. Descargue el dispositivo virtual XenServer Conversion Manager desde la página de descargas de XenServer.
2. Importe el dispositivo virtual XenServer Conversion Manager a XenServer mediante XenCenter.
3. Configure el dispositivo virtual XenServer Conversion Manager mediante XenCenter.
4. En XenCenter, inicie el asistente de conversión y comience a convertir las VM.
5. Complete las tareas posteriores a la conversión, que incluyen la instalación de XenServer VM Tools para Windows en las máquinas virtuales Windows. En el caso de las máquinas virtuales Linux, XenServer Conversion Manager instala automáticamente XenServer VM Tools for Linux durante el proceso de conversión.

Tras convertir las máquinas virtuales, Conversion Manager se apaga automáticamente por sí solo, lo que ahorra recursos en el host. Para obtener más información sobre cómo convertir máquinas virtuales VMware ESXi/vCenter, consulte Introducción a Conversion Manager.

---

layout: doc
description: Discover the features added in the latest XenServer Conversion Manager virtual appliance.—

Novedades de XenServer Conversion Manager

La versión más reciente del dispositivo virtual XenServer Conversion Manager es la 8.3.1. Puede descargar esta versión del dispositivo virtual XenServer Conversion Manager desde la página de descargas de XenServer.

Si ya tiene instalada una versión anterior del dispositivo virtual XenServer Conversion Manager y quiere actualizarla a la versión más reciente, no hay una ruta de actualización automática. Descargue la versión más reciente del dispositivo virtual y quite la versión anterior del sistema.

Novedades de la versión 8.3.1

Publicado el 1 de febrero de 2024

Esta actualización incluye la siguiente mejora:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Ahora puede convertir hasta 10 máquinas virtuales VMware ESXi/vCenter en paralelo al mismo tiempo.

---

layout: doc
description: Install and set up the XenServer Conversion Manager virtual appliance to benefit from the Conversion Manager feature in your XenServer pools.—

Introducción a XenServer Conversion Manager

Puede convertir fácilmente sus máquinas virtuales (VM) VMware ESXi/vCenter en XenServer en tan solo unos pasos:

1. Prepare el entorno de XenServer y revise la información sobre los requisitos previos.
2. Importe y configure el dispositivo virtual XenServer Conversion Manager mediante XenCenter.

   > **Nota:**
   >
   > Si ya tiene instalada una versión anterior del dispositivo virtual XenServer Conversion Manager y quiere actualizarla a la versión más reciente, no hay una ruta de actualización automática. Descargue la versión más reciente del dispositivo virtual desde la página de descargas de XenServer y quite la versión anterior del sistema.

3. Desde XenCenter, inicie el asistente de conversión y comience a convertir las máquinas virtuales VMware ESXi/vCenter en XenServer.
4. Complete las tareas posteriores a la conversión.
5. Revise otras tareas de conversión.

Prepare su entorno

Antes de convertir su entorno VMware, debe crear y preparar el host o grupo independiente de XenServer de destino para ejecutar las máquinas virtuales VMware ESXi/vCenter convertidas. La preparación del entorno incluye las siguientes actividades:

1. Definir una estrategia de cómo convertir su entorno de VMware. ¿Desea convertir 1 o 2 máquinas virtuales? ¿Quiere convertir todo su entorno? ¿Desea crear primero un piloto para asegurarse de que la configuración es correcta? ¿Ejecuta ambos entornos en paralelo? ¿Desea mantener su diseño de clúster actual al realizar la conversión a XenServer?

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Planificación de la configuración de redes. ¿Desea conectarse a las mismas redes físicas? ¿Desea simplificar o cambiar la configuración de red?
3. Instalar XenServer en los hosts que desee incluir en el grupo. Lo ideal sería conectar las NIC de los hosts a sus redes físicas antes de comenzar la instalación.
4. Crear un grupo y realizar cualquier configuración de red básica. Por ejemplo, haga lo siguiente:
    - Configure una red para conectarse al clúster de VMware en el host de XenServer (si el clúster no está en la misma red que el host de XenServer).
    - Configure una red para que se conecte a la cabina de almacenamiento. Es decir, si utiliza almacenamiento basado en IP, cree una red XenServer que se conecte a la red física de la matriz de almacenamiento.
    - Cree un grupo y agregue hosts a este grupo.
5. (Para almacenamiento compartido y grupos de XenServer). Preparar el almacenamiento compartido donde se almacenan los discos virtuales y crear una conexión al almacenamiento, conocida como repositorio de almacenamiento (SR) en el grupo.
6. (Opcional). Aunque no es un requisito para la conversión, es posible que desee configurar las cuentas de administrador del grupo de XenServer para que coincidan con las cuentas del servidor VMware. Para obtener información sobre cómo configurar el control de acceso basado en roles para cuentas de Active Directory, consulte Control de acceso basado en roles.

Instalar XenServer y crear un grupo

Antes de poder convertir las máquinas virtuales VMware ESXi/vCenter, asegúrese de crear un grupo o un host de XenServer en el que quiera ejecutar las máquinas virtuales convertidas. Este grupo debe tener una red configurada para poder conectarse al servidor VMware. Es posible que también desee configurar las mismas redes físicas en el grupo de XenServer que tiene en el clúster de VMware o simplificar la configuración de la red. Si quiere ejecutar las VM convertidas en un grupo, cree un repositorio de almacenamiento antes de la conversión y agregue el almacenamiento compartido al grupo.

Si es la primera vez que usa XenServer, puede obtener información sobre los aspectos básicos de XenServer, incluidas la instalación y la configuración básicas, leyendo Inicio rápido.

Consideraciones sobre el entorno de XenServer

Antes de instalar XenServer e importar el dispositivo virtual, tenga en cuenta los siguientes factores que podrían cambiar su estrategia de conversión:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Seleccionar el host en el que desea ejecutar el dispositivo virtual XenServer Conversion Manager. Importe el dispositivo virtual en el host independiente o en un host del grupo en el que ejecute las máquinas virtuales convertidas.

Para los grupos, puede ejecutar el dispositivo virtual en cualquier host del grupo, siempre que su almacenamiento cumpla con los requisitos de almacenamiento.

> **Nota:**
>
> Se recomienda ejecutar solo un XenServer Conversion Manager en una agrupación a la vez.

El almacenamiento configurado para la agrupación o host en el que quiere ejecutar las VM convertidas debe cumplir requisitos específicos. Si desea ejecutar las máquinas virtuales recién convertidas en un grupo, sus discos virtuales deben almacenarse en un almacenamiento compartido. Sin embargo, si las máquinas virtuales convertidas se ejecutan en un único host independiente (no en un grupo), sus discos virtuales pueden usar almacenamiento local.

Si desea ejecutar las máquinas virtuales convertidas en un grupo, asegúrese de agregar el almacenamiento compartido al grupo mediante la creación de un repositorio de almacenamiento.

Sistemas operativos invitados compatibles para la conversión:

Puede convertir máquinas virtuales VMware ESXi/vCenter que ejecuten los siguientes sistemas operativos invitados de Windows:

- Windows 10 (64 bits) Enterprise edition
- Edición estándar (escritorio) de Windows Server 2016 (64 bits)
- Edición estándar (escritorio) de Windows Server 2019 (64 bits)
- Edición estándar (escritorio) de Windows Server 2022 (64 bits)

> **Nota:**
>
> Solo se admiten las SKU de Windows que figuran en la lista para la conversión.

También se admiten los siguientes sistemas operativos Linux:

- Red Hat Enterprise Linux 7.9 (64 bits) con la siguiente configuración:
  - Sistema de archivos: EXT3 o EXT4
  - Tipo de partición de arranque: btrfs, lvm o simple
- Red Hat Enterprise Linux 8.x (64 bits) con la siguiente configuración:
  - Sistema de archivos: EXT3 o EXT4
  - Tipo de partición de arranque: lvm o simple
- Ubuntu 20.04 con la siguiente configuración:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Sistema de archivos: EXT3 o EXT4
  - Tipo de partición de arranque: lvm o regular

Para obtener más información sobre los sistemas operativos invitados compatibles con XenServer, consulte Compatibilidad con sistemas operativos invitados.

Cumplir con los requisitos Para convertir máquinas virtuales VMware ESXi/vCenter, el dispositivo virtual XenServer Conversion Manager necesita conectividad a una red física o VLAN que pueda contactar con el servidor VMware. (En las siguientes secciones, esta red se denomina "red VMware").

Si el servidor VMware se encuentra en una red física diferente a la de los hosts del grupo de XenServer, agregue la red a XenServer antes de la conversión.

> **Nota:**
>
> - El tiempo que tardan las máquinas virtuales en convertirse depende de la distancia física entre las redes de VMware y XenServer y también del tamaño del disco virtual de la máquina virtual. Puede estimar cuánto durará la conversión probando el rendimiento de la red entre el servidor VMware y XenServer.
> - De forma predeterminada, XenServer Conversion Manager usa HTTPS para descargar el disco virtual de la máquina virtual durante la conversión de la máquina virtual. Para acelerar el proceso de migración, puede cambiar la ruta de descarga a HTTP. Para obtener más información, consulte el artículo de VMware Cómo mejorar la velocidad de transferencia de tareas con elementos de biblioteca.

Mapee su configuración de red existente El dispositivo virtual XenServer Conversion Manager incluye funciones que pueden reducir la cantidad de configuración de red manual necesaria después de convertir las máquinas virtuales VMware ESXi/vCenter existentes a XenServer. Por ejemplo, el dispositivo virtual XenServer Conversion Manager hará lo siguiente:

- Conserve las direcciones MAC virtuales en las máquinas virtuales VMware ESXi/vCenter y reutilícelas en las máquinas virtuales XenServer resultantes. La conservación de las direcciones MAC asociadas a los adaptadores de red virtuales (direcciones MAC virtuales) puede:
  - Ayudar a preservar las direcciones IP en entornos que utilizan DHCP
  - Ser útil para programas de software cuyas licencias hacen referencia a las direcciones MAC virtuales
- Adaptadores de red de mapas (virtuales). El dispositivo virtual XenServer Conversion Manager puede mapear las redes de VMware a las redes de XenServer para que, una vez convertidas las máquinas virtuales, sus interfaces de red virtual se conecten en consecuencia.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Por ejemplo, si asigna la "Red virtual 4"de VMware a la "Red 0"de XenServer, cualquier máquina virtual de VMware que tuviera un adaptador virtual conectado a la "Red virtual 4"se conectará a la "Red 0"después de la conversión. El dispositivo virtual XenServer Conversion Manager no convierte ni migra ninguna configuración de red del hipervisor. El asistente solo modifica las conexiones de la interfaz de red virtual de una máquina virtual convertida en función de las asignaciones proporcionadas.

> **Nota:**
>
> No necesita mapear todas las redes de VMware a las redes de XenServer correspondientes. Sin embargo, si lo prefiere, puede cambiar las redes que utilizan las máquinas virtuales, reducir o consolidar la cantidad de redes en la nueva configuración de XenServer.

Para aprovechar al máximo estas funciones, recomendamos lo siguiente:

- Antes de instalar XenServer, conecte los hosts a las redes del conmutador (es decir, a los puertos) que desee configurar en el host.
- Asegúrese de que el grupo de XenServer pueda ver las redes que desea que se detecten. En concreto, conecte los hosts de XenServer a los puertos del conmutador que puedan acceder a las mismas redes que el clúster de VMware.

Si bien es más fácil conectar las NIC de XenServer a las mismas redes que las NIC de los hosts de VMware, no es obligatorio. Si desea cambiar la asociación NIC/red, puede conectar una NIC de XenServer a una red física diferente.

Prepárese para los requisitos de red del dispositivo virtual XenServer Conversion Manager Al realizar una conversión, debe crear una conexión de red a la red en la que reside el servidor VMware. El dispositivo virtual XenServer Conversion Manager utiliza esta conexión para el tráfico de conversión entre el host XenServer y el servidor VMware.

Para crear esta conexión de red, debe realizar dos tareas:

- Al importar el dispositivo virtual XenServer Conversion Manager, especifique la red que agregó para el tráfico de conversión como interfaz de red virtual. Puede hacerlo configurando la **interfaz 1** para que se conecte a esa red.
- Antes de ejecutar el asistente de conversión, agregue la red que conecta VMware y XenServer al host de XenServer en el que desea ejecutar las máquinas virtuales convertidas.

De forma predeterminada, al importar el dispositivo virtual XenServer Conversion Manager, XenCenter crea una interfaz de red virtual asociada a Network 0 y NIC0 (eth0). Sin embargo, de forma predeterminada, la configuración de XenServer configura NIC0 como *interfaz de administración, una NIC utilizada para el tráfico de administración*de XenServer. Como resultado, al agregar una red para la

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

conversión, es posible que quiera seleccionar una NIC que no sea NIC0. La selección de otra red puede mejorar el rendimiento en grupos ocupados. Para obtener más información sobre la interfaz de administración, consulte Redes.

Para agregar una red a XenServer:

1. En el panel **Recursos** de XenCenter, seleccione el grupo en el que desea ejecutar el dispositivo virtual XenServer Conversion Manager.
2. Haga clic en la ficha **Redes**.
3. Haga clic en **Agregar red**.
4. En la página **Seleccionar tipo**, seleccione **Red externa** y haga clic en **Siguiente**.
5. En la página **Nombre**, introduzca un nombre significativo para la red (por ejemplo, "Red VMware") y una descripción.
6. En la página **Interfaz**, especifique lo siguiente:
   - **NIC**. La NIC que desea que XenServer utilice para crear la red. Seleccione la NIC que está conectada a la red física o lógica del servidor VMware.
   - **VLAN**. Si la red de VMware es una VLAN, introduzca el ID de la VLAN (o "etiqueta").
   - **MTU**. Si la red de VMware utiliza tramas gigantes, introduzca un valor para la unidad de transmisión máxima (MTU) entre 1500 y 9216. De lo contrario, deje el cuadro MTU con el valor predeterminado de 1500.

     > **Nota:**
     >
     > No active la casilla **Agregar automáticamente esta red a las nuevas máquinas virtuales** .
7. Haga clic en **Finalizar**.

Cumplir con los requisitos Antes de convertir lotes de máquinas virtuales VMware ESXi/vCenter, tenga en cuenta sus requisitos de almacenamiento. Los discos de VM convertidos se almacenan en un repositorio de almacenamiento de XenServer.

Este repositorio de almacenamiento debe ser lo suficientemente grande como para contener los discos virtuales de todas las máquinas virtuales convertidas que quiera ejecutar en ese grupo. Para las máquinas convertidas que solo se ejecutan en un host independiente, puede especificar el almacenamiento local o compartido como la ubicación de los discos virtuales convertidos. Para las máquinas convertidas que se ejecutan en grupos, solo puede especificar el almacenamiento compartido.

Para crear un repositorio de almacenamiento:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. En el panel **Recursos** de XenCenter, seleccione el grupo en el que quiere ejecutar el dispositivo virtual XenServer Conversion Manager.
2. Haga clic en la ficha **Almacenamiento**.
3. Haga clic en **Nueva SR** y siga las instrucciones del asistente. Para obtener más instrucciones, presione **F1** para mostrar la ayuda en línea.

Requisitos de XenServer Puede ejecutar máquinas virtuales convertidas con esta versión de XenServer Conversion Manager en las siguientes versiones de XenServer:

- XenServer 8
- Actualización acumulativa 1 de Citrix Hypervisor 8.2

Requisitos de VMware El dispositivo virtual XenServer Conversion Manager puede convertir máquinas virtuales VMware ESXi/vCenter de las siguientes versiones de VMware:

- vCenter Server 6.7.x, 7.x y 8.x
- vSphere 6.7.x, 7.x y 8.x
- ESXi 6.7.x, 7.x y 8.x

> **Nota:**
>
> El dispositivo virtual XenServer Conversion Manager no puede convertir máquinas virtuales VMware ESXi/vCenter con cuatro o más discos en máquinas virtuales de XenServer. Las máquinas virtuales VMware ESXi/vCenter deben tener tres discos o menos.
>
> Las máquinas virtuales VMware ESXi/vCenter también deben tener una red y un controlador de almacenamiento configurados.

Prepararse para importar el dispositivo virtual Antes de importar el dispositivo virtual, tenga en cuenta la siguiente información y realice los cambios apropiados en su entorno, según corresponda.

Descargue el dispositivo virtual El dispositivo virtual XenServer Conversion Manager está empaquetado en formato XVA. Puede descargar el dispositivo virtual desde la página de descargas de XenServer. Al descargar el archivo, guárdelo en una carpeta del disco duro local (normalmente, pero no necesariamente, en el equipo donde está instalado XenCenter). Una vez que el archivo `.xva` esté en el disco duro, puede importarlo a XenCenter.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Requisitos previos del dispositivo virtual El dispositivo virtual XenServer Conversion Manager requiere un mínimo de:

- Actualización acumulativa 1 de Citrix Hypervisor 8.2, XenServer 8
- Espacio en disco: 30 GB de espacio en disco
- Memoria: 6 GB
- Asignación de CPU virtual: 2 vCPU

Importe y configure el dispositivo virtual

El dispositivo virtual XenServer Conversion Manager es una única máquina virtual preinstalada diseñada para ejecutarse en un host XenServer. Antes de importarlo, revise la información de requisitos previos y las consideraciones en la sección *Preparación para importar el dispositivo virtual*.

Importar el dispositivo virtual a XenServer

Para importar el dispositivo virtual XenServer Conversion Manager al grupo o host en el que quiere ejecutar las máquinas virtuales convertidas, utilice el asistente de importación de XenCenter:

1. Abra XenCenter. Haga clic con el botón derecho en el grupo (o host) en el que quiere importar el paquete del dispositivo virtual y seleccione **Importar**.
2. Navegue para localizar el paquete de dispositivo virtual.
3. Seleccione el grupo o el *servidor doméstico* en el que desee ejecutar el dispositivo virtual XenServer Conversion Manager.

   > **Nota:**
   >
   > Un servidor doméstico es el host que proporciona los recursos para una máquina virtual de un grupo. Si bien puede, un XenServer intenta iniciar la máquina virtual en ese host antes de intentarlo en otros hosts. Si selecciona un host, el dispositivo virtual XenServer Conversion Manager utiliza este host como servidor principal. Si selecciona el grupo, el dispositivo virtual se inicia automáticamente en el host más adecuado de ese grupo.

4. Elija un repositorio de almacenamiento en el que almacenar el disco virtual del dispositivo virtual de XenServer Conversion Manager y, a continuación, **haga clic en**Importar. Para agregar un repositorio de almacenamiento al grupo, consulte la sección “Cumplir con los requisitos de almacenamiento”. “Puede elegir almacenamiento local o compartido.
5. Asegúrese de que la red que se utilizará para la conversión (que conecta el servidor VMware al host XenServer) esté seleccionada como la red asociada a la **interfaz 1** (“NIC virtual 1”).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si la red correcta no aparece junto a la interfaz 1, utilice la lista de la columna **Red** para seleccionar una red diferente.
- Si no ha agregado la red de VMware que está en una red física diferente a la del grupo, haga lo siguiente:

  a) Salga del asistente.
  b) Agregue la red a la agrupación.
  c) Vuelva a ejecutar el asistente.

  Para obtener más información, consulte **Para agregar una red a XenServer**.

  > **Advertencia:**
  >
  > NO configure NIC0 en su red de clientes. Asigne NIC0 solo a "Red de administración interna del host". "

6. Deje activada la casilla de verificación **Iniciar máquina virtual después de la importación** y haga clic en **Finalizar** para importar el dispositivo virtual.
7. Tras importar el `.xva` archivo, el dispositivo virtual XenServer Conversion Manager aparece en **el** panel Recursos de XenCenter.

Configurar el dispositivo virtual XenServer Conversion Manager

Antes de poder usar el dispositivo virtual XenServer Conversion Manager para convertir máquinas virtuales VMware ESXi/vCenter, configúrelo mediante la ficha **Consola** de XenCenter:

1. Tras importar el dispositivo virtual de XenServer Conversion Manager, haga clic en **la** ficha Consola.
2. Lea el acuerdo de licencia. Para ver el contenido del contrato de licencia, abra la URL en un explorador web. Presiona cualquier tecla para continuar.
3. Introduzca y confirme una nueva contraseña raíz para el dispositivo virtual XenServer Conversion Manager. Recomendamos seleccionar una contraseña segura.
4. Introduzca un nombre de host para el dispositivo virtual XenServer Conversion Manager.
5. Introduzca el sufijo de dominio para el dispositivo virtual. Por ejemplo, si el nombre de dominio completo (FQDN) del dispositivo virtual es `citrix-migrate-vm.domain4.example.com`, introduzca `domain4.example.com`.
6. Introduzca **y** para usar DHCP y obtener automáticamente la dirección IP del dispositivo virtual XenServer Conversion Manager. De lo contrario, introduzca **n** y, a continuación, introduzca una dirección IP estática, una máscara de subred y una puerta de enlace para la máquina virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

7. Revise el nombre de host y la configuración de red e introduzca **y** cuando se le solicite. Este paso completa el proceso de configuración del dispositivo virtual XenServer Conversion Manager.
8. Cuando haya configurado correctamente el dispositivo, aparecerá un mensaje de inicio de sesión. Introduzca las credenciales de inicio de sesión y pulse Entrar para iniciar sesión en el dispositivo virtual XenServer Conversion Manager.

Convertir máquinas virtuales VMware ESXi/vCenter

Al convertir máquinas virtuales VMware ESXi/vCenter, se importan al grupo de XenServer o al host independiente donde se ejecuta el dispositivo virtual XenServer Conversion Manager. Las VM convertidas conservan su configuración original de VMware para el procesador virtual y la memoria virtual.

Antes de iniciar el procedimiento de conversión, asegúrese de que se cumple lo siguiente:

- Tiene las credenciales para el grupo de XenServer (o host independiente). Se aceptan las credenciales de la cuenta raíz o una cuenta de control de acceso basado en roles (RBAC) con el rol de administrador del grupo configurado.
- Tiene las credenciales del servidor VMware que contiene las máquinas virtuales que desea convertir. El procedimiento de conversión requiere que conecte la consola de XenServer Conversion Manager al servidor VMware.
- Las máquinas virtuales de VMware que se van a convertir están apagadas.
- Las máquinas virtuales de VMware que se van a convertir tienen una red y un controlador de almacenamiento configurados.
- El grupo (o host) de XenServer que ejecuta las máquinas virtuales convertidas está conectado a un repositorio de almacenamiento. El repositorio de almacenamiento debe contener espacio suficiente para los discos virtuales convertidos.
- Si desea ejecutar las máquinas virtuales recién convertidas en un grupo, el repositorio de almacenamiento debe ser almacenamiento compartido. Sin embargo, si las máquinas virtuales convertidas se ejecutan en un único host independiente (no en un grupo), puede usar almacenamiento local.
- Los discos virtuales de la máquina virtual que se va a convertir son inferiores a 2 TiB.
- El grupo (o host) de XenServer tiene redes que utilizan las máquinas virtuales convertidas.

Para convertir sus máquinas virtuales VMware ESXi/vCenter en máquinas virtuales que puedan ejecutarse en un entorno de XenServer:

1. Asegúrese de que el dispositivo virtual esté instalado y en ejecución en el host o grupo de XenServer al que desee importar las máquinas virtuales.
2. En XenCenter, vaya a **Agrupación** > **Administrador de conversiones**.

   Se abre la ventana **Administrador de conversiones**. Espere mientras el asistente se conecta a su dispositivo virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Haga clic en **Nueva conversión**.
4. En el asistente **Nueva conversión**, introduzca las credenciales para el servidor de VMware:

    - **Servidor**. Introduzca la dirección IP o el FQDN del servidor VMware que contiene las máquinas virtuales que desea convertir a XenServer.
    - **Nombre de usuario**. Introduzca un nombre de usuario válido para este servidor de VMware. Esta cuenta debe ser una cuenta de administrador de VMware o tener una función raíz.
    - **Contraseña**. Introduzca la contraseña de la cuenta de usuario que especificó en el cuadro **Nombre de usuario**.

    Haga clic en **Siguiente**. XenCenter se conecta al servidor de VMware.
5. En la página **Máquinas virtuales**, seleccione de la lista de máquinas virtuales alojadas en el servidor VMware las máquinas virtuales que desea convertir. Haga clic en **Siguiente**.
6. En la página **Almacenamiento**, selecciona el repositorio de almacenamiento que deseas usar durante la conversión. Este repositorio de almacenamiento es donde se almacenan permanentemente las máquinas virtuales y los discos virtuales que está creando.

    Esta ficha indica la proporción de almacenamiento disponible que consumen los discos virtuales de las máquinas virtuales convertidas.
7. En la página **Redes**, para cada red VMware de la lista, seleccione la red de XenServer a la que desea asignarla. También puede seleccionar si desea conservar las direcciones MAC virtuales. Haga clic en **Siguiente**.
8. Revisa las opciones que configuraste para el proceso de conversión. Puede hacer clic en **Anterior** para cambiar estas opciones. Para continuar con la configuración que se muestra, haga clic en **Finalizar**.

    Se inicia el proceso de conversión. La conversión desde ESXi o vSphere puede tardar varios minutos en función del tamaño de los discos vDisk.

    Tras convertir las máquinas virtuales, Conversion Manager se apaga automáticamente por sí solo, lo que ahorra recursos en el host. Para iniciar una máquina virtual, seleccione el host de la máquina virtual y, a continuación, haga clic en **Pool** > **Conversion Manager**.

La ventana **Conversion Manager** muestra las conversiones en curso y las conversiones completadas.

Pasos tras la conversión

Para las máquinas virtuales Windows, debe instalar XenServer VM Tools para Windows. En el caso de las máquinas virtuales Linux, no es necesario instalar XenServer VM Tools for Linux, ya que Conversion Manager las instala automáticamente durante el proceso de conversión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Después de la conversión, en XenCenter, lleve a cabo los siguientes pasos en las máquinas virtuales recién convertidas:

En máquinas Windows:

1. En las máquinas virtuales de Windows, según el modelo de licencia de Microsoft, es posible que deba reactivar la licencia de Windows de la máquina virtual. Esta reactivación se produce porque el sistema operativo Windows percibe la conversión como un cambio de hardware.
2. En las máquinas virtuales de Windows, instale XenServer VM Tools para Windows para obtener E/S de alta velocidad y mejorar el rendimiento del disco y la red. Las herramientas de máquinas virtuales de XenServer para Windows también permiten ciertas funciones y características, como el cierre limpio, el reinicio, la suspensión y la migración en vivo de las máquinas virtuales. Puede descargar XenServer VM Tools para Windows desde la página de descargas de XenServer.

Si trabaja con una máquina virtual que no tiene XenServer VM Tools instalado, aparecerá el mensaje XenServer VM Tools no instalado en la ficha **General** del panel **General**.

> **Nota:**
>
> Las herramientas de máquina virtual de XenServer para Windows deben estar instaladas en cada máquina virtual de Windows para que la máquina virtual tenga una configuración totalmente compatible. Si bien las máquinas virtuales de Windows funcionan sin XenServer VM Tools para Windows, su rendimiento puede verse afectado.

Habilitar VNC en máquinas Linux

En máquinas virtuales Linux, configure el servidor VNC. Para obtener más información, consulte Habilitar VNC para máquinas virtuales Linux.

> **Nota:**
>
> La contraseña de VNC debe tener al menos seis caracteres.

Otras tareas de conversión

La ventana **Administrar conversiones** le permite realizar otras tareas relacionadas con la conversión de máquinas virtuales. Estas tareas incluyen borrar trabajos, guardar un resumen de trabajos, volver a intentar trabajos, cancelar trabajos y mostrar el archivo de registro.

Para borrar todos los trabajos:

1. Seleccione **Borrar todo**.
2. Cuando se le pida que confirme esta acción, haga clic en **Sí** para continuar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para guardar un resumen de trabajos:

1. Haga clic en **Exportar todo**.
2. Especifique dónde quiere guardar el archivo CSV.
3. Haga clic en **Guardar**.

Para volver a intentar un trabajo:

1. Seleccione el trabajo de la lista.
2. Haga clic en **Reintentar**.

> **Nota:**
>
> La opción **Reintentar** solo está habilitada para los trabajos fallidos o cancelados.

Para cancelar un trabajo:

1. Seleccione el trabajo de la lista.
2. Haga clic en **Cancelar**.

> **Nota:**
>
> Cancelar trabajos solo está habilitado para trabajos en cola o en ejecución.

Para guardar el archivo de registro de conversión para un solo trabajo:

1. Seleccione el trabajo de la lista.
2. En el menú de registros, haga clic **en Obtener registro seleccionado**.
3. Especifique dónde quiere guardar el archivo de registro.

Para guardar el archivo de registro de conversión para todos los trabajos:

1. En el menú de registros, haga clic en **Obtener todos los registros**.
2. Especifique dónde quiere guardar el archivo de registro.

Para mostrar los detalles de la conversión:

1. Seleccione el trabajo de la lista.

   La información se muestra en el panel **Detalles**.

---

layout: doc
description: Diagnose and gather information about issues that might arise when using the XenServer Conversion Manager virtual appliance.—

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Solución de problemas de XenServer Conversion Manager

En esta sección se proporciona información sobre la solución de problemas del proceso de conversión y las VM convertidas.

Problemas al iniciar una VM convertida

En general, la conversión se realiza sin problemas y el dispositivo virtual XenServer Conversion Manager convierte las máquinas virtuales sin problemas. Sin embargo, en algunos casos excepcionales, es posible que reciba errores al intentar abrir máquinas virtuales convertidas. En las siguientes secciones se proporciona orientación sobre la resolución de errores y otros problemas.

Pantalla azul con código STOP de Windows 0x0000007B

Este código de parada indica que el dispositivo virtual XenServer Conversion Manager no pudo configurar un dispositivo Windows que es fundamental para arrancar en XenServer por primera vez. Guarda los registros y envíalos al equipo de soporte para obtener más información.

Activación de productos Windows

Según el modelo de licencia, puede aparecer un mensaje de error en la activación del sistema cuando intenta iniciar una VM Windows.

Se ha perdido la configuración de red en una VM Windows

Si importa una máquina virtual Windows desde un servidor ESXi a XenServer, es posible que se pierda la configuración de red IPv4/IPv6. Para conservar la configuración de red, vuelva a configurar la configuración de IPv4/IPv6 después de completar la conversión.

No se puede iniciar el disco SCSI de VMware

Si una máquina virtual de VMware se inicia desde un disco SCSI pero también tiene discos duros IDE configurados, es posible que la máquina virtual no arranque al convertirla a XenServer. Este problema se produce porque el proceso de migración asigna a los discos duros IDE números de dispositivos más bajos que los discos SCSI. Sin embargo, XenServer arranca desde el disco duro asignado al dispositivo 0. Para resolver este problema, reorganice la posición del disco virtual en XenCenter para que la máquina virtual se reinicie desde el disco virtual que contiene el sistema operativo.

Para cambiar la posición del disco virtual que contiene el sistema operativo:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. En el panel **Recursos** de XenCenter, seleccione la máquina virtual invitada apagada.
2. Seleccione la ficha **Almacenamiento**.
3. En la lista **Discos virtuales**, seleccione el disco virtual que contiene el sistema operativo y, a continuación, haga clic en **Propiedades**.
4. En el cuadro de diálogo **Propiedades** del disco virtual, haga clic en la ficha ***vm_name*** para mostrar las opciones del dispositivo.
5. En la lista **Postura del dispositivo**, seleccione **0** y haga clic en **Aceptar**.

Problemas durante la conversión

Si experimenta problemas o errores al convertir máquinas virtuales, intente exportar la máquina virtual de VMware como un paquete OVF. Si no puede exportar la VM de VMware como un paquete OVF, Conversion Manager no puede convertir esta VM. Use los mensajes de error que recibe al intentar exportar la máquina virtual como un paquete OVF para solucionar problemas y solucionar los problemas con su máquina virtual de VMware. Por ejemplo, puede que tenga que configurar una red o un controlador de almacenamiento antes de que la VM se pueda exportar como un paquete OVF o convertirse. Para obtener más información sobre la solución de problemas de las máquinas virtuales VMware ESXi/vCenter, consulte la documentación de VMware.

Si ve algún error al convertir las máquinas virtuales Linux, elimine la máquina virtual convertida, reinicie el dispositivo virtual XenServer Conversion Manager y vuelva a intentarlo.

Los registros de las conversiones fallidas se almacenan en el dispositivo virtual de XenServer Conversion Manager y se pueden recuperar haciendo **clic en Obtener todos los** registros en la ventana de **Conversion Manager** . Cuando te pongas en contacto con el equipo de soporte para plantear cualquier problema, te recomendamos que proporciones el archivo de registro de conversiones y, además, un informe completo del estado del servidor para solucionar problemas. Para obtener más información, consulte Creación de un informe de estado del servidor.

Interfaz de la línea de comandos

April 10, 2024

La CLI *xe* le permite crear scripts y automatizar las tareas de administración del sistema. Use la CLI para integrar XenServer en una infraestructura de TI existente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Introducción a la CLI xe

La interfaz de línea de comandos xe se instala de forma predeterminada en todos los hosts de XenServer. Con XenCenter se incluye una versión remota de Windows. También hay disponible una CLI remota independiente para Linux.

En el host de XenServer

La interfaz de línea de comandos xe se instala de forma predeterminada en el host. Puede ejecutar los comandos de la CLI xe en la consola dom0. Acceda a la consola dom0 de una de las siguientes maneras:

- En XenCenter, vaya a **la ficha Consola del** host en el que quiere ejecutar el comando.
- Utilice SSH en el host en el que quiera ejecutar el comando.

En Windows

En Windows, el comando `xe.exe` se instala junto con XenCenter.

Para usar el comando `xe.exe`, abra un símbolo del sistema de Windows y cambie los directorios al directorio en el que se encuentra el archivo `xe.exe` (normalmente `C:\Program Files (x86)\XenServer\XenCenter`). Si agrega la ubicación de instalación `xe.exe` a la ruta del sistema, puede usar el comando sin tener que cambiar al directorio.

En Linux

En las distribuciones basadas en RPM (como Red Hat), puede instalar el comando xe independiente desde el RPM mencionado `client_install/xapi-xe-BUILD.x86_64.rpm` en la ISO de instalación principal de XenServer.

Para instalar desde el RPM, use el siguiente comando:

```
1 rpm -ivh xapi-xe-BUILD.x86_64.rpm
2 <!--NeedCopy-->
```

Puede usar los parámetros de la línea de comandos para definir el host, el nombre de usuario y la contraseña de XenServer que se utilizarán al ejecutar los comandos xe. Sin embargo, también tiene la opción de establecer esta información como una variable de entorno. Por ejemplo:

```
1 export XE_EXTRA_ARGS="server=<host name>,username=<user name>,password
     =<password>"
2 <!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> La CLI xe remota en Linux puede bloquearse al intentar ejecutar comandos a través de una conexión segura y estos comandos implican la transferencia de archivos. Si es así, puede usar el `--no-ssl` parámetro para ejecutar el comando a través de una conexión insegura con el host de XenServer.

Obtener ayuda con los comandos xe

La ayuda básica está disponible para los comandos de CLI en el host escribiendo lo siguiente:

```
xe help command
<!--NeedCopy-->
```

Se muestra una lista de los comandos xe más utilizados si escribe:

```
xe help
<!--NeedCopy-->
```

O se muestra una lista de todos los comandos xe si escribe:

```
xe help --all
<!--NeedCopy-->
```

Sintaxis xe básica

La sintaxis básica de todos los comandos de la CLI de XenServer xe es:

```
xe command-name argument=value argument=value
<!--NeedCopy-->
```

Cada comando específico contiene su propio conjunto de argumentos que tienen la forma `argument=value`. Algunos comandos tienen argumentos requeridos y la mayoría tienen algún conjunto de argumentos opcionales. Normalmente, un comando asume valores predeterminados para algunos de los argumentos opcionales cuando se invoca sin ellos.

Si el comando xe se ejecuta de forma remota, se usan argumentos adicionales para conectarse y autenticarse. Estos argumentos también toman la forma `argument=argument_value`.

El argumento `server` se usa para especificar el nombre de host o la dirección IP. Los argumentos `username` y `password` se utilizan para especificar las credenciales.

Se puede especificar un argumento `password-file` en lugar de la contraseña directamente. En este caso, el comando xe intenta leer la contraseña del archivo especificado y usa esa contraseña para conectarse. (Todos los CR y LF finales al final del archivo se eliminan). Este método es más seguro que especificar la contraseña directamente en la línea de comandos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El `port` argumento opcional se puede usar para especificar el puerto del agente en el host remoto de XenServer (el valor predeterminado es 443).

Ejemplo: En el host local de XenServer:

```
xe vm-list
<!--NeedCopy-->
```

Ejemplo: En un host remoto de XenServer:

```
xe vm-list username=username password=password server=hostname
<!--NeedCopy-->
```

La sintaxis abreviada también está disponible para los argumentos de conexión remota:

- `-u` nombre de usuario
- `-pw` contraseña
- `-pwf` archivo de contraseñas
- Puerto `-p`
- `-s` servidor

Ejemplo: En un host remoto de XenServer:

```
xe vm-list -u myuser -pw mypassword -s hostname
<!--NeedCopy-->
```

Los argumentos también se toman de la variable de entorno XE_EXTRA_ARGS, en forma de pares clave/valor separados por comas. Por ejemplo, para introducir comandos que se ejecutan en un host XenServer remoto, ejecute primero el siguiente comando:

```
export XE_EXTRA_ARGS="server=jeffbeck,port=443,username=root,password=
    pass"
<!--NeedCopy-->
```

Tras ejecutar este comando, ya no es necesario especificar los parámetros del host remoto de XenServer en cada comando xe que ejecute.

El uso de la variable de entorno XE_EXTRA_ARGS también permite completar con fichas los comandos xe cuando se ejecutan en un host XenServer remoto, lo que está inhabilitado de forma predeterminada.

Caracteres especiales y sintaxis

Para especificar pares argumento/valor en la línea de comandos `xe`, escriba: `argument=value`

A menos que el valor incluya espacios, no use comillas. No incluya espacios en blanco entre el nombre del argumento, el signo igual (=) y el valor. Cualquier argumento que no se ajuste a este formato se ignora.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para los valores que contienen espacios, escriba: `argument="value with spaces"`

Cuando usa la CLI en el host de XenServer, los comandos tienen una función de finalización de fichas similar a la función del shell bash estándar de Linux. Por ejemplo, si escribe `xe vm-l` y, a continuación, pulsa la tecla **TAB**, se mostrará el resto del comando. Si comienza con más de un comando `vm-l`, al presionar **TAB** por segunda vez se muestran las posibilidades. Esta función es útil cuando se especifican los UUID de objetos en los comandos.

> **Nota:**
>
> La finalización de tabulaciones normalmente no funciona cuando se ejecutan comandos en un host XenServer remoto. Sin embargo, si establece la variable XE_EXTRA_ARGS en la máquina en la que introduce los comandos, se habilita la finalización de tabulaciones. Para obtener más información, consulte Sintaxis xe básica.

Tipos de comandos

Los comandos de la CLI se pueden dividir en dos mitades. Los comandos de bajo nivel se ocupan de la manipulación de listas y parámetros de los objetos de la API. Los comandos de nivel superior se utilizan para interactuar con máquinas virtuales o hosts en un nivel más abstracto.

Los comandos de bajo nivel son:

- *class*-list
- *clase*-param-get
- *clase*-param-set
- *class*-param-list
- *clase*-param-add
- *clase*-param-remove
- *clase*-param-clear

Donde *class* es una de las siguientes:

- `bond`
- `console`
- `host`
- `host-crashdump`
- `host-cpu`
- `network`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- patch
- pbd
- pif
- pool
- sm
- sr
- task
- template
- vbd
- vdi
- vif
- vlan
- vm

No todos los valores de *class* tienen el conjunto completo de comandos *class*-param-*action*. Algunos valores de *class* tienen un conjunto de comandos más pequeño.

Tipos de parámetros

Los objetos que se abordan con los comandos xe tienen conjuntos de parámetros que los identifican y definen sus estados.

La mayoría de los parámetros toman un solo valor. Por ejemplo, el parámetro `name-label` de una máquina virtual contiene un único valor de cadena. En la salida de los comandos de la lista de parámetros `xe vm-param-list`, como un valor entre paréntesis, indica si los parámetros son de lectura y escritura (RW) o de solo lectura (RO).
El resultado de `xe vm-param-list` en una máquina virtual especificada puede tener las siguientes líneas:

```
user-version ( RW): 1
 is-control-domain ( RO): false
```

En el primer parámetro, `user-version`, se puede escribir, y tiene el valor 1. El segundo, `is-control-domain`, es de solo lectura y tiene el valor false.

Los otros dos tipos de parámetros tienen varios valores. Un parámetro *set* contiene una lista de valores. Un parámetro de *mapa* es un conjunto de pares clave/valor. Como ejemplo, observe la siguiente parte de la salida de muestra de `xe vm-param-list` en una máquina virtual especificada:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
platform (MRW): acpi: true; apic: true; pae: true; nx: false
allowed-operations (SRO): pause; clean_shutdown; clean_reboot; \
hard_shutdown; hard_reboot; suspend
```

El parámetro `platform` tiene una lista de elementos que representan pares clave/valor. Los nombres de las claves van seguidos de un carácter de dos puntos (:). Cada par clave/valor está separado del siguiente por un carácter de punto y coma (;). La M que precede a la RW indica que este parámetro es un parámetro de mapa y se puede leer y escribir. El parámetro `allowed-operations` tiene una lista que constituye un conjunto de elementos. La S que precede al RO indica que este es un parámetro establecido y es legible pero no escribible.

Para filtrar por un parámetro de mapa o establecer un parámetro de mapa, utilice dos puntos (:) para separar el nombre del parámetro de mapa y el par clave/valor. Por ejemplo, para establecer el valor de la clave `foo` del parámetro `other-config` de una VM en `baa`, el comando sería

```
xe vm-param-set uuid=VM uuid other-config:foo=baa
<!--NeedCopy-->
```

Comandos de parámetros de bajo nivel

Hay varios comandos para operar en parámetros de objetos: *class*-param-get, *class*-param-set, *class*-param-add, *class*-param-remove, *class*-param-clear y *class*-param-list. Cada uno de estos comandos toma un parámetro `uuid` para especificar el objeto en particular. Como estos comandos se consideran comandos de bajo nivel, deben usar el UUID y no la etiqueta del nombre de la máquina virtual.

- `xe class-param-list uuid=uuid`

  Enumera todos los parámetros y sus valores asociados. A diferencia del comando *class*-list, este comando enumera los valores de los campos "caros".

- `xe class-param-get uuid=uuid param-name=parameter param-key=key`

  Devuelve el valor de un parámetro en particular. Para un parámetro de mapa, al especificar la clave de parámetro se obtiene el valor asociado a esa clave en el mapa. Si no se especifica param-key o si el parámetro es un conjunto, el comando devuelve una representación de cadena del conjunto o el mapa.

- `xe class-param-set uuid=uuid param=value`

  Establece el valor de uno o más parámetros.

- `xe class-param-add uuid=uuid param-name=parameter key=value param-key=key`

  Se agrega a un mapa o a un parámetro establecido. Para un parámetro de mapa, agregue pares clave/valor mediante la sintaxis key=value. Si el parámetro es un conjunto, agregue claves con

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

la sintaxis param-key=key.

- `xe class-param-remove uuid=uuid param-name=parameter param-key=key`

  Elimina un par clave/valor de un mapa o una clave de un conjunto.

- `xe class-param-clear uuid=uuid param-name=parameter`

  Borra completamente un conjunto o un mapa.

Comandos de lista de bajo nivel

El comando *class*-list enumera los objetos de tipo *class*. De forma predeterminada, este tipo de comando enumera todos los objetos e imprime un subconjunto de los parámetros. Este comportamiento se puede modificar de las siguientes maneras:

- Puede filtrar los objetos para que solo genere un subconjunto
- Los parámetros que se imprimen se pueden modificar.

Para cambiar los parámetros que se imprimen, especifique los *parámetros del argumento* como una lista separada por comas de los parámetros requeridos. Por ejemplo:

```
xe vm-list params=name-label,other-config
<!--NeedCopy-->
```

Como alternativa, para enumerar todos los parámetros, use la sintaxis:

```
xe vm-list params=all
<!--NeedCopy-->
```

El comando list no muestra algunos parámetros que sean costosos de calcular. Estos parámetros se muestran, por ejemplo:

```
allowed-VBD-devices (SRO): <expensive field>
<!--NeedCopy-->
```

Para obtener estos campos, use el comando *class*-param-list o *class*-param-get.

Para filtrar la lista, la CLI hace coincidir los valores de los parámetros con los valores especificados en la línea de comandos, imprimiendo solo los objetos que coinciden con todas las restricciones especificadas. Por ejemplo:

```
xe vm-list HVM-boot-policy="BIOS order" power-state=halted
<!--NeedCopy-->
```

Este comando enumera solo las máquinas virtuales para las que los *dos* campos, tanto `power-state` como `HVM-boot-policy`, tengan los valores *detenido* y *orden de BIOS* respectivamente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

También puede filtrar la lista por el valor de las claves en los mapas o por la existencia de valores en un conjunto. La sintaxis para filtrar en función de las claves en los mapas es `map-name:key=value`. La sintaxis para filtrar en función de los valores existentes en un conjunto es `set-name:contains=value`.

Al crear scripts, una técnica útil es pasar `--minimal` en la línea de comandos, lo que hace que `xe` se imprima solo el primer campo de una lista separada por comas. Por ejemplo, el comando `xe vm-list --minimal` en un host con tres VM instaladas proporciona los tres UUID de las VM:

```
    a85d6717-7264-d00e-069b-3b1d19d56ad9,aaa3eec5-9499-bcf3-4c03-
       af10baea96b7, \
    42c044de-df69-4b30-89d9-2c199564581d
<!--NeedCopy-->
```

Secretos

XenServer proporciona un mecanismo de secretos para evitar que las contraseñas se almacenen en texto sin formato en el historial de la línea de comandos o en objetos de la API. XenCenter usa esta función automáticamente y también se puede usar desde la CLI xe para cualquier comando que requiera una contraseña.

> **Nota:**
>
> Los secretos de contraseña no se pueden usar para autenticarse en un host de XenServer desde una instancia remota de la CLI xe.

Para crear un objeto secreto, ejecute el siguiente comando en el host de XenServer.

```
xe secret-create value=my-password
<!--NeedCopy-->
```

Se crea un secreto y se almacena en el host de XenServer. El comando genera el UUID del objeto secreto. Por ejemplo, `99945d96-5890-de2a-3899-8c04ef2521db`. Adjunte `_secret` al nombre del argumento password para pasar este UUID a cualquier comando que requiera una contraseña.

Ejemplo: En el host de XenServer en el que creó el secreto, puede ejecutar el siguiente comando:

```
    xe sr-create device-config:location=sr_address device-config:type=
       cifs device-config:username=cifs_username  \
    device-config:cifspassword_secret=secret_uuid name-label="CIFS ISO
       SR" type="iso" content-type="iso" shared="true"
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Historial de comandos

Algunos comandos xe, por ejemplo, `xe vm-migrate` o `xe pool-enable-external-auth`, toman secretos como contraseñas como parámetros. Estos pueden terminar en el historial del shell y, durante la ejecución del comando, son visibles en la tabla de procesos. Por lo tanto, es importante ejecutar estos comandos solo en entornos confiables.

Para el shell bash, puede usar la variable `HISTCONTROL` para controlar qué comandos se almacenan en el historial del shell.

referencia de comandos xe

En esta sección se agrupan los comandos por los objetos a los que se dirige el comando. Estos objetos se enumeran alfabéticamente.

Comandos del dispositivo

Comandos para crear y modificar dispositivos de VM (también conocidos como vApps). Para obtener más información, consulte vApps.

Parámetros del dispositivo

Los comandos del dispositivo tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
`uuid`	El uuid del dispositivo	Si son necesarias
`name-description`	La descripción del dispositivo	Opcional
`paused`		Opcional
`force`	Forzar el cierre	Opcional

`appliance-assert-can-be-recovered`

```
1 xe appliance-assert-can-be-recovered uuid=appliance-uuid database:vdi-
     uuid=vdi-uuid
2 <!--NeedCopy-->
```

Comprueba si hay almacenamiento disponible para recuperar este dispositivo de VM o vApp.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

appliance-create

```
xe appliance-create name-label=name-label [name-description=name-
    description]
<!--NeedCopy-->
```

Crea un dispositivo/vApp. Por ejemplo:

```
xe appliance-create name-label=my_appliance
<!--NeedCopy-->
```

Agregue máquinas virtuales al dispositivo:

```
xe vm-param-set uuid=VM-UUID appliance=appliance-uuid
<!--NeedCopy-->
```

appliance-destroy

```
xe appliance-destroy uuid=appliance-uuid
<!--NeedCopy-->
```

Destruye un dispositivo/vApp. Por ejemplo:

```
xe appliance-destroy uuid=appliance-uuid
<!--NeedCopy-->
```

appliance-recover

```
xe appliance-recover uuid=appliance-uuid database:vdi-uuid=vdi-uuid [
    paused=true|false]
<!--NeedCopy-->
```

Recupere una VM Appliance/vApp de la base de datos contenida en la VDI suministrada.

appliance-shutdown

```
xe appliance-shutdown uuid=appliance-uuid [force=true|false]
<!--NeedCopy-->
```

Apaga todas las máquinas virtuales de un dispositivo/vApp. Por ejemplo:

```
xe appliance-shutdown uuid=appliance-uuid
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

appliance-start

```
xe appliance-start uuid=appliance-uuid [paused=true|false]
<!--NeedCopy-->
```

Inicia un dispositivo/vApp. Por ejemplo:

```
xe appliance-start uuid=appliance-uuid
<!--NeedCopy-->
```

Comandos de auditoría

Los comandos de auditoría descargan todos los registros disponibles del archivo de auditoría RBAC en el grupo. Si el parámetro opcional `since` está presente, solo descarga los registros de ese punto específico en el tiempo.

Parámetros de audit-log-get

`audit-log-get` tiene los siguientes parámetros

Nombre del parámetro	Descripción	Tipo
`filename`	Escribir el registro de auditoría del grupo en el *nombre del archivo*	Si son necesarias
`since`	Punto de fecha/hora específico	Opcional

audit-log-get

```
xe audit-log-get [since=timestamp] filename=filename
<!--NeedCopy-->
```

Por ejemplo, para obtener registros de auditoría del grupo desde una marca de tiempo precisa en milisegundos, ejecute el siguiente comando:

Ejecute este comando:

```
xe audit-log-get since=2009-09-24T17:56:20.530Z filename=/tmp/auditlog-
    pool-actions.out
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Comandos de unión

Comandos para trabajar con vínculos de red, para la resiliencia con conmutación por error de interfaz física. Para obtener más información, consulte Redes.

El objeto de unión es un objeto de referencia que pega entre sí las PIF *maestras* y *miembros*. El PIF maestro es la interfaz de unión que debe usarse como el PIF general para referirse a la unión. Los PIF miembros son un conjunto de dos o más interfaces físicas que se han combinado en la interfaz enlazada de alto nivel.

Parámetros de vínculos

Los vínculos tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
`uuid`	Referencia de identificador/objeto única para el vínculo	Solo lectura
`master`	UUID para el bono principal (PIF)	Solo lectura
`members`	Conjunto de UUID para los PIF enlazados subyacentes	Solo lectura

bond-create

```
xe bond-create network-uuid=network_uuid pif-uuids=pif_uuid_1,
   pif_uuid_2,...
<!--NeedCopy-->
```

Cree una interfaz de red enlazada en la red especificada a partir de una lista de objetos PIF existentes. El comando falla en cualquiera de los siguientes casos:

- Si los PIF ya están en otro vínculo
- Si algún miembro tiene una etiqueta de VLAN configurada
- Si los PIF a los que se hace referencia no están en el mismo host de XenServer
- Si se suministran menos de 2 PIF

bond-destroy

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe bond-destroy uuid=bond_uuid
<!--NeedCopy-->
```

Elimina una interfaz enlazada especificada por su UUID de un host.

bond-set-mode

```
xe bond-set-mode uuid=bond_uuid mode=bond_mode
<!--NeedCopy-->
```

Cambia el modo de enlace.

Comandos de CD

Comandos para trabajar con unidades físicas de CD/DVD en hosts XenServer.

Parámetros de CD

Los CD tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
uuid	Referencia única de identificador/objeto para el CD	Solo lectura
name-**label**	Nombre del CD	Lectura/Escritura
name-description	Texto descriptivo del CD	Lectura/Escritura
allowed-operations	Una lista de las operaciones que se pueden realizar en este CD	Parámetro de conjunto de solo lectura
current-operations	Una lista de las operaciones que están actualmente en curso en este CD	Parámetro de conjunto de solo lectura
sr-uuid	La referencia única de identificador/objeto para la SR de la que forma parte este CD	Solo lectura
sr-name-**label**	El nombre de la SR de la que forma parte este CD	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
vbd-uuids	Una lista de los identificadores únicos para los VBD de las VM que se conectan a este CD	Parámetro de conjunto de solo lectura
crashdump-uuids	No se usa en CD. Porque los volcados de memoria no se pueden escribir en CD	Parámetro de conjunto de solo lectura
virtual-size	Tamaño del CD tal como aparece en las máquinas virtuales (en bytes)	Solo lectura
physical-utilisation	Cantidad de espacio físico que ocupa la imagen de CD en el SR (en bytes)	Solo lectura
type	Definir como Usuario para CD	Solo lectura
sharable	Indica si la unidad de CD se puede compartir o no. El valor predeterminado es **false**.	Solo lectura
read-only	Indica si el CD es de solo lectura **false**, si es posible escribir en el dispositivo. Siempre es cierto para los CD.	Solo lectura
storage-lock	El valor es **true** si este disco está bloqueado en el nivel de almacenamiento.	Solo lectura
parent	Referencia al disco principal, si este CD forma parte de una cadena.	Solo lectura
missing	El valor es **true** si la operación de escaneo SR informó que este CD no está presente en el disco	Solo lectura
other-config	Una lista de pares clave/valor que especifican parámetros de configuración adicionales para el CD	Parámetro de mapa de lectura y escritura
location	La ruta en la que se monta el dispositivo	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
managed	El valor es **true** si el dispositivo está administrado	Solo lectura
xenstore-data	Datos que se insertarán en el árbol xenstore	Parámetro de mapa de solo lectura
sm-config	Nombres y descripciones de las claves de configuración del dispositivo del administrador de almacenamiento	Parámetro de mapa de solo lectura
is-a-snapshot	El valor es **true** si esta plantilla es una instantánea de CD	Solo lectura
snapshot_of	El UUID del CD del que esta plantilla es una instantánea	Solo lectura
snapshots	Los UUID de cualquier instantánea que se haya tomado de este CD	Solo lectura
snapshot_time	La marca de tiempo de la operación de instantánea	Solo lectura

cd-list

```
xe cd-list [params=param1,param2,...] [parameter=parameter_value]
<!--NeedCopy-->
```

Enumere los CD e ISO (archivos de imagen de CD) del host o grupo de XenServer, filtrando según el argumento opcional. params

Si se usa el argumento opcional params, el valor de params es una cadena que contiene una lista de parámetros de este objeto que quiere mostrar. Como alternativa, puede usar la palabra clave all para mostrar todos los parámetros. Cuando params no se usa, la lista devuelta muestra un subconjunto predeterminado de todos los parámetros disponibles.

Los argumentos opcionales pueden ser cualquier número de los parámetros de CD enumerados al principio de esta sección.

Comandos de clúster

Comandos para trabajar con grupos agrupados.

Los grupos agrupados son grupos de recursos que tienen habilitada la función de agrupación en

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

clústeres. Use estas agrupaciones con SR de GFS2. Para obtener más información, consulte Grupos agrupados

Los objetos cluster y cluster-host se pueden enumerar con los comandos de listado de objetos estándar (`xe cluster-list` y `xe cluster-host-list`) y los parámetros manipulados con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel.
Comandos para trabajar con grupos agrupados.

Parámetros de clúster

Los clústeres tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
`uuid`	La referencia de identificador/objeto única para el clúster	Solo lectura
`cluster-hosts`	Una lista de referencias de identificadores/objetos únicos para los hosts del clúster	Parámetro de conjunto de solo lectura
`cluster-token`	La clave secreta que usa `xapi-clusterd` cuando habla consigo misma en otros hosts	Solo lectura
`cluster-stack`	La pila de tecnología que proporciona las capacidades de agrupación en clústeres. Los valores posibles son `corosync`.	Solo lectura
`allowed-operations`	Enumera las operaciones permitidas en este estado. Esta lista es solo de carácter consultivo y el estado del clúster puede haber cambiado en el momento en que un cliente lee este campo.	Parámetro de conjunto de solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
current-operations	Enumera las operaciones en curso en ese momento. Esta lista es solo de carácter consultivo y el estado del clúster puede haber cambiado en el momento en que un cliente lee este campo.	Parámetro de conjunto de solo lectura
token-timeout	El tiempo de espera del token corosync en segundos	Solo lectura
token-timeout-coefficient	El coeficiente de tiempo de espera del token corosync en segundos	Solo lectura
pool-auto-join	True si se unen automáticamente nuevos miembros del grupo al clúster. Esto está configurado para **true**.	Solo lectura
cluster-config	Una lista de pares clave/valor que especifican parámetros de configuración adicionales para el clúster.	Parámetro de mapa de solo lectura
other-config	Una lista de pares clave/valor que especifican parámetros de configuración adicionales para el clúster.	Parámetro de mapa de lectura y escritura

cluster-host-destroy

```
xe cluster-host-destroy uuid=host_uuid
<!--NeedCopy-->
```

Destruye un host de clúster y abandona el clúster de manera efectiva

cluster-host-disable

```
xe cluster-host-disable uuid=cluster_uuid
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Inhabilite la pertenencia al clúster para un host de clúster habilitado.

cluster-host-enable

```
xe cluster-host-enable uuid=cluster_uuid
<!--NeedCopy-->
```

Habilite la pertenencia al clúster para un host de clúster inhabilitado.

cluster-host-force-destroy

```
xe cluster-host-force-destroy uuid=cluster_host
<!--NeedCopy-->
```

Destruya un objeto host de clúster con fuerza y abandone el clúster de manera efectiva.

cluster-pool-create

```
xe cluster-pool-create network-uuid=network_uuid [cluster-stack=
    cluster_stack] [token-timeout=token_timeout] [token-timeout-
    coefficient=token_timeout_coefficient]
<!--NeedCopy-->
```

Cree un clúster para todo el grupo.

cluster-pool-destroy

```
xe cluster-pool-destroy cluster-uuid=cluster_uuid
<!--NeedCopy-->
```

Destruya el clúster de todo el grupo El grupo sigue existiendo, pero ya no está agrupado en clústeres y ya no puede usar SR de GFS2.

cluster-pool-force-destroy

```
xe cluster-pool-force-destroy cluster-uuid=cluster_uuid
<!--NeedCopy-->
```

Fuerce la destrucción del clúster de todo el grupo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

cluster-pool-resync

```
xe cluster-pool-resync cluster-uuid=cluster_uuid
<!--NeedCopy-->
```

Vuelva a sincronizar un clúster en un grupo.

Comandos de consola

Comandos para trabajar con consolas.

Los objetos de consola se pueden enumerar con el comando estándar de listado de objetos (`xe console-list`) y los parámetros manipulados con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel.

Parámetros de consola

Las consolas tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
`uuid`	La referencia de identificador/objeto única para la consola	Solo lectura
`vm-uuid`	La referencia única de identificador/objeto de la máquina virtual en la que está abierta esta consola	Solo lectura
`vm-name-label`	El nombre de la máquina virtual en la que está abierta esta consola	Solo lectura
`protocol`	Protocolo que usa esta consola. Los valores posibles son `vt100`: terminal VT100, `rfb`: Protocolo de búfer de cuadro remoto (como se usa en VNC) o `rdp`: Protocolo de escritorio remoto	Solo lectura
`location`	URI para el servicio de consola	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
other-config	Una lista de pares clave/valor que especifican parámetros de configuración adicionales para la consola.	Parámetro de mapa de lectura y escritura

console

```
xe console
<!--NeedCopy-->
```

Se conecta a una consola en particular.

Comandos de diagnóstico

Comandos para recopilar información de diagnóstico de XenServer.

diagnostic-compact

```
xe diagnostic-compact
<!--NeedCopy-->
```

Realice una recolección de GC importante y una compactación de pilas.

diagnostic-db-stats

```
xe diagnostic-db-stats
<!--NeedCopy-->
```

Imprimir estadísticas de bases de datos.

diagnostic-gc-stats

```
xe diagnostic-gc-stats
<!--NeedCopy-->
```

Imprime las estadísticas de GC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

diagnostic-license-status

```
xe diagnostic-license-status
<!--NeedCopy-->
```

Ayude a diagnosticar problemas de licencias en todo el grupo.

diagnostic-net-stats

```
xe diagnostic-net-stats [uri=uri] [method=method] [params=param1,param2
    ...]
<!--NeedCopy-->
```

Imprime estadísticas de red.

diagnostic-timing-stats

```
xe diagnostic-timing-stats
<!--NeedCopy-->
```

Estadísticas de tiempo de impresión.

diagnostic-vdi-status

```
xe diagnostic-vdi-status uuid=vdi_uuid
<!--NeedCopy-->
```

Consulte el estado de bloqueo y uso compartido de una VDI.

diagnostic-vm-status

```
xe diagnostic-vm-status uuid=vm_uuid
<!--NeedCopy-->
```

Consulte los hosts en los que la VM puede arrancar y compruebe el estado de compartición/bloqueo de todos los VBD.

Comandos de recuperación ante

Comandos para recuperar máquinas virtuales después de un desastre

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

drtask-create

```
xe drtask-create type=type sr-whitelist=sr-white-list device-config=
    device-config
<!--NeedCopy-->
```

Crea una tarea de recuperación ante desastres. Por ejemplo, para conectarse a una SR iSCSI en preparación para la recuperación ante desastres:

```
xe drtask-create type=lvmoiscsi device-config:target=target-ip-address
    \
     device-config:targetIQN=targetIQN device-config:SCSIid=SCSIid \
     sr-whitelist=sr-uuid-list
<!--NeedCopy-->
```

> **Nota:**
>
> El comando `sr-whitelist` enumera los UUID de SR que están permitidos. El comando `drtask-create` solo introduce y se conecta a un SR que tiene uno de los UUID permitidos

drtask-destroy

```
xe drtask-destroy uuid=dr-task-uuid
<!--NeedCopy-->
```

Destruye una tarea de recuperación ante desastres y olvida la SR introducida.

vm-assert-can-be-recovered

```
xe vm-assert-can-be-recovered uuid=vm-uuid database:vdi-uuid=vdi-uuid
<!--NeedCopy-->
```

Comprueba si hay almacenamiento disponible para recuperar esta VM.

appliance-assert-can-be-recovered

```
xe appliance-assert-can-be-recovered uuid=appliance-uuid database:vdi-
    uuid=vdi-uuid
<!--NeedCopy-->
```

Comprueba si el almacenamiento (que contiene el disco de vApp o del dispositivo) está visible.

appliance-recover

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe appliance-recover uuid=appliance-uuid database:vdi-uuid=vdi-uuid [
    force=true|false]
<!--NeedCopy-->
```

Recupere un dispositivo/vApp de la base de datos contenida en la VDI suministrada.

vm-recover

```
xe vm-recover uuid=vm-uuid database:vdi-uuid=vdi-uuid [force=true|false
    ]
<!--NeedCopy-->
```

Recupera una VM de la base de datos contenida en la VDI suministrada.

sr-enable-database-replication

```
xe sr-enable-database-replication uuid=sr_uuid
<!--NeedCopy-->
```

Permite la replicación de base de datos XAPI en el SR especificado (compartido).

sr-disable-database-replication

```
xe sr-disable-database-replication uuid=sr_uuid
<!--NeedCopy-->
```

Inhabilita la replicación de base de datos XAPI en el SR especificado.

Uso de ejemplo

El siguiente ejemplo muestra los comandos de la CLI de DR en contexto:

En el sitio principal, habilite la replicación de base de datos:

```
xe sr-database-replication uuid=sr=uuid
<!--NeedCopy-->
```

Después de un desastre, en el sitio secundario, conéctese al SR. El comando `device-config` tiene los mismos campos que `sr-probe`.

```
xe drtask-create type=lvmoiscsi \
    device-config:target=target ip address \
    device-config:targetIQN=target-iqn \
    device-config:SCSIid=scsi-id \
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    sr-whitelist=sr-uuid
<!--NeedCopy-->
```

Busque los VDI de base de datos en el SR:

```
xe vdi-list sr-uuid=sr-uuid type=Metadata
<!--NeedCopy-->
```

Consulte una VDI de base de datos para las máquinas virtuales presentes:

```
xe vm-list database:vdi-uuid=vdi-uuid
<!--NeedCopy-->
```

Recuperar una VM:

```
xe vm-recover uuid=vm-uuid database:vdi-uuid=vdi-uuid
<!--NeedCopy-->
```

Destruye la tarea de DR. Se destruyen todos los SR introducidos por la tarea de DR y que no sean requeridos por las VM:

```
xe drtask-destroy uuid=drtask-uuid
<!--NeedCopy-->
```

Comandos de eventos

Comandos para trabajar con eventos.

Clases de eventos

Las clases de eventos se enumeran en la siguiente tabla:

Nombre de la clase	Descripción
pool	Un conjunto de hosts físicos
vm	Una máquina virtual
host	Un host físico
network	Una red virtual
vif	Una interfaz de red virtual
pif	Una interfaz de red física (las VLAN separadas se representan como varios PIF)
sr	Un repositorio de almacenamiento

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre de la clase	Descripción
vdi	Una imagen de disco virtual
vbd	Un dispositivo de bloques virtual
pbd	Los dispositivos de bloques físicos a través de los cuales los hosts acceden

event-wait

```
xe event-wait class=class_name [param-name=param_value] [param-name=/=
    param_value]
<!--NeedCopy-->
```

Impide la ejecución de otros comandos hasta que exista un objeto que cumpla las condiciones dadas en la línea de comandos. El argumento `x=y` significa "esperar a que el campo x tome el valor y", y `x=/=y` significa "esperar a que el campo x tome cualquier valor que no sea y".

Ejemplo: espere a que se ejecute una VM específica.

```
xe event-wait class=vm name-label=myvm power-state=running
<!--NeedCopy-->
```

Bloquea otros comandos hasta que una máquina virtual llamada `myvm` tenga el estado `power-state` "activo".

Ejemplo: espere a que se reinicie una VM específica:

```
xe event-wait class=vm uuid=$VM start-time=/=$(xe vm-list uuid=$VM
    params=start-time --minimal)
<!--NeedCopy-->
```

Bloquea otros comandos hasta que se reinicie una VM con UUID *$VM*. El comando usa el valor de `start-time` para decidir cuándo se reinicia la VM.

El nombre de la clase puede ser cualquiera de las clases de eventos que se enumeran al principio de esta sección. Los parámetros pueden ser cualquiera de los parámetros enumerados en el comando de la CLI *class*-param-list.

Comandos de GPU

Comandos para trabajar con GPU físicas, grupos de GPU y GPU virtuales.

Los objetos de GPU se pueden enumerar con los comandos de lista de objetos estándar: `xe pgpu-list`, `xe gpu-group-list` y `xe vgpu-list`. Los parámetros se pueden manipular con los

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel.

Parámetros de GPU física

Las GPU físicas (PGPU) tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
`uuid`	La referencia única de identificador/objeto para la PGPU	Solo lectura
`vendor-name`	El nombre del proveedor de la PGPU	Solo lectura
`device-name`	El nombre asignado por el proveedor a este modelo de PGPU	Solo lectura
`gpu-group-uuid`	La referencia única de identificador/objeto para el grupo de GPU al que XenServer ha asignado automáticamente esta PGPU. Las PGPU idénticas en todos los hosts de un grupo se agrupan	Solo lectura
`gpu-group-name-label`	El nombre del grupo de GPU al que se asigna la PGPU	Solo lectura
`host-uuid`	La referencia única de identificador/objeto para el host de XenServer al que está conectada la PGPU	Solo lectura
`host-name-label`	El nombre del host de XenServer al que está conectada la PGPU	Solo lectura
`pci-id`	Identificador de PCI	Solo lectura
`dependencies`	Enumera los dispositivos PCI dependientes que se han pasado a la misma VM	Parámetro de mapa de lectura y escritura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
other-config	Una lista de pares clave/valor que especifican parámetros de configuración adicionales para la PGPU	Parámetro de mapa de lectura y escritura
supported-VGPU-types	Lista de tipos de GPU virtuales compatibles con el hardware subyacente	Solo lectura
enabled-VGPU-types	Lista de tipos de GPU virtuales que se han habilitado para esta PGPU	Lectura/escritura
resident-VGPUs	Lista de vGPU que se ejecutan en esta PGPU	Solo lectura

pgpu-disable-dom0-access

```
xe pgpu-disable-dom0-access uuid=uuid
<!--NeedCopy-->
```

Desactiva el acceso de la PGPU a dom0.

pgpu-enable-dom0-access

```
xe pgpu-enable-dom0-access uuid=uuid
<!--NeedCopy-->
```

Habilite el acceso de la PGPU a dom0.

Parámetros del grupo de GPU

Los grupos de GPU tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
uuid	La referencia única de identificador/objeto para el grupo de GPU	Solo lectura
name-**label**	El nombre del grupo de GPU	Lectura/Escritura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
name-description	El texto descriptivo del grupo de GPU	Lectura/Escritura
VGPU-uuids	Muestra las referencias únicas de identificador/objeto para las GPU virtuales en el grupo de GPU	Parámetro de conjunto de solo lectura
PGPU-uuids	Muestra las referencias únicas de identificador/objeto para las GPU en el grupo de GPU	Parámetro de conjunto de solo lectura
other-config	Una lista de pares clave/valor que especifican parámetros de configuración adicionales para el grupo de GPU	Parámetro de mapa de lectura y escritura
supported-VGPU-types	Unión de todos los tipos de GPU virtuales admitidos por el hardware subyacente	Solo lectura
enabled-VGPU-types	Unión de todos los tipos de GPU virtuales que se han habilitado en las GPU subyacentes	Solo lectura
allocation-algorithm	Configuración de primero en profundidad/amplitud para la asignación de GPU virtuales en PGPU dentro del grupo	Parámetro enum de lectura y escritura

Operaciones de grupos de GPU Comandos para trabajar con grupos de GPU

gpu-group-create

```
xe gpu-group-create name-label=name_for_group [name-description=
    description]
<!--NeedCopy-->
```

Crea un nuevo grupo de GPU (vacío) al que se pueden mover las GPU.

gpu-group-destroy

```
xe gpu-group-destroy uuid=uuid_of_group
<!--NeedCopy-->
```

Destruye el grupo de GPU; solo se permite para grupos vacíos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

gpu-group-get-remaining-capacity

```
xe gpu-group-get-remaining-capacity uuid=uuid_of_group vgpu-type-uuid=
   uuid_of_vgpu_type
<!--NeedCopy-->
```

Devuelve cuántas GPU virtuales más del tipo especificado se pueden crear instancias en este grupo de GPU.

gpu-group-param-set

```
xe gpu-group-param-set uuid=uuid_of_group allocation-algorithm=breadth-
   first|depth-first
<!--NeedCopy-->
```

Cambia el algoritmo que el grupo de GPU utiliza para asignar GPU virtuales a las GPU.

Parámetros de GPU virtual

Las GPU virtuales tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
uuid	La referencia única de identificador/objeto para la GPU virtual	Solo lectura
vm-uuid	La referencia única de identificador/objeto para la máquina virtual a la que se asigna la GPU virtual	Solo lectura
vm-name-**label**	El nombre de la VM a la que se asigna la GPU virtual	Solo lectura
gpu-group-uuid	La referencia única de identificador/objeto para el grupo de GPU en el que se encuentra la GPU virtual	Solo lectura
gpu-group-name-**label**	El nombre del grupo de GPU en el que se encuentra la GPU virtual	Solo lectura
currently-attached	True si se está ejecutando una máquina virtual con paso a través de GPU, falso en caso contrario	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
other-config	Una lista de pares clave/valor que especifican parámetros de configuración adicionales para la GPU virtual	Parámetro de mapa de lectura y escritura
type-uuid	La referencia única de identificador/objeto para el tipo de GPU virtual de esta GPU virtual	Parámetro de mapa de lectura y escritura
type-model-name	Nombre del modelo asociado al tipo de GPU virtual	Solo lectura

Parámetros de tipo de GPU virtual

> **Nota:**
>
> Las GPU virtuales y de transferencia de GPU no son compatibles con la migración en vivo, la migración en vivo del almacenamiento ni la suspensión de máquinas virtuales, a menos que haya software y tarjetas gráficas compatibles de los proveedores de GPU. Las máquinas virtuales sin este soporte no se pueden migrar para evitar el tiempo de inactividad. Para obtener información sobre la compatibilidad de vGPU de NVIDIA con la migración en vivo, la migración en vivo de almacenamiento y la suspensión de VM, consulte Gráficos.

Los tipos de GPU virtuales tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
uuid	La referencia única de identificador/objeto para el tipo de GPU virtual	Solo lectura
vendor-name	Nombre del proveedor de GPU virtual	Solo lectura
model-name	Nombre del modelo asociado al tipo de GPU virtual	Solo lectura
freeze-frame	Tamaño del búfer de fotogramas del tipo de GPU virtual, en bytes	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
max-heads	Número máximo de pantallas admitidas por el tipo de GPU virtual	Solo lectura
supported-on-PGPUs	Lista de GPU que admiten este tipo de GPU virtual	Solo lectura
enabled-on-PGPUs	Lista de las GPU que tienen habilitado este tipo de GPU virtual	Solo lectura
VGPU-uuids	Lista de GPU virtuales de este tipo	Solo lectura

Operaciones de GPU virtual

vgpu-create

```
xe vgpu-create vm-uuid=uuid_of_vm gpu_group_uuid=uuid_of_gpu_group [
   vgpu-type-uuid=uuid_of_vgpu-type]
<!--NeedCopy-->
```

Crea una GPU virtual. Este comando conecta la VM al grupo de GPU especificado y, de manera opcional, especifica el tipo de GPU virtual. Si no se especifica ningún tipo de GPU virtual, se asume el tipo de "transferencia".

vgpu-destroy

```
xe vgpu-destroy uuid=uuid_of_vgpu
<!--NeedCopy-->
```

Destruye la GPU virtual especificada.

Desactivación de VNC para máquinas virtuales con GPU virtual

```
xe vm-param-add uuid=uuid_of_vmparam-name=platform vgpu_vnc_enabled=
   true|false
<!--NeedCopy-->
```

El uso de **false** inhabilita la consola de VNC para una VM a medida que disablevnc=1 pasa al emulador de pantalla. De forma predeterminada, la VNC está habilitada.

Comandos de host

Comandos para interactuar con el host de XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Los hosts XenServer son los servidores físicos que ejecutan el software XenServer. Tienen máquinas virtuales ejecutándose en ellas bajo el control de una máquina virtual con privilegios especiales, conocida como dominio de control o dominio 0.

Los objetos host de XenServer se pueden enumerar con los comandos estándar de listado de objetos: `xe host-listxe host-cpu-list`, y `xe host-crashdump-list`). Los parámetros se pueden manipular con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel.

Selectores de host

Varios de los comandos que se enumeran aquí tienen un mecanismo común para seleccionar uno o más hosts XenServer en los que realizar la operación. Lo más simple es proporcionar el argumento `host=uuid_or_name_label`. También puede especificar XenServer filtrando la lista completa de hosts según los valores de los campos. Por ejemplo, al especificar `enabled=true` se seleccionan todos los hosts de XenServer cuyo campo `enabled` sea igual a `true`. Si coinciden varios hosts de XenServer y la operación se puede realizar en varios hosts de XenServer, debe especificar si quiere `--multiple` realizar la operación. La lista completa de parámetros que se pueden hacer coincidir se describe al principio de esta sección. Puede obtener esta lista de comandos ejecutando el comando `xe host-list params=all`. Si no se proporcionan parámetros para seleccionar los hosts de XenServer, la operación se realiza en todos los hosts de XenServer.

Parámetros de host

Los hosts de XenServer tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
`uuid`	La referencia única de identificador/objeto para el host de XenServer	Solo lectura
`name-label`	El nombre del host de XenServer	Lectura/Escritura
`name-description`	La cadena de descripción del host de XenServer	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
enabled	El valor es **false** si está inhabilitado. Esto evita que las máquinas virtuales nuevas se inicien en los hosts y prepara los hosts para que se apaguen o reinicien. El valor es **true** si el host está habilitado	Solo lectura
API-version-major	Número de versión principal	Solo lectura
API-version-minor	Número de versión menor	Solo lectura
API-version-vendor	Identificación del proveedor de API	Solo lectura
API-version-vendor-implementation	Detalles de la implementación del proveedor	Parámetro de mapa de solo lectura
logging	Configuración de registros	Parámetro de mapa de lectura y escritura
suspend-image-sr-uuid	La referencia única de identificador/objeto para el SR donde se colocan imágenes suspendidas	Lectura/Escritura
crash-dump-sr-uuid	La referencia única de identificador/objeto para el SR donde se colocan los volcados de memoria	Lectura/Escritura
software-version	Lista de parámetros de control de versiones y sus valores	Parámetro de mapa de solo lectura
capabilities	Lista de versiones de Xen que puede ejecutar el host de XenServer	Parámetro de conjunto de solo lectura
other-config	Una lista de pares clave/valor que especifican parámetros de configuración adicionales para el host de XenServer	Parámetro de mapa de lectura y escritura
chipset-info	Una lista de pares clave/valor que especifican información sobre el conjunto de chips	Parámetro de mapa de solo lectura
hostname	Nombre de host del host de XenServer	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
address	Dirección IP del host de XenServer	Solo lectura
license-server	Una lista de pares clave/valor que especifican información sobre el servidor de licencias. El puerto predeterminado para las comunicaciones con los productos Citrix es 27000. Para obtener información sobre cómo cambiar los números de puerto debido a conflictos, consulte Cambiar los números de puerto	Parámetro de mapa de solo lectura
supported-bootloaders	Lista de gestores de arranque que admite el host de XenServer, por ejemplo, pygrubeliloader	Parámetro de conjunto de solo lectura
memory-total	Cantidad total de RAM física en el host de XenServer, en bytes	Solo lectura
memory-free	Cantidad total de RAM física restante que se puede asignar a las VM, en bytes	Solo lectura
host-metrics-live	True si el host está operativo	Solo lectura
logging	La clave syslog_destination se puede establecer en el nombre de host de un servicio syslog de escucha remota.	Parámetro de mapa de lectura y escritura
allowed-operations	Enumera las operaciones permitidas en este estado. Esta lista es solo informativa y es posible que el estado del host haya cambiado cuando un cliente lea este campo.	Parámetro de conjunto de solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
current-operations	Enumera las operaciones en curso en ese momento. Esta lista es solo informativa y es posible que el estado del host haya cambiado cuando un cliente lea este campo.	Parámetro de conjunto de solo lectura
patches	Conjunto de parches de host	Parámetro de conjunto de solo lectura
blobs	almacén de datos binarios	Solo lectura
memory-free-computed	Una estimación conservadora de la cantidad máxima de memoria libre en un host	Solo lectura
ha-statefiles	Los UUID de todos los archivos de estado de HA	Solo lectura
ha-network-peers	Los UUID de todos los hosts que pueden alojar las VM en este host si se produce un error	Solo lectura
external-auth-type	Tipo de autenticación externa, por ejemplo, Active Directory.	Solo lectura
external-auth-service-name	El nombre del servicio de autenticación externo	Solo lectura
external-auth-configuration	Información de configuración para el servicio de autenticación externo.	Parámetro de mapa de solo lectura

Los hosts de XenServer contienen otros objetos que también tienen listas de parámetros.

Las CPU de los hosts de XenServer tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
uuid	La referencia única de identificador/objeto para la CPU	Solo lectura
number	El número del núcleo físico de la CPU en el host de XenServer	Solo lectura
vendor	La cadena de proveedor para el nombre de la CPU	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
speed	La velocidad del reloj de la CPU, en Hz	Solo lectura
modelname	La cadena de proveedor para el modelo de CPU, por ejemplo, “CPU Intel(R) Xeon(TM) de 3,00 GHz”	Solo lectura
stepping	El número de revisión de la CPU	Solo lectura
flags	Los indicadores de la CPU física (una versión descodificada del campo de funciones)	Solo lectura
Utilisation	La utilización actual de la CPU	Solo lectura
host-uuid	El UUID si el host en el que se encuentra la CPU	Solo lectura
model	El número de modelo de la CPU física	Solo lectura
family	El número de familia de CPU física	Solo lectura

Los volcados de fallos en los hosts de XenServer tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
uuid	La referencia de identificador/objeto única para el volcado de bloqueo	Solo lectura
host	El host de XenServer al que corresponde el crashdump	Solo lectura
timestamp	Marca de tiempo de la fecha y hora en que se produjo el volcado, en el formulario yyyymmdd-hhmmss-ABC, donde *ABC* es el indicador de zona horaria, por ejemplo, GMT	Solo lectura
size	Tamaño del volcado de bloqueo, en bytes	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

host-all-editions

```
xe host-all-editions
<!--NeedCopy-->
```

Obtenga una lista de todas las ediciones disponibles

host-apply-edition

```
xe host-apply-edition [host-uuid=host_uuid] [edition=xenserver_edition=
    "free" "per-socket" "xendesktop"]
<!--NeedCopy-->
```

Asigna la licencia de XenServer a un servidor host. Al asignar una licencia, XenServer se pone en contacto con el servidor de licencias y solicita el tipo de licencia especificado. Si hay una licencia disponible, se retira del servidor de licencias.

Para obtener información sobre la configuración inicial de licencias, consulte también `license-server-address` y `license-server-port`.

host-backup

```
xe host-backup file-name=backup_filename host=host_name
<!--NeedCopy-->
```

Descargue una copia de seguridad del dominio de control del host XenServer especificado en la máquina desde la que se invoca el comando. Guárdalo ahí como un archivo con el nombre `file-name`.

> **Importante:**
>
> Si bien el comando `xe host-backup` funciona si se ejecuta en el host local (es decir, sin especificar un nombre de host específico), no lo use de esta manera. Hacerlo llenaría la partición del dominio de control con el archivo de copia de seguridad. Utilice el comando únicamente desde una máquina remota fuera del host en la que tenga espacio para guardar el archivo de copia de seguridad.

host-bugreport-upload

```
xe host-bugreport-upload [host-selector=host_selector_value...] [url=
    destination_url http-proxy=http_proxy_name]
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Genera un nuevo informe de errores (mediantexen-bugtool, con todos los archivos opcionales incluidos) y súbelo al sitio FTP de Soporte o a alguna otra ubicación.

Los hosts en los que se realizará esta operación se seleccionan mediante el mecanismo de selección estándar (consulte los selectores de anfitriones más arriba). Los argumentos opcionales pueden ser cualquier número de los parámetros de host enumerados al principio de esta sección.

Los parámetros opcionales sonhttp-proxy: Utilizar proxy HTTP especificado yurl: Cargar a esta URL de destino. Si no se utilizan parámetros opcionales, no se identifica ningún servidor proxy y el destino es el sitio FTP de soporte predeterminado.

host-call-plugin

```
xe host-call-plugin host-uuid=host_uuid plugin=plugin fn=function [args
   =args]
<!--NeedCopy-->
```

Llama a la función dentro del complemento en el host dado con argumentos opcionales.

host-compute-free-memory

```
xe host-compute-free-memory
<!--NeedCopy-->
```

Calcula la cantidad de memoria libre en el host.

host-compute-memory-overhead

```
xe host-compute-memory-overhead
<!--NeedCopy-->
```

Calcula la sobrecarga de memoria de virtualización de un host.

host-cpu-info

```
xe host-cpu-info [uuid=uuid]
<!--NeedCopy-->
```

Muestra información sobre las CPU físicas del host.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

host-crashdump-destroy

```
xe host-crashdump-destroy uuid=crashdump_uuid
<!--NeedCopy-->
```

Elimine un crashdump de host especificado por su UUID del host de XenServer.

host-crashdump-upload

```
xe host-crashdump-upload uuid=crashdump_uuid [url=destination_url] [
   http-proxy=http_proxy_name]
<!--NeedCopy-->
```

Cargue un volcado en el sitio FTP de soporte u otra ubicación. Si no se utilizan parámetros opcionales, no se identifica ningún servidor proxy y el destino es el sitio FTP de soporte predeterminado. Los parámetros opcionales son`http-proxy`: Utilizar proxy HTTP especificado y`url`: Cargar a esta URL de destino.

host-declare-dead

```
xe host-declare-dead uuid=host_uuid
<!--NeedCopy-->
```

Declara que el host está inactivo sin contactarlo explícitamente.

> **Advertencia:**
>
> Esta llamada es peligrosa y puede provocar la pérdida de datos si el host no está realmente muerto.

host-disable

```
xe host-disable [host-selector=host_selector_value...]
<!--NeedCopy-->
```

Inhabilita los hosts de XenServer especificados, lo que impide que se inicien nuevas máquinas virtuales en ellos. Esta acción prepara los hosts de XenServer para apagarse o reiniciarse. Una vez reiniciado el host, si se cumplen todas las condiciones para la activación (por ejemplo, si hay almacenamiento disponible), el host se vuelve a habilitar automáticamente.

Los hosts en los que se realizará esta operación se seleccionan mediante el mecanismo de selección estándar (consulte los selectores de anfitriones). Los argumentos opcionales pueden ser cualquier número de los parámetros de host enumerados al principio de esta sección.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

host-disable-display

```
xe host-disable-display uuid=host_uuid
<!--NeedCopy-->
```

Inhabilitar la visualización para el host.

host-disable-local-storage-caching

```
xe host-disable-local-storage-caching
<!--NeedCopy-->
```

Inhabilite el almacenamiento en caché del almacenamiento local en el host especificado.

host-dmesg

```
xe host-dmesg [host-selector=host_selector_value...]
<!--NeedCopy-->
```

Obtenga un Xen `dmesg` (la salida del búfer en anillo del núcleo) de los hosts XenServer específicos.

Los hosts en los que se realizará esta operación se seleccionan mediante el mecanismo de selección estándar (consulte los selectores de anfitriones más arriba). Los argumentos opcionales pueden ser cualquier número de los parámetros de host enumerados al principio de esta sección.

host-emergency-ha-disable

```
xe host-emergency-ha-disable  [--force]
<!--NeedCopy-->
```

Inhabilite HA en el host local. Solo se usa para recuperar un grupo con una configuración de alta disponibilidad rota.

host-emergency-management-reconfigure

```
xe host-emergency-management-reconfigure interface=
   uuid_of_management_interface_pif
<!--NeedCopy-->
```

Vuelva a configurar la interfaz de administración de este host de XenServer. Use este comando solo si el host de XenServer está en modo de emergencia. El modo de emergencia significa que el host es miembro de un grupo de recursos cuyo coordinador de grupo ha desaparecido de la red y no se puede contactar con él después de varios intentos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

host-emergency-reset-server-certificate

```
xe host-emergency-reset-server-certificate
<!--NeedCopy-->
```

Instala un certificado autofirmado en el host de XenServer en el que se ejecuta el comando.

host-enable

```
xe host-enable [host-selector=host_selector_value...]
<!--NeedCopy-->
```

Habilita los hosts de XenServer especificados, lo que permite iniciar nuevas máquinas virtuales en ellos.

Los hosts en los que se realizará esta operación se seleccionan mediante el mecanismo de selección estándar (consulte los selectores de anfitriones más arriba). Los argumentos opcionales pueden ser cualquier número de los parámetros de host enumerados al principio de esta sección.

host-enable-display

```
xe host-enable-display uuid=host_uuid
<!--NeedCopy-->
```

Habilite la visualización para el host.

host-enable-local-storage-caching

```
xe host-enable-local-storage-caching  sr-uuid=sr_uuid
<!--NeedCopy-->
```

Habilite el almacenamiento en caché local en el host especificado.

host-evacuate

```
xe host-evacuate [host-selector=host_selector_value...]
<!--NeedCopy-->
```

Live migra todas las VM en ejecución a otros hosts adecuados de un grupo. En primer lugar, inhabilite el host mediante el comando `host-disable`.

Si el host evacuado es el coordinador del grupo, se debe seleccionar otro host para que sea el coordinador del grupo. Para cambiar el coordinador del grupo con HA inhabilitada, utilice el comando

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

`pool-designate-new-master`. Para obtener más información, consulte pool-designate-new-master.

Con HA habilitada, la única opción es cerrar el host de XenServer, lo que hace que HA elija un nuevo coordinador de grupo de forma aleatoria. Para obtener más información, consulte host-shutdown.

Los hosts en los que se realizará esta operación se seleccionan mediante el mecanismo de selección estándar (consulte los selectores de anfitriones más arriba). Los argumentos opcionales pueden ser cualquier número de los parámetros de host enumerados al principio de esta sección.

host-forget

```
xe host-forget uuid=host_uuid
<!--NeedCopy-->
```

El agente XAPI olvida el host de XenServer especificado sin ponerse en contacto con él de forma explícita.

Utilice el parámetro `--force` para evitar que se le pida que confirme que realmente quiere realizar esta operación.

> **Advertencia:**
>
> No utilice este comando si la alta disponibilidad está habilitada en el grupo. Desactive primero HA y, a continuación, vuelva a activarla cuando haya olvidado el host.

Este comando es útil si el host de XenServer que se debe "olvidar"está inactivo. Sin embargo, si el host de XenServer está activo y forma parte del grupo, `xe pool-eject` utilícelo en su lugar.

host-get-server-certificate

```
xe host-get-server-certificate
<!--NeedCopy-->
```

Obtenga el certificado TLS del servidor instalado.

host-get-sm-diagnostics

```
xe host-get-sm-diagnostics uuid=uuid
<!--NeedCopy-->
```

Muestra información de diagnóstico de SM por host.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

host-get-system-status

```
xe host-get-system-status filename=name_for_status_file [entries=
    comma_separated_list] [output=tar.bz2|zip] [host-selector=
    host_selector_value...]
<!--NeedCopy-->
```

Descargue la información del estado del sistema en el archivo especificado. El parámetro opcional `entries` es una lista separada por comas de entradas de estado del sistema, tomada del fragmento XML de capacidades devuelto por el comando `host-get-system-status-capabilities`. Para obtener más información, consulte host-get-system-status-capabilities. Si no se especifica, toda la información de estado del sistema se guarda en el archivo. El parámetro `output` puede ser *tar.bz2* (el valor predeterminado) o *zip*. Si no se especifica este parámetro, el archivo se guarda como `tar.bz2`.

Los hosts en los que se realizará esta operación se seleccionan mediante el mecanismo de selección estándar (consulte los selectores de anfitriones más arriba).

host-get-system-status-capabilities

```
xe host-get-system-status-capabilities [host-selector=
    host_selector_value...]
<!--NeedCopy-->
```

Obtenga las capacidades de estado del sistema para los hosts especificados. Las capacidades se devuelven como un fragmento XML similar al siguiente ejemplo:

```
<?xml version="1.0" ?>
<system-status-capabilities>
    <capability content-type="text/plain" default-checked="yes" key="
       xenserver-logs"  \
        max-size="150425200" max-time="-1" min-size="150425200" min-
           time="-1" \
        pii="maybe"/>
    <capability content-type="text/plain" default-checked="yes" \
        key="xenserver-install" max-size="51200" max-time="-1" min-size
           ="10240" \
        min-time="-1" pii="maybe"/>
    ...
</system-status-capabilities>
<!--NeedCopy-->
```

Cada entidad de capacidad puede tener los siguientes atributos.

- `key` Un identificador único para la capacidad.
- `content-type` Puede ser texto/sin formato o aplicación/datos. Indica si una interfaz de usuario puede renderizar las entradas para consumo humano.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **default**-checked Puede ser sí o no. Indica si una interfaz de usuario selecciona esta entrada de forma predeterminada.
- min-size, max-size indica un intervalo aproximado para el tamaño, en bytes, de esta entrada. -1 indica que el tamaño no es importante.
- min-time, max-time indica un intervalo aproximado para el tiempo, en segundos, que tardó en recopilar esta entrada. -1 indica que el tiempo no es importante.
- pii Información de identificación personal. Indica si la entrada tiene información que puede identificar al propietario del sistema o detalles de su topología de red. El atributo puede tener uno de los valores siguientes:
  - no: No hay información de identificación personal en estas entradas
  - yes: Es probable o seguro que la PII está en estas entradas
  - maybe: Puede que quiera auditar estas entradas para obtener información de identificación personal
  - if_customized si los archivos no están modificados, no contienen PII. Sin embargo, dado que alentamos la edición de estos archivos, es posible que dicha personalización haya introducido la PII. Este valor se usa en particular para los scripts de red en el dominio de control.

  Las contraseñas nunca se incluirán en ningún informe de errores, independientemente de cualquier declaración de PII.

Los hosts en los que se realizará esta operación se seleccionan mediante el mecanismo de selección estándar (consulte los selectores de anfitriones más arriba).

host-get-thread-diagnostics

```
xe host-get-thread-diagnostics uuid=uuid
<!--NeedCopy-->
```

Muestra información de diagnóstico de subprocesos por host.

host-get-vms-which-prevent-evacuation

```
xe host-get-vms-which-prevent-evacuation uuid=uuid
<!--NeedCopy-->
```

Devuelva una lista de máquinas virtuales que eviten la evacuación de un host específico y muestre los motivos de cada una.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

host-is-in-emergency-mode

```
xe host-is-in-emergency-mode
<!--NeedCopy-->
```

Devuelve **true** si el host con el que está hablando la CLI está en modo de emergencia; de lo contrario, devuelve **false**. Este comando CLI funciona directamente en los hosts de los miembros del grupo, incluso sin la presencia de un coordinador del grupo.

host-license-add

```
xe host-license-add [license-file=path/license_filename] [host-uuid=
   host_uuid]
<!--NeedCopy-->
```

En el caso de XenServer, se usa para analizar un archivo de licencia local y agregarlo al host de XenServer especificado.

host-license-remove

```
xe host-license-remove [host-uuid=host_uuid]
<!--NeedCopy-->
```

Elimina cualquier licencia aplicada a un host.

host-license-view

```
xe host-license-view [host-uuid=host_uuid]
<!--NeedCopy-->
```

Muestra el contenido de la licencia de host de XenServer.

host-logs-download

```
xe host-logs-download [file-name=logfile_name] [host-selector=
   host_selector_value...]
<!--NeedCopy-->
```

Descargue una copia de los registros de los hosts de XenServer especificados. La copia se guarda de forma predeterminada en un archivo con marca de tiempo llamado `hostname-yyyy-mm-dd Thh:mm:ssZ.tar.gz`. Puede especificar un nombre de archivo diferente mediante el parámetro opcional *nombre-archivo*.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Los hosts en los que se realizará esta operación se seleccionan mediante el mecanismo de selección estándar (consulte los selectores de anfitriones más arriba). Los argumentos opcionales pueden ser cualquier número de los parámetros de host enumerados al principio de esta sección.

> **Importante:**
>
> Si bien el comando `xe host-logs-download` funciona si se ejecuta en el host local (es decir, sin especificar un nombre de host específico), *no* lo use de esta manera. Al hacerlo, se desordena la partición del dominio de control con la copia de los registros. Utilice el comando únicamente desde un equipo remoto ajeno al servidor en el que disponga de espacio para guardar la copia de los registros.

host-management-disable

```
xe host-management-disable
<!--NeedCopy-->
```

Inhabilita la escucha del agente host en una interfaz de red de administración externa y desconecta todos los clientes de API conectados (como XenCenter). Este comando funciona directamente en el host de XenServer al que está conectada la CLI. El comando no se reenvía al coordinador del grupo cuando se aplica a un host XenServer miembro.

> **Advertencia:**
>
> Tenga cuidado al usar este comando CLI fuera del host. Después de ejecutar este comando, no puede conectarse al dominio de control de forma remota a través de la red para volver a habilitar el agente de host.

host-management-reconfigure

```
xe host-management-reconfigure [interface=device] [pif-uuid=uuid]
<!--NeedCopy-->
```

Reconfigura el host de XenServer para que utilice la interfaz de red especificada como interfaz de administración, que es la interfaz que se utiliza para conectarse al XenCenter. El comando reescribe la clave MANAGEMENT_INTERFACE en `/etc/xensource-inventory`.

Si se especifica el nombre del dispositivo de una interfaz (que debe tener una dirección IP), el host de XenServer se vuelve a vincular inmediatamente. Este comando funciona tanto en modo normal como de emergencia.

Si se especifica el UUID de un objeto PIF, el host de XenServer determina qué dirección IP se va a volver a vincular a sí mismo. No debe estar en modo de emergencia cuando se ejecute este comando.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Advertencia:**
>
> Tenga cuidado al usar este comando CLI fuera del host y asegúrese de tener conectividad de red en la nueva interfaz. Use `xe pif-reconfigure` para configurar uno primero. De lo contrario, los comandos CLI posteriores no podrán acceder al host de XenServer.

host-power-on

```
xe host-power-on [host=host_uuid]
<!--NeedCopy-->
```

Enciende los hosts de XenServer con la función *Host Power On habilitada*. Antes de usar este comando, `host-set-power-on` habilítelo en el host.

host-reboot

```
xe host-reboot [host-selector=host_selector_value...]
<!--NeedCopy-->
```

Reinicie los hosts de XenServer especificados. Los hosts especificados deben inhabilitarse primero mediante el comando `xe host-disable`; de lo contrario, se mostrará un mensaje de error `HOST_IN_USE`.

Los hosts en los que se realizará esta operación se seleccionan mediante el mecanismo de selección estándar (consulte los selectores de anfitriones más arriba). Los argumentos opcionales pueden ser cualquier número de los parámetros de host enumerados al principio de esta sección.

Si los hosts de XenServer especificados son miembros de un grupo, se controla la pérdida de conectividad al apagarse y el grupo se recupera cuando los hosts de XenServer regresan. Los otros miembros y el coordinador de la agrupación siguen funcionando.

Si cierra el coordinador del grupo, el grupo queda fuera de acción hasta que se produzca una de las siguientes acciones:

- Convierte a uno de los miembros en el coordinador de la agrupación
- El coordinador original de la agrupación se reinicia y vuelve a estar en línea.

  Cuando el coordinador de la agrupación vuelve a estar en línea, los miembros se vuelven a conectar y se sincronizan con el coordinador de la agrupación.

host-restore

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe host-restore [file-name=backup_filename] [host-selector=
    host_selector_value...]
<!--NeedCopy-->
```

Restaure una copia de seguridad con el nombre `file-name` del software de control de host XenServer. El uso de la palabra "restaurar"aquí no significa una restauración completa en el sentido habitual, simplemente significa que el archivo de copia de seguridad comprimido se ha descomprimido y desempaquetado en la partición secundaria. Después de haber hecho un `xe host-restore`, debe arrancar el CD de instalación y usar su opción Restaurar desde copia de seguridad.

Los hosts en los que se realizará esta operación se seleccionan mediante el mecanismo de selección estándar (consulte los selectores de anfitriones más arriba). Los argumentos opcionales pueden ser cualquier número de los parámetros de host enumerados al principio de esta sección.

host-send-debug-keys

```
xe host-send-debug-keys  host-uuid=host_uuid keys=keys
<!--NeedCopy-->
```

Envíe las claves de depuración del hipervisor especificadas al host especificado.

host-server-certificate-install

```
xe host-server-certificate-install certificate=path_to_certificate_file
     private-key=path_to_private_key [certificate-chain=
    path_to_chain_file] [host=host_name | uuid=host_uuid]
<!--NeedCopy-->
```

Instale un certificado TLS en un host de XenServer.

host-set-hostname-live

```
xe host-set-hostname-live host-uuid=uuid_of_host host-name=new_hostname
<!--NeedCopy-->
```

Cambie el nombre de host del host de XenServer especificado por. `host-uuid` Este comando establece de forma persistente tanto el nombre de host en la base de datos del dominio de control como el nombre de host Linux real del host de XenServer. El valor de `host-name` *no* es el mismo que el valor del campo `name_label`.

host-set-power-on-mode

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe host-set-power-on-mode host=host_uuid power-on-mode={
 "" | "wake-on-lan" | "DRAC" | "custom" }
  \
    [ power-on-config:power_on_ip=ip-address power-on-config:
       power_on_user=user power-on-config:power_on_password_secret=
       secret-uuid ]
<!--NeedCopy-->
```

Utilícela para habilitar la función *Host Power On* en los hosts de XenServer que son compatibles con las soluciones de alimentación remota. Al usar el comando `host-set-power-on`, debe especificar el tipo de solución de administración de energía en el host (es decir, el modo de encendido). A continuación, especifique las opciones de configuración mediante el argumento power-on-config y sus pares clave-valor asociados.

Para utilizar la función de secretos para almacenar la contraseña, especifique la clave `"power_on_password_secret"`. Para obtener más información, consulte Secretos.

host-shutdown

```
xe host-shutdown [host-selector=host_selector_value...]
<!--NeedCopy-->
```

Cierre los hosts de XenServer especificados. Los hosts de XenServer especificados deben inhabilitarse primero mediante el comando `xe host-disable`; de lo contrario, aparecerá un mensaje de error `HOST_IN_USE`.

Los hosts en los que se realizará esta operación se seleccionan mediante el mecanismo de selección estándar (consulte los selectores de anfitriones más arriba). Los argumentos opcionales pueden ser cualquier número de los parámetros de host enumerados al principio de esta sección.

Si los hosts de XenServer especificados son miembros de un grupo, se controla la pérdida de conectividad al apagarse y el grupo se recupera cuando los hosts de XenServer regresan. Los otros miembros y el coordinador de la agrupación siguen funcionando.

Si cierra el coordinador del grupo, el grupo queda fuera de acción hasta que se produzca una de las siguientes acciones:

- Convierte a uno de los miembros en el coordinador de la agrupación
- El coordinador original de la agrupación se reinicia y vuelve a estar en línea.

  Cuando el coordinador de la agrupación vuelve a estar en línea, los miembros se vuelven a conectar y se sincronizan con el coordinador de la agrupación.

Si la HA está habilitada para el grupo, uno de los miembros pasa a ser un coordinador del grupo automáticamente. Si HA está inhabilitado, debe designar manualmente el host de XenServer deseado

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

como coordinador de grupos con el comando `pool-designate-new-master`. Para obtener más información, consulte pool-designate-new-master.

host-sm-dp-destroy

```
xe host-sm-dp-destroy uuid=uuid dp=dp [allow-leak=true|false]
<!--NeedCopy-->
```

Intente destruir y limpiar una ruta de datos de almacenamiento en un host. Si se proporciona `allow-leak=true`, elimina todos los registros de la ruta de datos, incluso si no se cierra limpiamente.

host-sync-data

```
xe host-sync-data
<!--NeedCopy-->
```

Sincronice los datos almacenados en el coordinador del grupo con el host designado. Esto no incluye los datos de la base de datos).

host-syslog-reconfigure

```
xe host-syslog-reconfigure [host-selector=host_selector_value...]
<!--NeedCopy-->
```

Vuelva a configurar el `syslog` daemon en los hosts de XenServer especificados. Este comando aplica la información de configuración definida en el parámetro `logging` de host.

Los hosts en los que se realizará esta operación se seleccionan mediante el mecanismo de selección estándar (consulte los selectores de anfitriones más arriba). Los argumentos opcionales pueden ser cualquier número de los parámetros de host enumerados al principio de esta sección.

host-data-source-list

```
xe host-data-source-list [host-selectors=host selector value...]
<!--NeedCopy-->
```

Enumerar las fuentes de datos que se pueden grabar para un host.

Seleccione los hosts en los que quiere realizar esta operación mediante el mecanismo de selección estándar (consulte selectores de host). Los argumentos opcionales pueden ser cualquier número de los parámetros de host enumerados al principio de esta sección. Si no se dan parámetros para seleccionar hosts, la operación se lleva a cabo en todos los hosts.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Los orígenes de datos tienen dos parámetros: `standard` y `enabled`. Este comando genera los valores de los parámetros:

- Si un origen de datos tiene `enabled` establecido en **`true`**, las métricas se están registrando actualmente en la base de datos de rendimiento.
- Si un origen de datos tiene `standard` establecido en **`true`**, las métricas se registran en la base de datos de rendimiento *de forma predeterminada*. El valor de `enabled` también se establece en **`true`** para este origen de datos.
- Si un origen de datos tiene `standard` establecido en **`false`**, las métricas *no* se registran en la base de datos de rendimiento de forma predeterminada. El valor de `enabled` también se establece en **`false`** para este origen de datos.

Para empezar a registrar métricas de fuentes de datos en la base de datos de rendimiento, ejecute el comando `host-data-source-record`. Este comando establece `enabled` en **`true`**. Para detener, ejecute el `host-data-source-forget`. Este comando establece `enabled` en **`false`**.

host-data-source-record

```
xe host-data-source-record data-source=name_description_of_data_source
    [host-selectors=host_selector_value...]
<!--NeedCopy-->
```

Registre la fuente de datos especificada para un host.

Esta operación escribe la información de la fuente de datos en la base de datos de métricas de rendimiento persistentes de los hosts especificados. Por motivos de rendimiento, esta base de datos es distinta de la base de datos de agentes normal.

Seleccione los hosts en los que quiere realizar esta operación mediante el mecanismo de selección estándar (consulte selectores de host). Los argumentos opcionales pueden ser cualquier número de los parámetros de host enumerados al principio de esta sección. Si no se dan parámetros para seleccionar hosts, la operación se lleva a cabo en todos los hosts.

host-data-source-forget

```
xe host-data-source-forget data-source=name_description_of_data_source
    [host-selectors=host_selector_value...]
<!--NeedCopy-->
```

Deje de grabar la fuente de datos especificada para un host y olvide todos los datos grabados.

Seleccione los hosts en los que quiere realizar esta operación mediante el mecanismo de selección estándar (consulte selectores de host). Los argumentos opcionales pueden ser cualquier número de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

los parámetros de host enumerados al principio de esta sección. Si no se dan parámetros para seleccionar hosts, la operación se lleva a cabo en todos los hosts.

host-data-source-query

```
xe host-data-source-query data-source=name_description_of_data_source [
   host-selectors=host_selector_value...]
<!--NeedCopy-->
```

Muestra la fuente de datos especificada para un host.

Seleccione los hosts en los que quiere realizar esta operación mediante el mecanismo de selección estándar (consulte selectores de host). Los argumentos opcionales pueden ser cualquier número de los parámetros de host enumerados al principio de esta sección. Si no se dan parámetros para seleccionar hosts, la operación se lleva a cabo en todos los hosts.

Comandos de mensajes

Comandos para trabajar con mensajes. Los mensajes se crean para notificar a los usuarios sobre eventos importantes y se muestran en XenCenter como alertas.

Los objetos de mensaje se pueden enumerar con el comando estándar de listado de objetos (`xe message-list`) y los parámetros manipulados con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

Parámetros de mensajes

Nombre del parámetro	Descripción	Tipo
`uuid`	La referencia de identificador/objeto única para el mensaje	Solo lectura
`name`	El nombre único del mensaje	Solo lectura
`priority`	La prioridad del mensaje. Los números más altos indican una mayor prioridad	Solo lectura
`class`	La clase de mensaje, por ejemplo, VM.	Solo lectura
`obj-uuid`	El uuid del objeto afectado.	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
timestamp	La hora en que se generó el mensaje.	Solo lectura
body	El contenido del mensaje.	Solo lectura

message-create

```
xe message-create name=message_name body=message_text [[host-uuid=
    uuid_of_host] | [sr-uuid=uuid_of_sr] | [vm-uuid=uuid_of_vm] | [pool-
    uuid=uuid_of_pool]]
<!--NeedCopy-->
```

Crea un mensaje.

message-destroy

```
xe message-destroy [uuid=message_uuid]
<!--NeedCopy-->
```

Destruye un mensaje existente. Puede crear un script para destruir todos los mensajes. Por ejemplo:

```
# Dismiss all alerts   \
    IFS=","; for m in $(xe message-list params=uuid --minimal); do  \
    xe message-destroy uuid=$m  \
    done
<!--NeedCopy-->
```

Comandos de red

Comandos para trabajar con redes.

Los objetos de red se pueden enumerar con el comando estándar de listado de objetos (`xe network -list`) y los parámetros se pueden manipular con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

Parámetros de red

Las redes tienen los siguientes parámetros:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
uuid	La referencia única de identificador/objeto para la red	Solo lectura
name-**label**	El nombre de la red	Lectura/Escritura
name-description	El texto descriptivo de la red	Lectura/Escritura
VIF-uuids	Una lista de identificadores únicos de las VIF (interfaces de red virtual) que se conectan desde las VM a esta red	Parámetro de conjunto de solo lectura
PIF-uuids	Una lista de identificadores únicos de las PIF (interfaces de red físicas) que se conectan desde los hosts de XenServer a esta red	Parámetro de conjunto de solo lectura
bridge	Nombre del puente correspondiente a esta red en el host local de XenServer	Solo lectura
default-locking-mode	Objeto de red que se utiliza con objetos VIF para el filtrado ARP. Se establece en unlocked para eliminar todas las reglas de filtrado asociadas con el VIF. Se establece en disabled para que el VIF interrumpa todo el tráfico.	Lectura/Escritura
purpose	Conjunto de propósitos para los que el host de XenServer utiliza esta red. Se establece en nbd para usar la red para realizar conexiones NBD.	Lectura/Escritura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
other-config: staticroutes	Lista separada por comas de entradas con formato de *subred/máscara de red/puerta de enlace* que especifican la dirección de la puerta de enlace a través de la cual se redirigen. Por ejemplo, configurar other-config: **static**-routes en 172.16.0.0/15/192.168.0.3,172.18.0.0/16/192.168.0.4 provoca que el tráfico en 172.16.0.0/15 se redirija a 192.168.0.3 y el tráfico en 172.18.0.0/16 se redirija a 192.168.0.4.	Lectura/Escritura
other-config: ethtoolautoneg	Actívela para inhabilitar la negociación automática de la interfaz física o el puente. El valor predeterminado es sí.	Lectura/Escritura
other-config:ethtool-rx	Actívela para habilitar la suma de comprobación de recepción y desactívela para inhabilitarla.	Lectura/Escritura
other-config:ethtool-tx	Actívela para habilitar la suma de comprobación de transmisión y desactívela para inhabilitarla.	Lectura/Escritura
other-config:ethtool-sg	Actívela para activar la recopilación de dispersión y desactívela para inhabilitarla.	Lectura/Escritura
other-config:ethtool-tso	Actívela para habilitar la descarga de segmentación de TCP y desactívela para inhabilitarla.	Lectura/Escritura
other-config:ethtool-ufo	Actívela para habilitar la descarga de fragmentos UDP y desactívela para inhabilitarla.	Lectura/Escritura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
other-config:ethtool-gso	Actívela para habilitar la descarga de segmentación genérica y desactívela para inhabilitarla.	Lectura/Escritura
blobs	almacén de datos binarios	Solo lectura

network-create

```
xe network-create name-label=name_for_network [name-description=
    descriptive_text]
<!--NeedCopy-->
```

Crea una red.

network-destroy

```
xe network-destroy uuid=network_uuid
<!--NeedCopy-->
```

Destruye una red existente.

Comandos de SR-IOV

Comandos para trabajar con SR-IOV.

Los objetos network-sriov se pueden enumerar con el comando estándar de listado de objetos (xe network-sriov-list) y los parámetros se pueden manipular con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

Parámetros de SR-IOV

El SR-IOV tiene los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
physical-PIF	El PIF para habilitar SR-IOV.	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
logical-PIF	Un PIF lógico de SR-IOV. Los usuarios pueden usar este parámetro para crear una red VLAN SR-IOV.	Solo lectura
requires-reboot	Si se establece en True, se usa para reiniciar el host para que la habilitación de SR-IOV entre en vigor.	Solo lectura
remaining-capacity	Número de VF disponibles restantes.	Solo lectura

network-sriov-create

```
xe network-sriov-create network-uuid=network_uuid pif-uuid=
   physical_pif_uuid
<!--NeedCopy-->
```

Crea un objeto de red SR-IOV para una PIF física determinada y habilita SR-IOV en la PIF física.

network-sriov-destroy

```
xe network-sriov-destroy uuid=network_sriov_uuid
<!--NeedCopy-->
```

Quita un objeto SR-IOV de red e inhabilita SR-IOV en su PIF físico.

Asignar una VF SR-IOV

```
xe vif-create device=device_index mac=vf_mac_address network-uuid=
   sriov_network vm-uuid=vm_uuid
<!--NeedCopy-->
```

Asigna una VF desde una red SR-IOV a una VM.

Comandos del controlador SDN

Comandos para trabajar con el controlador SDN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

sdn-controller-forget

```
xe sdn-controller-introduce [address=address] [protocol=protocol] [tcp-
    port=tcp_port]
<!--NeedCopy-->
```

Presente un controlador SDN.

sdn-controller-introduce

```
xe sdn-controller-forget uuid=uuid
<!--NeedCopy-->
```

Retire un controlador SDN.

Comandos de túnel

Comandos para trabajar con túneles.

tunnel-create

```
xe tunnel-create pif-uuid=pif_uuid network-uuid=network_uuid
<!--NeedCopy-->
```

Crea un túnel nuevo en un host.

tunnel-destroy

```
xe tunnel-destroy uuid=uuid
<!--NeedCopy-->
```

Destruye un túnel.

Comandos de parches

Comandos para trabajar con parches.

patch-apply

```
xe patch-apply uuid=patch_uuid host-uuid=host_uuid
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aplique el parche cargado anteriormente al host especificado.

patch-clean

```
xe patch-clean uuid=uuid
<!--NeedCopy-->
```

Elimina un archivo de parches cargado anteriormente.

patch-destroy

```
xe patch-destroy uuid=uuid
<!--NeedCopy-->
```

Elimine un registro de parches y archivos no aplicados del host.

patch-pool-apply

```
xe patch-pool-apply uuid=uuid
<!--NeedCopy-->
```

Aplique el parche cargado anteriormente a todos los hosts del grupo.

patch-pool-clean

```
xe patch-pool-clean uuid=uuid
<!--NeedCopy-->
```

Elimine un archivo de parches cargado anteriormente en todos los hosts del grupo.

patch-precheck

```
xe patch-precheck uuid=uuid host-uuid=host_uuid
<!--NeedCopy-->
```

Ejecute las comprobaciones previas incluidas en el parche cargado anteriormente en el host especificado.

patch-upload

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe patch-upload file-name=file_name
<!--NeedCopy-->
```

Cargue un archivo de parche en el host.

Comandos PBD

Comandos para trabajar con PBD (dispositivos de bloques físicos). Los PBD son los objetos de software a través de los cuales el host de XenServer accede a los repositorios de almacenamiento (SR).

Los objetos PBD se pueden enumerar con el comando estándar de listado de objetos (`xe pbd-list`) y los parámetros manipulados con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

Parámetros de PBD

Los PBD tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
`uuid`	La referencia de identificador/objeto única para el PBD.	Solo lectura
`sr-uuid`	El repositorio de almacenamiento al que apunta el PBD	Solo lectura
`device-config`	Información de configuración adicional que se proporciona al controlador de backend de SR de un host	Parámetro de mapa de solo lectura
`currently-attached`	True si el SR está conectado a este host, False en caso contrario	Solo lectura
`host-uuid`	UUID de la máquina física en la que está disponible el PBD	Solo lectura
`host`	El campo host está en desuso. Usa host_uuid en su lugar.	Solo lectura
`other-config`	Información de configuración adicional.	Parámetro de mapa de lectura y escritura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

pbd-create

```
xe pbd-create host-uuid=uuid_of_host sr-uuid=uuid_of_sr [device-config:
    key=corresponding_value]
<!--NeedCopy-->
```

Cree un PBD en el host de XenServer. El parámetro `device-config` de solo lectura solo se puede configurar en el momento de la creación.

Para agregar una asignación desde 'path'a '/tmp', asegúrese de que la línea de comandos contenga el argumento `device-config:path=/tmp`

Para obtener una lista completa de los pares clave/valor de configuración de dispositivo compatibles en cada tipo de SR, consulte Almacenamiento.

pbd-destroy

```
xe pbd-destroy uuid=uuid_of_pbd
<!--NeedCopy-->
```

Destruye el PBD especificado.

pbd-plug

```
xe pbd-plug uuid=uuid_of_pbd
<!--NeedCopy-->
```

Intenta conectar el PBD al host de XenServer. Si este comando se ejecuta correctamente, el SR al que se hace referencia (y los VDI que contiene) pasan a ser visibles para el host de XenServer.

pbd-unplug

```
xe pbd-unplug uuid=uuid_of_pbd
<!--NeedCopy-->
```

Intente desconectar el PBD del host de XenServer.

Comandos PIF

Comandos para trabajar con PIF (objetos que representan las interfaces de red físicas).

Los objetos de PIF se pueden enumerar con el comando estándar de lista de objetos (`xe pif-list`) y los parámetros manipulados con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Parámetros PIF

Los PIF tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
`uuid`	La referencia única de identificador/objeto para el PIF	Solo lectura
`device machine-readable`	Nombre de la interfaz (por ejemplo, eth0)	Solo lectura
`MAC`	La dirección MAC del PIF	Solo lectura
`other-config`	Pares `name:value` de configuración PIF adicionales.	Parámetro de mapa de lectura y escritura
`physical`	Si es cierto, el PIF apunta a una interfaz de red física real	Solo lectura
`currently-attached`	¿El PIF está conectado actualmente a este host? **`true`** o **`false`**	Solo lectura
`MTU`	Unidad de transmisión máxima del PIF en bytes.	Solo lectura
`VLAN`	Etiqueta VLAN para todo el tráfico que pasa a través de esta interfaz. -1 indica que no se ha asignado ninguna etiqueta VLAN	Solo lectura
`bond-master-of`	El UUID del enlace del que este PIF es la interfaz principal (si existe)	Solo lectura
`bond-slave-of`	El UUID del vínculo del que forma parte este PIF (si lo hay)	Solo lectura
`management`	¿Se ha designado este PIF para que sea una interfaz de administración para el dominio de control?	Solo lectura
`network-uuid`	La referencia única de identificador/objeto de la red virtual a la que está conectado este PIF	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
network-name-**label**	El nombre de la red virtual a la que está conectado este PIF	Solo lectura
host-uuid	La referencia única de identificador/objeto del host de XenServer al que está conectado este PIF	Solo lectura
host-name-**label**	El nombre del host de XenServer al que está conectado este PIF	Solo lectura
IP-configuration-mode	Tipo de configuración de dirección de red utilizada; DHCP o estática	Solo lectura
IP	Dirección IP del PIF. Se define aquí cuando el modo de configuración de IP es estático; indefinido cuando DHCP	Solo lectura
netmask	Máscara de red del PIF. Se define aquí cuando el modo de configuración de IP es estático; indefinido cuando lo suministra DHCP	Solo lectura
gateway	Dirección de puerta de enlace del PIF. Se define aquí cuando el modo de configuración de IP es estático; indefinido cuando lo suministra DHCP	Solo lectura
DNS	Dirección DNS del PIF. Se define aquí cuando el modo de configuración de IP es estático; indefinido cuando lo suministra DHCP	Solo lectura
io_read_kbs	Velocidad de lectura media en kb/s para el dispositivo	Solo lectura
io_write_kbs	Velocidad de escritura promedio en kb/s para el dispositivo	Solo lectura
carrier	Estado del enlace para este dispositivo	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
vendor-id	El identificador asignado al proveedor de NIC	Solo lectura
vendor-name	Nombre del proveedor de NIC	Solo lectura
device-id	El identificador asignado por el proveedor a este modelo de NIC	Solo lectura
device-name	El nombre asignado por el proveedor a este modelo de NIC	Solo lectura
speed	Velocidad de transferencia de datos de la NIC	Solo lectura
duplex	Modo dúplex de la NIC; completo o medio	Solo lectura
pci-bus-path	Dirección de ruta de bus PCI	Solo lectura
other-config: ethtoolspeed	Establece la velocidad de conexión en Mbps	Lectura/Escritura
other-config: ethtoolautoneg	Actívela para inhabilitar la negociación automática de la interfaz física o el puente. El valor predeterminado es sí.	Lectura/Escritura
other-config: ethtoolduplex	Establece la capacidad de duplexación de la PIF, ya sea completa o media.	Lectura/Escritura
other-config:ethtool-rx	Actívela para habilitar la suma de comprobación de recepción y desactívela para inhabilitarla.	Lectura/Escritura
other-config:ethtool-tx	Actívela para habilitar la suma de comprobación de transmisión y desactívela para inhabilitarla.	Lectura/Escritura
other-config:ethtool-sg	Actívela para activar la recopilación de dispersión y desactívela para inhabilitarla.	Lectura/Escritura
other-config:ethtool-tso	Actívela para habilitar la descarga de segmentación de TCP y desactívela para inhabilitarla.	Lectura/Escritura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
other-config:ethtool-ufo	Actívela para habilitar la descarga de fragmentos UDP y desactívela para inhabilitarla.	Lectura/Escritura
other-config:ethtool-gso	Actívela para habilitar la descarga de segmentación genérica y desactívela para inhabilitarla.	Lectura/Escritura
other-config:domain	Lista separada por comas utilizada para establecer la ruta de búsqueda de DNS	Lectura/Escritura
other-config:bondmiimon	Intervalo entre comprobaciones de vida de enlace, en milisegundos	Lectura/Escritura
other-config:bonddowndelay	Número de milisegundos a esperar después de que se pierde el enlace antes de considerar realmente que el enlace se ha ido. Este parámetro permite la pérdida de enlace transitoria	Lectura/Escritura
other-config:bondupdelay	Número de milisegundos a esperar después de que aparezca el enlace antes de considerarlo realmente. Permite que los enlaces se activen. El valor predeterminado es 31s para permitir que los conmutadores comiencen a reenviar el tráfico.	Lectura/Escritura
disallow-unplug	True si este PIF es una NIC de almacenamiento dedicada, falso en caso contrario	Lectura/Escritura

> **Nota:**
>
> Los cambios realizados en los campos other-config de un PIF solo surtirán efecto después de un reinicio. También puede utilizar los comandos xe pif-unplug y xe pif-plug para

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> hacer que se reescriba la configuración de PIF.

pif-forget

```
xe pif-forget uuid=uuid_of_pif
<!--NeedCopy-->
```

Destruye el objeto PIF especificado en un host en particular.

pif-introduce

```
xe pif-introduce host-uuid=host_uuid mac=mac_address_for_pif device=
    interface_name
<!--NeedCopy-->
```

Cree un objeto PIF que represente una interfaz física en el host de XenServer especificado.

pif-plug

```
xe pif-plug uuid=uuid_of_pif
<!--NeedCopy-->
```

Intente abrir la interfaz física especificada.

pif-reconfigure-ip

```
xe pif-reconfigure-ip uuid=uuid_of_pif [mode=dhcp|mode=static] gateway=
    network_gateway_address IP=static_ip_for_this_pif netmask=
    netmask_for_this_pif [DNS=dns_address]
<!--NeedCopy-->
```

Modifique la dirección IP del PIF. Para la configuración de IP estática, establezca el parámetro `mode` en **`static`**, con los parámetros `gateway`, `IP` y `netmask` establecidos en los valores apropiados. Para usar DHCP, defina el parámetro `mode` en `DHCP` y deje los parámetros estáticos sin definir.

> **Nota:**
>
> El uso de direcciones IP estáticas en interfaces de red físicas conectadas a un puerto de un conmutador que utiliza Spanning Tree Protocol con STP Fast Link desactivado (o no compatible) da como resultado un período durante el cual no hay tráfico.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

pif-reconfigure-ipv6

```
xe pif-reconfigure-ipv6 uuid=uuid_of_pif mode=mode [gateway=
    network_gateway_address] [IPv6=static_ip_for_this_pif] [DNS=
    dns_address]
<!--NeedCopy-->
```

Vuelva a configurar la configuración de la dirección IPv6 en un PIF.

pif-scan

```
xe pif-scan host-uuid=host_uuid
<!--NeedCopy-->
```

Busque nuevas interfaces físicas en el host de XenServer.

pif-set-primary-address-type

```
xe pif-set-primary-address-type  uuid=uuid primary_address_type=
    address_type
<!--NeedCopy-->
```

Cambie el tipo de dirección principal que utiliza este PIF.

pif-unplug

```
xe pif-unplug uuid=uuid_of_pif
<!--NeedCopy-->
```

Intente desactivar la interfaz física especificada.

Comandos de agrupación

Comandos para trabajar con grupos. Un *grupo* es un conjunto de uno o más hosts de XenServer. Un grupo usa uno o más repositorios de almacenamiento compartidos para que las máquinas virtuales que se ejecutan en un host del grupo se puedan migrar casi en tiempo real a otro host del grupo. Esta migración se produce mientras la VM sigue en ejecución, sin que sea necesario apagarla y volver a activarla.

Cada host de XenServer es en realidad un grupo que consta de un solo miembro de forma predeterminada. Cuando el host de XenServer se une a un grupo, se designa como miembro. Si el grupo al que está unido el anfitrión consta de un solo miembro, ese miembro pasa a ser el coordinador del grupo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si el grupo al que está unido el anfitrión ya tiene varios miembros, uno de estos miembros ya es el coordinador del grupo y seguirá siéndolo cuando el nuevo anfitrión se una al grupo.

El objeto de agrupación singleton se puede enumerar con el comando estándar de listado de objetos (`xe pool-list`). Sus parámetros se pueden manipular con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

Parámetros de la agrupación

Los grupos tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
`uuid`	La referencia única de identificador/objeto para el grupo	Solo lectura
`name-label`	El nombre de la agrupación	Lectura/Escritura
`name-description`	La cadena de descripción de la agrupación	Lectura/Escritura
`master`	La referencia única de identificador/objeto del host de XenServer designado como coordinador del grupo	Solo lectura
`default-SR`	La referencia única de identificador/objeto del SR predeterminado para el grupo	Lectura/Escritura
`crash-dump-SR`	La referencia única de identificador/objeto del SR donde se guardan los volcados de memoria para los miembros del grupo	Lectura/Escritura
`metadata-vdis`	Todos los VDI de metadatos conocidos para el grupo	Solo lectura
`suspend-image-SR`	La referencia única de identificador/objeto del SR donde se guardan las VM suspendidas en los miembros del grupo	Lectura/Escritura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
other-config	Una lista de pares clave/valor que especifican parámetros de configuración adicionales para el grupo	Parámetro de mapa de lectura y escritura
supported-sr-types	Tipos de SR que puede usar este grupo	Solo lectura
ha-enabled	True si la alta disponibilidad está habilitada para el grupo, falso en caso contrario	Solo lectura
ha-configuration	Reservado para uso futuro.	Solo lectura
ha-statefiles	Enumera los UUID de los VDI que utiliza HA para determinar el estado del almacenamiento	Solo lectura
ha-host-failures-to-tolerate	La cantidad de errores de host que se deben tolerar antes de enviar una alerta del sistema	Lectura/Escritura
ha-plan-exists-**for**	El número de fallos de hosts que realmente se pueden gestionar, de acuerdo con los cálculos del algoritmo de alta disponibilidad	Solo lectura
ha-allow-overcommit	True si se permite que el grupo se comprometa en exceso, False en caso contrario	Lectura/Escritura
ha-overcommitted	True si el grupo está sobrecomprometido	Solo lectura
blobs	almacén de datos binarios	Solo lectura
live-patching-disabled	Se establece en False para habilitar la aplicación de parches en vivo. Establézcala en True para inhabilitar la aplicación de parches en vivo.	Lectura/Escritura
igmp-snooping-enabled	Se establece en True para habilitar la indagación IGMP. Establézcala en False para inhabilitar la indagación IGMP.	Lectura/Escritura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
https-only	Establézcalo en False para permitir que los clientes externos que utilizan la API de administración se conecten a XenServer mediante HTTPS a través del puerto 443 o HTTP a través del puerto 80. Establézcalo en True para bloquear el puerto 80 y exigir que los clientes se conecten exclusivamente mediante HTTPS a través del puerto 443.	Lectura/Escritura
migration-compression	Configúrelo en True para habilitar la compresión del flujo de migración para el grupo de XenServer. Establézcalo en False para inhabilitar la compresión del flujo de migración. El valor predeterminado es False. Puede ser anulado por el parámetro del comando vm-migratecompress.	Lectura/Escritura

pool-apply-edition

```
xe pool-apply-edition edition=edition [uuid=uuid] [license-server-
    address=address] [license-server-port=port]
<!--NeedCopy-->
```

Aplica una edición en toda la agrupación.

pool-certificate-install

```
xe pool-certificate-install filename=file_name
<!--NeedCopy-->
```

Instale un certificado TLS en todo el grupo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

pool-certificate-list

```
xe pool-certificate-list
<!--NeedCopy-->
```

Enumera todos los certificados TLS instalados en un grupo.

pool-certificate-sync

```
xe pool-certificate-sync
<!--NeedCopy-->
```

Sincronice certificados TLS y listas de revocación de certificados del coordinador del grupo con los otros miembros del grupo.

pool-certificate-uninstall

```
xe pool-certificate-uninstall name=name
<!--NeedCopy-->
```

Desinstale un certificado TLS.

pool-crl-install

```
xe pool-crl-install filename=file_name
<!--NeedCopy-->
```

Instale una lista de revocación de certificados TLS para todo el grupo.

pool-crl-list

```
xe pool-crl-list
<!--NeedCopy-->
```

Enumera todas las listas de revocación de certificados TLS instaladas.

pool-crl-uninstall

```
xe pool-crl-uninstall name=name
<!--NeedCopy-->
```

Desinstale una lista de revocación de certificados TLS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

pool-deconfigure-wlb

```
xe pool-deconfigure-wlb
<!--NeedCopy-->
```

Elimine permanentemente la configuración para equilibrar la carga de trabajo.

pool-designate-new-master

```
xe pool-designate-new-master host-uuid=uuid_of_new_master
<!--NeedCopy-->
```

Indique al host de XenServer miembro especificado que se convierta en el coordinador (antes denominado "maestro") de un grupo existente. Este comando realiza un traspaso ordenado de la función de coordinador del grupo a otro host del grupo de recursos. Este comando solo funciona cuando el coordinador del grupo actual está en línea. No reemplaza los comandos del modo de emergencia que se enumeran a continuación.

pool-disable-external-auth

```
xe pool-disable-external-auth [uuid=uuid] [config=config]
<!--NeedCopy-->
```

Inhabilita la autenticación externa en todos los hosts de un grupo.

pool-disable-local-storage-caching

```
xe pool-disable-local-storage-caching uuid=uuid
<!--NeedCopy-->
```

Inhabilite el almacenamiento en caché local en todo el grupo.

pool-disable-redo-log

```
xe pool-disable-redo-log
<!--NeedCopy-->
```

Inhabilite el registro de rehacer si se está usando, a menos que se habilite HA.

pool-dump-database

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe pool-dump-database file-name=filename_to_dump_database_into_(
    on_client)
<!--NeedCopy-->
```

Descargue una copia de toda la base de datos del grupo y viértala en un archivo en el cliente.

pool-enable-external-auth

```
xe pool-enable-external-auth  auth-type=auth_type service-name=
    service_name [uuid=uuid] [config:=config]
<!--NeedCopy-->
```

Permite la autenticación externa en todos los hosts de un grupo. Tenga en cuenta que algunos valores de `auth-type` requerirán valores `config:` particulares.

pool-enable-local-storage-caching

```
xe pool-enable-local-storage-caching uuid=uuid
<!--NeedCopy-->
```

Habilite el almacenamiento en caché local en todo el grupo.

pool-enable-redo-log

```
xe pool-ensable-redo-log sr-uuid=sr_uuid
<!--NeedCopy-->
```

Habilite el registro de rehacer en el SR dado si está en uso, a menos que la alta disponibilidad esté habilitada.

pool-eject

```
xe pool-eject host-uuid=uuid_of_host_to_eject
<!--NeedCopy-->
```

Indique al host XenServer especificado que abandone un grupo existente.

pool-emergency-reset-master

```
xe pool-emergency-reset-master master-address=address_of_pool_master
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Indique al anfitrión miembro del grupo que restablezca la dirección del coordinador del grupo al nuevo valor e intente conectarse a él. No ejecute este comando en los coordinadores del grupo.

pool-emergency-transition-to-master

```
xe pool-emergency-transition-to-master
<!--NeedCopy-->
```

Indique a un host miembro de XenServer que se convierta en el coordinador del grupo (antes denominado "el maestro del grupo"). El host XenServer acepta este comando solo después de que el host haya pasado al modo de emergencia. El modo de emergencia significa que es un miembro de un grupo cuyo coordinador ha desaparecido de la red y no se puede contactar con él tras varios intentos.

Si la contraseña del host se ha modificado desde que el host se unió al grupo, este comando puede provocar que se restablezca la contraseña del host. Para obtener más información, consulte (Comandos del usuario).

pool-ha-enable

```
xe pool-ha-enable heartbeat-sr-uuids=uuid_of_heartbeat_sr
<!--NeedCopy-->
```

Habilite la alta disponibilidad en la agrupación de recursos, mediante el UUID SR especificado como repositorio de latido de almacenamiento central.

pool-ha-disable

```
xe pool-ha-disable
<!--NeedCopy-->
```

Inhabilita la función de alta disponibilidad en el grupo de recursos.

pool-ha-compute-hypothetical-max-host-failures-to-tolerate

Calcule el número máximo de errores de host que se deben tolerar en la configuración de grupo actual.

pool-ha-compute-max-host-failures-to-tolerate

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe pool-ha-compute-hypothetical-max-host-failures-to-tolerate [vm-uuid=
    vm_uuid] [restart-priority=restart_priority]
<!--NeedCopy-->
```

Calcule la cantidad máxima de errores de host que se deben tolerar con las máquinas virtuales protegidas propuestas y suministradas.

pool-initialize-wlb

```
xe pool-initialize-wlb wlb_url=url wlb_username=wlb_username
    wlb_password=wlb_password xenserver_username=username
    xenserver_password=password
<!--NeedCopy-->
```

Inicialice el equilibrio de carga de trabajo del grupo actual con el servidor de equilibrio de carga de trabajo de destino

pool-join

```
xe pool-join master-address=address master-username=username master-
    password=password
<!--NeedCopy-->
```

Indique al host de XenServer que se una a un grupo existente.

pool-management-reconfigure

```
xe pool-management-reconfigure [network-uuid=network-uuid]
<!--NeedCopy-->
```

Reconfigura la interfaz de administración de todos los hosts del grupo para que usen la interfaz de red especificada, que es la interfaz que se usa para conectarse a XenCenter. El comando reescribe la clave MANAGEMENT_INTERFACE en `/etc/xensource-inventory` para todos los hosts del grupo.

Si se especifica el nombre del dispositivo de una interfaz (que debe tener una dirección IP), el coordinador del grupo de XenServer se vuelve a vincular inmediatamente. Este comando funciona tanto en modo normal como de emergencia.

A partir del UUID de red especificado, el UUID del objeto PIF se identifica y se asigna al host de XenServer, que determina qué dirección IP se debe volver a vincular a sí mismo. No debe estar en modo de emergencia cuando se ejecute este comando.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Advertencia:**
>
> Tenga cuidado al usar este comando CLI fuera del host y asegúrese de tener conectividad de red en la nueva interfaz. Use `xe pif-reconfigure` para configurar uno primero. De lo contrario, los comandos CLI posteriores no podrán acceder al host de XenServer.

pool-recover-slaves

```
xe pool-recover-slaves
<!--NeedCopy-->
```

Indique al coordinador de la agrupación que intente restablecer la dirección de todos los miembros que se encuentran actualmente en modo de emergencia. Este comando se utiliza normalmente después de `pool-emergency-transition-to-master` que se haya utilizado para establecer a uno de los miembros como el nuevo coordinador del grupo.

pool-restore-database

```
xe pool-restore-database file-name=filename_to_restore_from_on_client [
    dry-run=true|false]
<!--NeedCopy-->
```

Cargue una copia de seguridad de base de datos (creada con `pool-dump-database`) en un grupo. Al recibir la carga, el coordinador del grupo se reinicia con la nueva base de datos.

También hay una opción de *ejecución en seco*, que le permite comprobar que la base de datos del grupo se puede restaurar sin realizar la operación. De forma predeterminada, `dry-run` se establece en false.

pool-retrieve-wlb-configuration

```
xe pool-retrieve-wlb-configuration
<!--NeedCopy-->
```

Recupera los criterios de optimización del grupo del servidor de equilibrio de carga de trabajo.

pool-retrieve-wlb-diagnostics

```
xe pool-retrieve-wlb-diagnostics [filename=file_name]
<!--NeedCopy-->
```

Recupera los diagnósticos del servidor de equilibrio de carga de trabajo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

pool-retrieve-wlb-recommendations

```
xe pool-retrieve-wlb-recommendations
<!--NeedCopy-->
```

Recupera recomendaciones de migración de VM para el grupo desde el servidor de equilibrio de carga de trabajo.

pool-retrieve-wlb-report

```
xe pool-retrieve-wlb-report report=report [filename=file_name]
<!--NeedCopy-->
```

Recupera informes del servidor de equilibrio de carga de trabajo.

pool-secret-rotate

```
xe pool-secret-rotate
<!--NeedCopy-->
```

Gira el secreto de la agrupación.

El secreto del grupo es un secreto compartido entre los hosts de XenServer de un grupo que permite al host demostrar su pertenencia a un grupo. Los usuarios con el rol de administrador del grupo pueden ver este secreto cuando se conectan al host a través de SSH. Rote el secreto del grupo si uno de estos usuarios abandona su organización o pierde su función de administrador del grupo.

pool-send-test-post

```
xe pool-send-test-post dest-host=destination_host dest-port=
   destination_port body=post_body
<!--NeedCopy-->
```

Envíe el cuerpo dado al host y puerto dados, mediante HTTPS, e imprima la respuesta. Se usa para depurar la capa TLS.

pool-send-wlb-configuration

```
xe pool-send-wlb-configuration [config:=config]
<!--NeedCopy-->
```

Establece los criterios de optimización del grupo para el servidor de equilibrio de carga de trabajo

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

pool-sync-database

```
xe pool-sync-database
<!--NeedCopy-->
```

Forzar la sincronización de la base de datos del grupo en todos los hosts del grupo de recursos. Este comando no es necesario en el funcionamiento normal, ya que la base de datos se replica automáticamente de forma regular. Sin embargo, el comando puede ser útil para garantizar que los cambios se repliquen rápidamente después de realizar un conjunto significativo de operaciones de CLI.

Establecer https-only

```
xe pool-param-set [uuid=pool-uuid] [https-only=true|false]
<!--NeedCopy-->
```

Habilita o inhabilita el bloqueo del puerto 80 en la interfaz de administración de los hosts de XenServer.

Comandos del acelerador PVS

Comandos para trabajar con el acelerador PVS.

pvs-cache-storage-create

```
xe pvs-cache-storage-create sr-uuid=sr_uuid pvs-site-uuid=pvs_site_uuid
    size=size
<!--NeedCopy-->
```

Configure una memoria caché de PVS en un SR determinado para un host determinado.

pvs-cache-storage-destroy

```
xe pvs-cache-storage-destroy uuid=uuid
<!--NeedCopy-->
```

Elimina una memoria caché de PVS.

pvs-proxy-create

```
xe pvs-proxy-create pvs-site-uuid=pvs_site_uuid vif-uuid=vif_uuid
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configure una VM/VIF para que use un proxy PVS.

pvs-proxy-destroy

```
xe pvs-proxy-destroy uuid=uuid
<!--NeedCopy-->
```

Elimine (o apague) un proxy PVS para esta VIF/VM.

pvs-server-forget

```
xe pvs-server-forget uuid=uuid
<!--NeedCopy-->
```

Olvídese de un servidor PVS.

pvs-server-introduce

```
xe pvs-server-introduce addresses=adresses first-port=first_port last-
    port=last_port pvs-site-uuid=pvs_site_uuid
<!--NeedCopy-->
```

Introducir un nuevo servidor PVS.

pvs-site-forget

```
xe pvs-site-forget uuid=uuid
<!--NeedCopy-->
```

Olvídate de un sitio PVS.

pvs-site-introduce

```
xe pvs-site-introduce name-label=name_label [name-description=
    name_description] [pvs-uuid=pvs_uuid]
<!--NeedCopy-->
```

Presentamos el nuevo sitio de PVS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

comandos de Storage Manager

Comandos para controlar los complementos de Storage Manager.

Los objetos del administrador de almacenamiento se pueden enumerar con el comando estándar de listado de objetos (`xe sm-list`). Los parámetros se pueden manipular con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

Parámetros SM

Los SM tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
`uuid`	La referencia única de identificador/objeto para el complemento SM	Solo lectura
`name-label`	El nombre del complemento SM	Solo lectura
`name-description`	La cadena de descripción del complemento SM	Solo lectura
`type`	El tipo de SR al que se conecta este complemento	Solo lectura
`vendor`	Nombre del proveedor que creó este complemento	Solo lectura
`copyright`	Declaración de derechos de autor para este complemento SM	Solo lectura
`required-api-version`	Se requiere una versión mínima de la API SM en el host de XenServer	Solo lectura
`configuration`	Nombres y descripciones de las claves de configuración de dispositivos	Solo lectura
`capabilities`	Capacidades del complemento SM	Solo lectura
`driver-filename`	Nombre de archivo del controlador SR.	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Comandos de instantáneas

Comandos para trabajar con instantáneas.

snapshot-clone

```
xe snapshot-clone new-name-label=name_label [uuid=uuid] [new-name-
    description=description]
<!--NeedCopy-->
```

Cree una nueva plantilla mediante la clonación de una instantánea existente, mediante la operación de clonación rápida de discos en el nivel de almacenamiento cuando esté disponible.

snapshot-copy

```
xe snapshot-copy new-name-label=name_label [uuid=uuid] [new-name-
    description=name_description] [sr-uuid=sr_uuid]
<!--NeedCopy-->
```

Cree una nueva plantilla copiando una VM existente, pero sin usar la operación de clonación rápida de disco a nivel de almacenamiento (incluso si está disponible). Se garantiza que las imágenes de disco de la máquina virtual copiada serán "imágenes completas", es decir, no formarán parte de una cadena CoW.

snapshot-destroy

```
xe snapshot-destroy  [uuid=uuid] [snapshot-uuid=snapshot_uuid]
<!--NeedCopy-->
```

Destruye una instantánea. Esto deja intacto el almacenamiento asociado a la instantánea. Para eliminar el almacenamiento también, use snapshot-uninstall.

snapshot-disk-list

```
xe snapshot-disk-list [uuid=uuid] [snapshot-uuid=snapshot_uuid] [vbd-
    params=vbd_params] [vdi-params=vdi_params]
<!--NeedCopy-->
```

Enumera los discos en las VM seleccionadas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

snapshot-export-to-template

```
xe snapshot-export-to-template filename=file_name snapshot-uuid=
    snapshot_uuid  [preserve-power-state=true|false]
<!--NeedCopy-->
```

Exportar una instantánea a un *nombre de archivo*.

snapshot-reset-powerstate

```
xe snapshot-reset-powerstate [uuid=uuid] [snapshot-uuid=snapshot_uuid]
    [--force]
<!--NeedCopy-->
```

Forzar que el estado de energía de la VM se detenga solo en la base de datos de la pila de herramientas Este comando se usa para recuperar una instantánea que está marcada como "suspendida". Se trata de una operación potencialmente peligrosa: debe asegurarse de que ya no necesita la imagen de memoria. Ya no podrás reanudar la instantánea.

snapshot-revert

```
xe snapshot-revert [uuid=uuid] [snapshot-uuid=snapshot_uuid]
<!--NeedCopy-->
```

Revertir una VM existente a un estado de punto de control o instantánea anterior.

snapshot-uninstall

```
xe snapshot-uninstall [uuid=uuid] [snapshot-uuid=snapshot_uuid] [--
    force]
<!--NeedCopy-->
```

Desinstale una instantánea. Esta operación destruirá los VDI marcados como RW y conectados solo a esta instantánea. Para destruir simplemente el registro de VM, use snapshot-destroy.

Comandos SR

Comandos para controlar los SR (repositorios de almacenamiento).

Los objetos de SR se pueden enumerar con el comando estándar de lista de objetos (`xe sr-list`) y los parámetros manipulados con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Parámetros de SR

Los SR tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
uuid	La referencia única de identificador/objeto para el SR	Solo lectura
name-label	El nombre de la SR	Lectura/Escritura
name-description	La cadena de descripción de la SR	Lectura/Escritura
host	Nombre de host del repositorio de almacenamiento	Solo lectura
allowed-operations	Lista de las operaciones permitidas en el SR en este estado	Parámetro de conjunto de solo lectura
current-operations	Lista de las operaciones que están actualmente en curso en este SR	Parámetro de conjunto de solo lectura
VDIs	Referencia única de identificador/objeto para los discos virtuales de esta SR	Parámetro de conjunto de solo lectura
PBDs	Referencia de identificador/objeto única para los PBD adjuntos a este SR	Parámetro de conjunto de solo lectura
virtual-allocation	Suma de los valores de tamaño virtual de todos los VDI en este repositorio de almacenamiento (en bytes)	Solo lectura
physical-utilisation	Espacio físico utilizado actualmente en este SR, en bytes. Para los formatos de disco de aprovisionamiento delgado, la utilización física puede ser inferior a la asignación virtual.	Solo lectura
physical-size	Tamaño físico total de la SR, en bytes	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
type	Tipo de SR, que se utiliza para especificar el controlador de back-end de SR que se va a usar	Solo lectura
content-type	El tipo de contenido de la SR. Se utiliza para distinguir las bibliotecas ISO de otras SR. Para los repositorios de almacenamiento que almacenan una biblioteca de ISO, se content-typedebe establecer eniso. En otros casos, le recomendamos que establezca este parámetro en vacío o en el usuario de cadena.	Solo lectura
shared	Es cierto si este SR se puede compartir entre varios hosts. De lo contrario, es falso.	Lectura/Escritura
introduced-by	El drtask (si lo hay) que introdujo el SR	Solo lectura
is-tools-sr	Cierto si se trata del SR que contiene los VDI ISO de Tools. De lo contrario, es falso.	Solo lectura
other-config	Lista de pares clave/valor que especifican parámetros de configuración adicionales para el SR	Parámetro de mapa de lectura y escritura
sm-config	Datos dependientes de SM	Parámetro de mapa de solo lectura
blobs	almacén de datos binarios	Solo lectura
local-cache-enabled	Verdadero si este SR está asignado como la caché local de su host. De lo contrario, es falso.	Solo lectura
tags	Etiquetas especificadas por el usuario para fines de categorización	Parámetro establecido de lectura/escritura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
clustered	Es cierto que el SR utiliza almacenamiento local agregado. De lo contrario, es falso.	Solo lectura

sr-create

```
xe sr-create name-label=name physical-size=size type=type content-type=
    content_type device-config:config_name=value [host-uuid=host_uuid] [
    shared=true|false]
<!--NeedCopy-->
```

Crea un SR en el disco, lo introduce en la base de datos y crea un PBD que conecta el SR al host de XenServer. Si `shared` se establece en **`true`**, se crea un PBD para cada host de XenServer del grupo. Si `shared` no se especifica ni se establece en **`false`**, se crea un PBD solo para el host XenServer especificado con `host-uuid`.

Los parámetros `device-config` exactos difieren según el dispositivo `type`. Para obtener más información sobre estos parámetros en los distintos back-ends de almacenamiento, consulte Crear una SR .

sr-data-source-forget

```
xe sr-data-source-forget data-source=data_source
<!--NeedCopy-->
```

Deje de grabar la fuente de datos especificada para una SR y olvide todos los datos grabados.

sr-data-source-list

```
xe sr-data-source-list
<!--NeedCopy-->
```

Enumere las fuentes de datos que se pueden grabar para una SR.

sr-data-source-query

```
xe sr-data-source-query data-source=data_source
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Consulte el último valor leído de un origen de datos de SR.

sr-data-source-record

```
xe sr-data-source-record  data-source=data_source
<!--NeedCopy-->
```

Registre la fuente de datos especificada para un SR.

sr-destroy

```
xe sr-destroy uuid=sr_uuid
<!--NeedCopy-->
```

Destruye el SR especificado en el host de XenServer.

sr-enable-database-replication

```
xe sr-enable-database-replication uuid=sr_uuid
<!--NeedCopy-->
```

Permite la replicación de base de datos XAPI en el SR especificado (compartido).

sr-disable-database-replication

```
xe sr-disable-database-replication uuid=sr_uuid
<!--NeedCopy-->
```

Inhabilita la replicación de base de datos XAPI en el SR especificado.

sr-forget

```
xe sr-forget uuid=sr_uuid
<!--NeedCopy-->
```

El agente XAPI olvida un SR específico en el host de XenServer. Cuando el agente XAPI olvida un SR, el SR se separa y no puede acceder a los VDI en él, pero permanece intacto en el medio de origen (los datos no se pierden).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

sr-introduce

```
xe sr-introduce name-label=name physical-size=physical_size type=type
    content-type=content_type uuid=sr_uuid
<!--NeedCopy-->
```

Simplemente coloca un registro SR en la base de datos. Use `device-config` para especificar parámetros adicionales en la forma `device-config:parameter_key=parameter_value`. Por ejemplo:

```
xe sr-introduce device-config:device=/dev/sdb1
<!--NeedCopy-->
```

> **Nota:**
>
> Este comando nunca se usa en funcionamiento normal. Esta operación avanzada puede ser útil cuando un SR debe reconfigurarse como compartido después de que se creó o para ayudar a recuperarse de varios casos de error.

sr-probe

```
xe sr-probe type=type [host-uuid=host_uuid] [device-config:config_name=
    value]
<!--NeedCopy-->
```

Realiza un escaneo del backend con las claves `device-config` proporcionadas. Si el comando `device-config` devuelve una lista de los SRs presentes en el dispositivo, si los hay. Si los`device-config` parámetros son solo parciales, se realiza un análisis específico de back-end, que devuelve resultados que le guiarán en la mejora de los`device-config` parámetros restantes. Los resultados del análisis se devuelven como XML específico para el back-end, impresos en la CLI.

Los parámetros `device-config` exactos difieren según el dispositivo `type`. Para obtener detalles de estos parámetros en los diferentes back-ends de almacenamiento, consulte Almacenamiento.

sr-probe-ext

```
xe sr-probe-ext type=type [host-uuid=host_uuid] [device-config:=config]
     [sm-config:-sm_config]
<!--NeedCopy-->
```

Realice una sonda de almacenamiento. Los parámetros device-config se pueden especificar, por ejemplo, device-config:devs=/dev/sdb1. A diferencia de sr-probe, este comando devuelve resultados en el mismo formato legible por humanos para cada tipo de SR.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

sr-scan

```
xe sr-scan uuid=sr_uuid
<!--NeedCopy-->
```

Forzar un escaneo de SR, sincronizando la base de datos XAPI con los VDI presentes en el sustrato de almacenamiento subyacente.

sr-update

```
xe sr-update uuid=uuid
<!--NeedCopy-->
```

Actualice los campos del objeto SR en la base de datos.

lvhd-enable-thin-provisioning

```
xe lvhd-enable-thin-provisioning  sr-uuid=sr_uuid initial-allocation=
   initial_allocation allocation-quantum=allocation_quantum
<!--NeedCopy-->
```

Habilite el aprovisionamiento ligero en una SR LVHD.

Comandos de materia

Comandos para trabajar con sujetos.

session-subject-identifier-list

```
xe session-subject-identifier-list
<!--NeedCopy-->
```

Devuelve una lista de todos los identificadores de sujeto de usuario de todas las sesiones existentes autenticadas externamente.

session-subject-identifier-logout

```
xe session-subject-identifier-logout subject-identifier=
   subject_identifier
<!--NeedCopy-->
```

Cierre sesión en todas las sesiones autenticadas externamente asociadas a un identificador de asunto de usuario.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

session-subject-identifier-logout-all

```
xe session-subject-identifier-logout-all
<!--NeedCopy-->
```

Cierre sesión en todas las sesiones autenticadas externamente.

subject-add

```
xe subject-add subject-name=subject_name
<!--NeedCopy-->
```

Agregue un tema a la lista de temas que pueden acceder al grupo.

subject-remove

```
xe subject-remove subject-uuid=subject_uuid
<!--NeedCopy-->
```

Elimina un tema de la lista de temas que pueden acceder al grupo.

subject-role-add

```
xe subject-role-add uuid=uuid [role-name=role_name] [role-uuid=
    role_uuid]
<!--NeedCopy-->
```

Agrega una función a una asignatura.

subject-role-remove

```
xe subject-role-remove uuid=uuid [role-name=role_name] [role-uuid=
    role_uuid]
<!--NeedCopy-->
```

Elimina una función de una asignatura.

secret-create

```
xe secret-create value=value
<!--NeedCopy-->
```

Crea un secreto.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

secret-destroy

```
xe secret-destroy uuid=uuid
<!--NeedCopy-->
```

Destruye un secreto.

Comandos de tareas

Comandos para trabajar con tareas asíncronas de larga ejecución. Estos comandos son tareas como iniciar, detener y suspender una máquina virtual. Las tareas se componen típicamente de un conjunto de otras subtareas atómicas que juntas llevan a cabo la operación solicitada.

Los objetos de tarea se pueden enumerar con el comando estándar de listado de objetos (`xe task -list`) y los parámetros manipulados con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

Parámetros de tareas

Las tareas tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
`uuid`	La referencia única de identificador/objeto para la tarea	Solo lectura
`name-label`	El nombre de la tarea	Solo lectura
`name-description`	La cadena de descripción de la tarea	Solo lectura
`resident-on`	La referencia única de identificador/objeto del host en el que se ejecuta la tarea	Solo lectura
`status`	Estado de la tarea	Solo lectura
`progress`	Si la tarea sigue pendiente, este campo contiene el porcentaje estimado completado, de 0 a 1. Si la tarea se ha completado, con éxito o sin éxito, el valor es 1.	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
type	Si la tarea se ha completado correctamente, este parámetro contiene el tipo de resultado codificado. El tipo es el nombre de la clase cuya referencia se encuentra en el campo de resultados. De lo contrario, el valor de este parámetro no está definido	Solo lectura
result	Si la tarea se ha completado correctamente, este campo contiene el valor del resultado, ya sea Nulo o una referencia a objeto; de lo contrario, el valor de este parámetro no está definido	Solo lectura
error_info	Si la tarea ha fallado, este parámetro contiene el conjunto de cadenas de error asociadas. De lo contrario, el valor de este parámetro no está definido	Solo lectura
allowed_operations	Lista de las operaciones permitidas en este estado	Solo lectura
created	Hora en que se creó la tarea	Solo lectura
finished	Hora de finalización de la tarea (es decir, correcta o fallida). Si el estado de la tarea está pendiente, el valor de este campo no tiene significado	Solo lectura
subtask_of	Contiene el UUID de las tareas de las que esta tarea es una subtarea	Solo lectura
subtasks	Contiene los UUID de todas las subtareas de esta tarea	Solo lectura

task-cancel

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe task-cancel [uuid=task_uuid]
<!--NeedCopy-->
```

Indique a la tarea especificada que se cancele y devuelva.

Comandos de plantilla

Comandos para trabajar con plantillas de VM.

Las plantillas son esencialmente máquinas virtuales con el parámetro `is-a-template` establecido en **`true`**. Una plantilla es una "imagen dorada"que contiene todas las distintas opciones de configuración para crear instancias de una VM específica. XenServer incluye un conjunto básico de plantillas, que son máquinas virtuales genéricas "sin procesar"que pueden arrancar un CD de instalación de un proveedor de sistemas operativos (por ejemplo: RHEL, CentOS, SLES, Windows). Puede crear máquinas virtuales, configurarlas en formularios estándar para sus necesidades particulares y guardar una copia de ellas como plantillas para usarlas en el futuro en la implementación de máquinas virtuales.

Los objetos de plantilla se pueden enumerar con el comando estándar de listado de objetos (`xe template-list`) y los parámetros manipulados con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

> **Nota:**
>
> Las plantillas no se pueden convertir directamente en máquinas virtuales estableciendo el parámetro `is-a-template` en **`false`**. Establecer el parámetro `is-a-template` en **`false`** no se admite y resulta en una máquina virtual que no se puede iniciar.

Parámetros de plantilla de VM

Las plantillas tienen los siguientes parámetros:

- `uuid` (solo lectura) la referencia única de identificador/objeto para la plantilla
- `name-label` (lectura/escritura) el nombre de la plantilla
- `name-description` (lectura/escritura) la cadena de descripción de la plantilla
- `user-version` (lectura/escritura) para creadores de máquinas virtuales y plantillas para poner información de versión
- `is-a-template` (lectura/escritura) true si esta máquina virtual es una plantilla.
  Las VM de plantilla nunca se pueden iniciar, solo se usan para clonar otras VM. Una vez que este valor se ha establecido en verdadero, no se puede restablecer en falso. Las máquinas virtuales de plantilla no se pueden convertir en máquinas virtuales con este parámetro.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puede convertir una máquina virtual en una plantilla con:

```
xe vm-param-set uuid=<vm uuid> is-a-template=true
<!--NeedCopy-->
```

- `is-control-domain` (solo lectura) true si se trata de un dominio de control (dominio 0 o un dominio de controlador)
- `power-state` (solo lectura) estado de energía actual. El valor siempre se detiene para una plantilla
- `memory-dynamic-max` (solo lectura) memoria dinámica máxima en bytes.
  Actualmente no se utiliza, pero si se cambia, se debe cumplir la siguiente restricción: `memory_static_max >= memory_dynamic_max >= memory_dynamic_min >= memory_static_min`.
- `memory-dynamic-min` (lectura/escritura) memoria mínima dinámica en bytes.
  No se usa actualmente, pero, si se cambia, se deben cumplir las mismas restricciones para `memory-dynamic-max`.
- `memory-static-max` (lectura/escritura) establece estáticamente (absoluta) la memoria máxima en bytes. Este campo es el valor principal que se utiliza para determinar la cantidad de memoria asignada a una VM.
- `memory-static-min` (lectura/escritura) establece estáticamente la memoria mínima (absoluta) en bytes.
  Este campo representa la memoria mínima absoluta y `memory-static-min` debe ser inferior a `memory-static-max`.
  Este valor no se utiliza en el funcionamiento normal, pero se debe cumplir la restricción anterior.
- `suspend-VDI-uuid` (solo lectura) la VDI en la que está almacenada una imagen suspendida (no significa nada para una plantilla)
- `VCPUs-params` (parámetro de mapa de lectura/escritura) para la directiva de vCPU seleccionada.

  Puede ajustar la fijación de una vCPU con:

```
xe template-param-set uuid=<template_uuid> vCPUs-params:mask
   =1,2,3
<!--NeedCopy-->
```

  Una máquina virtual creada a partir de esta plantilla se ejecuta solo en las CPU físicas 1, 2 y 3.

  También puede ajustar la prioridad de la vCPU (programación xen) con los parámetros de límite y peso. Por ejemplo:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe template-param-set uuid=<template_uuid> VCPUs-params:weight
   =512 xe template-param-set uuid=<template_uuid> VCPUs-params:
   cap=100
<!--NeedCopy-->
```

Una máquina virtual basada en esta plantilla con un peso de 512 obtiene el doble de CPU que un dominio con un peso de 256 en un host con competencia. Los pesos legales varían de 1 a 65535 y el valor predeterminado es 256.

El límite fija, de forma opcional, la cantidad máxima de CPU que puede consumir una máquina virtual basada en esta plantilla, incluso si el host XenServer tiene ciclos de CPU inactivos. El límite se expresa en porcentaje de una CPU física: 100 es 1 CPU física, 50 es media CPU, 400 son 4 CPU, etc. El valor predeterminado, 0, significa que no hay límite superior.

- `VCPUs-max` (lectura/escritura) cantidad máxima de vCPU
- `VCPUs-at-startup` (lectura/escritura) número de arranque de vCPU
- `actions-after-crash` (lectura/escritura) que se debe realizar cuando una máquina virtual basada en esta plantilla se bloquea
- `console-uuids` (parámetro establecido de solo lectura) dispositivos de consola virtual
- `platform` (parámetro de mapa de lectura/escritura) configuración específica de la plataforma

  Para inhabilitar la emulación de un puerto paralelo para los huéspedes:

```
xe vm-param-set uuid=<vm_uuid> platform:parallel=none
<!--NeedCopy-->
```

  Para inhabilitar la emulación de un puerto serie:

```
xe vm-param-set uuid=<vm_uuid> platform:hvm_serial=none
<!--NeedCopy-->
```

  Para inhabilitar la emulación de una controladora USB y una tableta USB:

```
xe vm-param-set uuid=<vm_uuid> platform:usb=false
xe vm-param-set uuid=<vm_uuid> platform:usb_tablet=false
<!--NeedCopy-->
```

- `allowed-operations` (parámetro de conjunto de solo lectura) lista de las operaciones permitidas en este estado
- `current-operations` (parámetro de conjunto de solo lectura) lista de las operaciones que están actualmente en curso en esta plantilla
- `allowed-VBD-devices` (parámetro conjunto de solo lectura) de identificadores VBD disponibles para su uso, representados por enteros del rango 0—15. Esta lista es solo informativa y se pueden usar otros dispositivos (pero puede que no funcionen).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- `allowed-VIF-devices` (parámetro conjunto de solo lectura) de identificadores VIF disponibles para su uso, representados por enteros del rango 0—15. Esta lista es solo informativa y se pueden usar otros dispositivos (pero puede que no funcionen).
- `HVM-boot-policy` (leer/escribir) la directiva de arranque para los huéspedes. Orden de BIOS o una cadena vacía.
- `HVM-boot-params` (parámetro del mapa de lectura/escritura) la tecla de orden controla el orden de arranque del invitado, representado como una cadena en la que cada carácter es un método de arranque: d para el CD/DVD, c para el disco raíz y n para el arranque PXE de red. El valor por defecto es dc.
- `PV-kernel` (lectura/escritura) al núcleo
- `PV-ramdisk` (lectura/escritura) a la `initrd`
- `PV-args` (lectura/escritura) de argumentos de línea de comandos del núcleo
- `PV-legacy-args` (lectura/escritura) de argumentos para hacer que las máquinas virtuales heredadas basadas en esta plantilla se inicien
- `PV-bootloader` (lectura/escritura) nombre o ruta al gestor de arranque
- `PV-bootloader-args` (lectura/escritura) de argumentos varios para el gestor de arranque
- `last-boot-CPU-flags` (solo lectura) describe los indicadores de CPU en los que se arrancó por última vez una máquina virtual basada en esta plantilla; no se rellenó para una plantilla
- `resident-on` (solo lectura) el host de XenServer en el que reside una máquina virtual basada en esta plantilla. Aparece como `not in database` para una plantilla
- `affinity` (lectura/escritura) el host de XenServer en el que prefiere ejecutarse una máquina virtual basada en esta plantilla. Utilizado por el comando `xe vm-start` para decidir dónde ejecutar la VM
- `other-config` (parámetro de mapa de lectura/escritura) lista de pares clave/valor que especifican parámetros de configuración adicionales para la plantilla
- `start-time` (solo lectura) marca de tiempo de la fecha y hora en que se leyeron las métricas de una VM basadas en esta plantilla, en el formulario `yyyymmddThh:mm:ss z`, donde z es el indicador de zona horaria militar de una sola letra, por ejemplo, Z para UTC (GMT). Establecer en `1 Jan 1970 Z` (comienzo de la época UNIX/POSIX) para una plantilla
- `install-time` (solo lectura) marca de tiempo de la fecha y hora en que se leyeron las métricas de una VM basadas en esta plantilla, en el formulario `yyyymmddThh:mm:ss z`, donde z es el indicador de zona horaria militar de una sola letra, por ejemplo, Z para UTC (GMT). Establecer en `1 Jan 1970 Z` (comienzo de la época UNIX/POSIX) para una plantilla
- `memory-actual` (solo lectura) la memoria real que utiliza una VM basada en esta plantilla; 0 para una plantilla

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- `VCPUs-number` (solo lectura) el número de CPU virtuales asignadas a una máquina virtual basada en esta plantilla; 0 para una plantilla
- `VCPUs-Utilization` (parámetro de asignación de solo lectura) Lista de CPU virtuales y su parámetro de peso de asignación de solo lectura `os-version` La versión del sistema operativo para una máquina virtual basada en esta plantilla. Aparece como `not in database` para una plantilla
- `PV-drivers-version` (parámetro de mapa de solo lectura) las versiones de los controladores paravirtualizados para una VM basada en esta plantilla. Aparece como `not in database` para una plantilla
- `PV-drivers-detected` (solo lectura) para la última versión de los controladores paravirtualizados para una máquina virtual basada en esta plantilla. Aparece como `not in database` para una plantilla
- `memory` (parámetro de mapa de solo lectura) métricas de memoria notificadas por el agente en una máquina virtual basada en esta plantilla. Aparece como `not in database` para una plantilla
- `disks` (parámetro de mapa de solo lectura) métricas de disco informadas por el agente en una máquina virtual basada en esta plantilla. Aparece como `not in database` para una plantilla
- `networks` (parámetro de mapa de solo lectura) métricas de red informadas por el agente en una máquina virtual basada en esta plantilla. Aparece como `not in database` para una plantilla
- `other` (parámetro de mapa de solo lectura) otras métricas notificadas por el agente en una máquina virtual basada en esta plantilla. Aparece como `not in database` para una plantilla
- `guest-metrics-last-updated` (solo lectura) marca de tiempo cuando el agente invitado realizó la última escritura en estos campos. En el formulario `yyyymmddThh:mm:ss z`, donde z es el indicador de zona horaria militar de una sola letra, por ejemplo, Z para UTC (GMT)
- `actions-after-shutdown` (lectura/escritura) que se debe realizar después de que la máquina virtual se haya apagado
- `actions-after-reboot` (lectura/escritura) que se debe realizar después de que la VM se haya reiniciado
- `possible-hosts` (solo lectura) lista de hosts que potencialmente pueden alojar la VM
- `HVM-shadow-multiplier` (lectura/escritura) se aplica a la cantidad de sombra que se pone a disposición del huésped
- `dom-id` (solo lectura) ID de dominio (si está disponible, -1 en caso contrario)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- `recommendations` (solo lectura) Especificación XML de valores y rangos recomendados para las propiedades de esta máquina virtual
- `xenstore-data` (parámetro de asignación de lectura/escritura) Datos que se insertarán en el árbol `xenstore` (/`local`/`domain`/`*domid*`/`vmdata`) después de crear la máquina virtual.
- `is-a-snapshot` (solo lectura) True si esta plantilla es una instantánea de VM
- `snapshot_of` (solo lectura) el UUID de la máquina virtual de la que esta plantilla es una instantánea
- `snapshots` (solo lectura) los UUID de cualquier instantánea que se haya tomado de esta plantilla
- `snapshot_time` (solo lectura) la marca de tiempo de la instantánea de VM más reciente tomada
- `memory-target` (solo lectura) la cantidad objetivo de memoria establecida para esta plantilla
- `blocked-operations` (parámetro de mapa de lectura/escritura) muestra las operaciones que no se pueden realizar en esta plantilla
- `last-boot-record` (solo lectura) de los últimos parámetros de arranque para esta plantilla, en formato XML
- `ha-always-run` (lectura/escritura) True si una instancia de esta plantilla siempre se reinicia en otro host si se produce un error en el host en el que reside. Este parámetro ahora está en desuso. Utilice el parámetro `ha-restartpriority` en su lugar.
- `ha-restart-priority` (solo lectura) reinicio o lo mejor que se pueda hacer con almacenes de datos binarios de blobs de lectura/escritura
- `live` (solo lectura) relevante solo para una VM en ejecución.

template-export

```
1 xe template-export template-uuid=uuid_of_existing_template filename=
     filename_for_new_template
2 <!--NeedCopy-->
```

Exporta una copia de una plantilla especificada a un archivo con el nombre de archivo nuevo especificado.

template-uninstall

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe template-uninstall template-uuid=template_uuid [--force]
<!--NeedCopy-->
```

Desinstale una plantilla personalizada. Esta operación destruirá los VDI que estén marcados como "propiedad"de esta plantilla.

Comandos de actualización

La siguiente sección contiene los comandos de actualización del host de XenServer.

Los objetos de actualización se pueden enumerar con el comando estándar de listado de objetos (`xe update-list`) y los parámetros manipulados con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

Parámetros de actualización

Las actualizaciones del host de XenServer tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
`uuid`	La referencia única de identificador/objeto para la actualización	Solo lectura
`host`	La lista de hosts a los que se aplica esta actualización	Solo lectura
`host-uuid`	El identificador único del host de XenServer que se va a consultar	Solo lectura
`name-label`	El nombre de la actualización	Solo lectura
`name-description`	La cadena de descripción de la actualización	Solo lectura
`applied`	Si la actualización se ha aplicado o no; verdadero o falso	Solo lectura
`installation-size`	El tamaño de la actualización en bytes	Solo lectura
`after-apply-guidance`	Si la pila de herramientas XAPI o el host requieren un reinicio	Solo lectura
`version`	La versión de la actualización	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

update-upload

```
xe update-upload file-name=update_filename
<!--NeedCopy-->
```

Cargue un archivo de actualización especificado en el host de XenServer. Este comando prepara una actualización para aplicarla. Si tiene éxito, se imprime el UUID de la actualización cargada. Si la actualización se cargó anteriormente, se devuelve un error `UPDATE_ALREADY_EXISTS` y el parche no se vuelve a cargar.

update-precheck

```
xe update-precheck uuid=update_uuid host-uuid=host_uuid
<!--NeedCopy-->
```

Ejecute las comprobaciones previas incluidas en la actualización especificada en el host de XenServer especificado.

update-destroy

```
xe update-destroy uuid=update_file_uuid
<!--NeedCopy-->
```

Elimina un archivo de actualización que no se ha aplicado del grupo. Se puede usar para eliminar un archivo de actualización que no se puede aplicar a los hosts.

update-apply

```
xe update-apply host-uuid=host_uuid uuid=update_file_uuid
<!--NeedCopy-->
```

Aplica el archivo de actualización especificado.

update-pool-apply

```
xe update-pool-apply uuid=update_uuid
<!--NeedCopy-->
```

Aplique la actualización especificada a todos los hosts de XenServer del grupo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

update-introduce

```
xe update-introduce vdi-uuid=vdi_uuid
<!--NeedCopy-->
```

Introduce la actualización de VDI.

update-pool-clean

```
xe update-pool-clean uuid=uuid
<!--NeedCopy-->
```

Elimina los archivos de la actualización de todos los hosts del grupo.

Comandos del usuario

user-password-change

```
xe user-password-change old=old_password new=new_password
<!--NeedCopy-->
```

Cambia la contraseña del usuario que ha iniciado sesión. El campo de contraseña anterior no está marcado porque necesita privilegios de supervisor para usar este comando.

Comandos de VBD

Comandos para trabajar con VBD (dispositivos de bloques virtuales).

Un VBD es un objeto de software que conecta una máquina virtual a la VDI, que representa el contenido del disco virtual. El VBD tiene los atributos que vinculan el VDI a la VM (si es de arranque, sus métricas de lectura/escritura, etc.). El VDI tiene la información sobre los atributos físicos del disco vDisk (qué tipo de SR, si el disco es compartible, si el medio es de lectura/escritura o de solo lectura, etc.).

Los objetos de VBD se pueden enumerar con el comando estándar de lista de objetos (`xe vbd-list`) y los parámetros manipulados con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

Parámetros VBD

Los VBD tienen los siguientes parámetros:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
uuid	La referencia única de identificador/objeto para el VBD	Solo lectura
vm-uuid	La referencia de identificador/objeto única para la máquina virtual a la que está conectado este VBD	Solo lectura
vm-name-**label**	El nombre de la máquina virtual a la que está conectado este VBD	Solo lectura
vdi-uuid	La referencia de identificador/objeto única para la VDI a la que se asigna este VBD	Solo lectura
vdi-name-**label**	El nombre de la VDI a la que se asigna este VBD	Solo lectura
empty	Si **true**, este VBD representa una unidad vacía	Solo lectura
device	El dispositivo que ve el invitado, por ejemplo hda	Solo lectura
userdevice	Número de dispositivo especificado por el parámetro de dispositivo durante vbd-create, por ejemplo hda, 0 para hdb, 1 para, etc.	Lectura/Escritura
bootable	True si este VBD es de arranque	Lectura/Escritura
mode	El modo con el que se monta el VBD	Lectura/Escritura
type	Cómo se ve el VBD en la VM, por ejemplo, disco o CD	Lectura/Escritura
currently-attached	True si el VBD está conectado a este host, falso en caso contrario	Solo lectura
storage-lock	True si se adquirió un bloqueo a nivel de almacenamiento	Solo lectura
status-code	Código de error/éxito asociado a la última operación de conexión	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
status-detail	Información de error/éxito asociada con el estado de la última operación de conexión	Solo lectura
qos_algorithm_type	El algoritmo de priorización a utilizar	Lectura/Escritura
qos_algorithm_params	Parámetros del algoritmo de priorización elegido	Parámetro de mapa de lectura y escritura
qos_supported_algorithms	Algoritmos de priorización compatibles para este VBD	Parámetro de conjunto de solo lectura
io_read_kbs	Velocidad media de lectura en kb por segundo para este VBD	Solo lectura
io_write_kbs	Velocidad media de escritura en kb por segundo para este VBD	Solo lectura
allowed-operations	Lista de las operaciones permitidas en este estado. Esta lista es solo consultiva y es posible que el estado del servidor haya cambiado para cuando un cliente lea este campo.	Parámetro de conjunto de solo lectura
current-operations	Vincula cada una de las tareas en ejecución que utilizan este objeto (por referencia) a una enumeración current_operation que describe la naturaleza de la tarea.	Parámetro de conjunto de solo lectura
unpluggable	True si este VBD admite la desconexión en caliente	Lectura/Escritura
attachable	True si el dispositivo se puede conectar	Solo lectura
other-config	Configuración extra	Parámetro de mapa de lectura y escritura

vbd-create

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe vbd-create vm-uuid=uuid_of_the_vm device=device_value vdi-uuid=
    uuid_of_vdi_to_connect_to [bootable=true] [type=Disk|CD] [mode=RW|RO
    ]
<!--NeedCopy-->
```

Crea un VBD en una VM.

Los valores permitidos para el campo `device` son enteros 0—15, y el número debe ser único para cada máquina virtual. Los valores permitidos actuales se pueden ver en el parámetro `allowed-VBD-devices` de la VM especificada. Esto se ve como `userdevice` en los parámetros `vbd`.

Si el `type` es `Disk`, `vdi-uuid` es necesario. El modo puede ser `RO` o `RW` para un disco.

Si el `type` es `CD`, `vdi-uuid` es opcional. Si no se especifica VDI, se crea un VBD vacío para el CD. El modo debe ser `RO` para un CD.

vbd-destroy

```
xe vbd-destroy uuid=uuid_of_vbd
<!--NeedCopy-->
```

Destruye el VBD especificado.

Si el VBD tiene su parámetro `other-config:owner` establecido en **`true`**, el VDI asociado también se destruye.

vbd-eject

```
xe vbd-eject uuid=uuid_of_vbd
<!--NeedCopy-->
```

Retire los medios de la unidad representada por un VBD. Este comando solo funciona si el medio es de un tipo extraíble (un CD físico o una ISO). De lo contrario, se devuelve un mensaje de error `VBD_NOT_REMOVABLE_MEDIA`.

vbd-insert

```
xe vbd-insert uuid=uuid_of_vbd vdi-uuid=uuid_of_vdi_containing_media
<!--NeedCopy-->
```

Inserte nuevos medios en la unidad representada por un VBD. Este comando solo funciona si el medio es de un tipo extraíble (un CD físico o una ISO). De lo contrario, se devuelve un mensaje de error `VBD_NOT_REMOVABLE_MEDIA`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

vbd-plug

```
xe vbd-plug uuid=uuid_of_vbd
<!--NeedCopy-->
```

Intente conectar el VBD mientras la máquina virtual se encuentra en estado de ejecución.

vbd-unplug

```
xe vbd-unplug uuid=uuid_of_vbd
<!--NeedCopy-->
```

Intenta desconectar el VBD de la VM mientras está en ejecución.

Comandos de VDI

Comandos para trabajar con VDI (imágenes de disco virtual).

Una VDI es un objeto de software que representa el contenido del disco virtual que ve una VM. Esto es diferente al VBD, que es un objeto que vincula una VM a la VDI. El VDI tiene la información sobre los atributos físicos del disco vDisk (qué tipo de SR, si el disco es compartible, si el medio es de lectura/escritura o de solo lectura, etc.). El VBD tiene los atributos que vinculan el VDI a la VM (si es de arranque, sus métricas de lectura/escritura, etc.).

Los objetos de VDI se pueden enumerar con el comando estándar de lista de objetos (`xe vdi-list`) y los parámetros manipulados con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

Parámetros VDI

Los VDI tienen los siguientes parámetros:

Nombre del parámetro	Descripción	Tipo
`uuid`	La referencia única de identificador/objeto para la VDI	Solo lectura
`name-label`	El nombre de la VDI	Lectura/Escritura
`name-description`	La cadena de descripción de la VDI	Lectura/Escritura
`allowed-operations`	Una lista de las operaciones permitidas en este estado	Parámetro de conjunto de solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
current-operations	Una lista de las operaciones que están actualmente en curso en esta VDI	Parámetro de conjunto de solo lectura
sr-uuid	SR en la que reside la VDI	Solo lectura
vbd-uuids	Una lista de VBD que hacen referencia a este VDI	Parámetro de conjunto de solo lectura
crashdump-uuids	Lista de volcados de memoria que hacen referencia a este VDI	Parámetro de conjunto de solo lectura
virtual-size	Tamaño del disco tal como se presenta a la máquina virtual, en bytes. Según el tipo de back-end de almacenamiento, es posible que el tamaño no se respete exactamente	Solo lectura
physical-utilisation	Cantidad de espacio físico que la VDI ocupa en el SR, en bytes	Solo lectura
type	Tipo de VDI, por ejemplo, sistema o usuario	Solo lectura
sharable	True si este VDI se puede compartir	Solo lectura
read-only	True si este VDI solo se puede montar en modo de solo lectura	Solo lectura
storage-lock	True si este VDI está bloqueado en el nivel de almacenamiento	Solo lectura
parent	Hace referencia a la VDI principal cuando esta VDI forma parte de una cadena	Solo lectura
missing	True si la operación de exploración SR informó que este VDI no estaba presente	Solo lectura
other-config	Información de configuración adicional para este VDI	Parámetro de mapa de lectura y escritura
sr-name-**label**	Nombre del repositorio de almacenamiento que lo contiene	Solo lectura
location	Información de ubicación	Solo lectura

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
managed	True si se administra la VDI	Solo lectura
xenstore-data	Datos que se insertarán en el árbol xenstore (/local/domain/0/backend/vbd/*domid*/*device-id*/smdata) después de conectar la VDI. Los back-ends SM generalmente establecen este campo en vdi_attach.	Parámetro de mapa de solo lectura
sm-config	Datos dependientes de SM	Parámetro de mapa de solo lectura
is-a-snapshot	True si este VDI es una instantánea de almacenamiento de VM	Solo lectura
snapshot_of	El UUID del almacenamiento del que este VDI es una instantánea	Solo lectura
snapshots	Los UUID de todas las instantáneas de este VDI	Solo lectura
snapshot_time	La marca de tiempo de la operación de instantánea que creó esta VDI	Solo lectura
metadata-of-pool	El uuid del grupo que creó este VDI de metadatos	Solo lectura
metadata-latest	Marca que indica si la VDI contiene los últimos metadatos conocidos para este grupo	Solo lectura
cbt-enabled	Bandera que indica si el seguimiento de bloques modificados está habilitado para la VDI	Lectura/Escritura

vdi-clone

```
xe vdi-clone uuid=uuid_of_the_vdi [driver-params:key=value]
<!--NeedCopy-->
```

Cree una nueva copia en la que se pueda escribir de la VDI especificada que se pueda usar directa-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

mente. Es una variante de `vdi-copy` que puede exponer instalaciones de clonación de imágenes de alta velocidad donde existan.

Utilice el parámetro de asignación `driver-params` opcional para pasar información de configuración adicional específica del proveedor al controlador de almacenamiento back-end en el que se basa el VDI. Para obtener más información, consulte la documentación del controlador del proveedor de almacenamiento.

vdi-copy

```
xe vdi-copy uuid=uuid_of_the_vdi sr-uuid=uuid_of_the_destination_sr
<!--NeedCopy-->
```

Copie un VDI en un SR especificado.

vdi-create

```
xe vdi-create sr-uuid=uuid_of_sr_to_create_vdi_on name-label=
    name_for_the_vdi type=system|user|suspend|crashdump virtual-size=
    size_of_virtual_disk sm-config-*=storage_specific_configuration_data
<!--NeedCopy-->
```

Crea una VDI.

El parámetro `virtual-size` se puede especificar en bytes o mediante los sufijos estándar IEC KiB, MiB, GiB y TiB.

> **Nota:**
>
> Los tipos de SR que admiten el aprovisionamiento controlado de discos (como VHD local y NFS) no imponen la asignación virtual de discos. Tenga mucho cuidado al sobreasignar espacio de disco virtual en un SR. Si un SR sobreasignado se llena, el espacio en disco debe estar disponible en el sustrato de destino de SR o eliminando los VDI no utilizados en el SR.
>
> Algunos tipos SR pueden redondear el valor `virtual-size` para que sea divisible por un tamaño de bloque configurado.

vdi-data-destroy

```
xe vdi-data-destroy uuid=uuid_of_vdi
<!--NeedCopy-->
```

Destruya los datos asociados a la VDI especificada, pero conserve los metadatos de seguimiento de bloques modificados.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Si utiliza el seguimiento de bloques modificados para realizar copias de seguridad incrementales de la VDI, asegúrese de utilizar el comando `vdi-data-destroy` para eliminar las instantáneas pero conservar los metadatos. No utilice `vdi-destroy` en instantáneas de VDI que hayan cambiado el seguimiento de bloques habilitado.

vdi-destroy

```
xe vdi-destroy uuid=uuid_of_vdi
<!--NeedCopy-->
```

Destruya el VDI especificado.

> **Nota:**
>
> Si utiliza el seguimiento de bloques modificados para realizar copias de seguridad incrementales de la VDI, asegúrese de utilizar el comando `vdi-data-destroy` para eliminar las instantáneas pero conservar los metadatos. No utilice `vdi-destroy` en instantáneas de VDI que hayan cambiado el seguimiento de bloques habilitado.
>
> Para los tipos de SR de VHD local y NFS, el espacio en disco no se libera inmediatamente `vdi-destroy`, sino periódicamente durante una operación de exploración del repositorio de almacenamiento. Si debe forzar la disponibilidad del espacio en disco eliminado, llame `sr-scan` manualmente.

vdi-disable-cbt

```
xe vdi-disable-cbt uuid=uuid_of_vdi
<!--NeedCopy-->
```

Inhabilite el seguimiento de bloques cambiados para la VDI.

vdi-enable-cbt

```
xe vdi-enable-cbt uuid=uuid_of_vdi
<!--NeedCopy-->
```

Habilite el seguimiento de bloques modificados para la VDI.

> **Nota:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Puede habilitar el seguimiento de los bloques modificados solo en las instancias con licencia de XenServer Premium Edition.

vdi-export

```
xe vdi-export uuid=uuid_of_vdi filename=filename_to_export_to [format=
    format] [base=uuid_of_base_vdi] [--progress]
<!--NeedCopy-->
```

Exporte una VDI al nombre de archivo especificado. Puede exportar un VDI en uno de los siguientes formatos:

- `raw`
- `vhd`

El formato VHD puede ser *escaso*. Si hay bloques sin asignar en la VDI, es posible que estos bloques se omita en el archivo VHD, lo que reduce el tamaño del archivo VHD. Puede exportar a formato VHD desde todos los tipos de almacenamiento compatibles basados en VHD (EXT3/EXT4, NFS).

Si especifica el comando `base` exporta solo los bloques que han cambiado entre el VDI exportado y el VDI base.

vdi-forget

```
xe vdi-forget uuid=uuid_of_vdi
<!--NeedCopy-->
```

Elimina incondicionalmente un registro VDI de la base de datos sin tocar el back-end de almacenamiento. En funcionamiento normal, use `vdi-destroy` en su lugar.

vdi-import

```
xe vdi-import uuid=uuid_of_vdi filename=filename_to_import_from [format
    =format] [--progress]
<!--NeedCopy-->
```

Importe un VDI. Puede importar un VDI desde uno de los siguientes formatos:

- `raw`
- `vhd`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

vdi-introduce

```
xe vdi-introduce uuid=uuid_of_vdi sr-uuid=uuid_of_sr name-label=
    name_of_new_vdi type=system|user|suspend|crashdump location=
    device_location_(varies_by_storage_type) [name-description=
    description_of_vdi] [sharable=yes|no] [read-only=yes|no] [other-
    config=map_to_store_misc_user_specific_data] [xenstore-data=
    map_to_of_additional_xenstore_keys] [sm-config=
    storage_specific_configuration_data]
<!--NeedCopy-->
```

Cree un objeto VDI que represente un dispositivo de almacenamiento existente, sin modificar ni crear ningún almacenamiento. Este comando se usa principalmente de forma interna para introducir automáticamente dispositivos de almacenamiento conectables en caliente.

vdi-list-changed-blocks

```
xe vdi-list-changed-blocks vdi-from-uuid=first-vdi-uuid vdi-to-uuid=
    second-vdi-uuid
<!--NeedCopy-->
```

Compare dos VDI y devuelva la lista de bloques que han cambiado entre los dos como una cadena codificada en base64. Este comando solo funciona para los VDI que han cambiado el seguimiento de bloques habilitado.

Para obtener más información, consulte Seguimiento de bloques modificados.

vdi-pool-migrate

```
xe vdi-pool-migrate uuid=VDI_uuid sr-uuid=destination-sr-uuid
<!--NeedCopy-->
```

Migre un VDI a un SR especificado, mientras el VDI está conectado a un invitado en ejecución. (Migración de almacenamiento en vivo)

Para obtener más información, consulte Migrar máquinas virtuales.

vdi-resize

```
xe vdi-resize uuid=vdi_uuid disk-size=new_size_for_disk
<!--NeedCopy-->
```

Cambia el tamaño del VDI especificado por el UUID.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

vdi-snapshot

```
xe vdi-snapshot uuid=uuid_of_the_vdi [driver-params=params]
<!--NeedCopy-->
```

Produce una versión de lectura y escritura de una VDI que se puede utilizar como referencia para crear copias de seguridad o plantillas, o ambas cosas. Use la instantánea para realizar una copia de seguridad en lugar de instalar y ejecutar el software de copia de seguridad dentro de la VM. La VM sigue ejecutándose mientras el software de reserva externo transmite el contenido de la instantánea a los medios de reserva. Del mismo modo, una instantánea se puede usar como una "imagen dorada"en la que basar una plantilla. Se puede crear una plantilla con cualquier VDI.

Utilice el parámetro de asignación `driver-params` opcional para pasar información de configuración adicional específica del proveedor al controlador de almacenamiento back-end en el que se basa el VDI. Para obtener más información, consulte la documentación del controlador del proveedor de almacenamiento.

Un clon de una instantánea siempre produce una VDI grabable.

vdi-unlock

```
xe vdi-unlock uuid=uuid_of_vdi_to_unlock [force=true]
<!--NeedCopy-->
```

Intenta desbloquear los VDI especificados. Si `force=true` se pasa al comando, fuerza la operación de desbloqueo.

vdi-update

```
xe vdi-update uuid=uuid
<!--NeedCopy-->
```

Actualice los campos del objeto VDI en la base de datos.

Comandos VIF

Comandos para trabajar con VIF (interfaces de red virtuales).

Los objetos de VIF se pueden enumerar con el comando estándar de lista de objetos (`xe vif-list`) y los parámetros manipulados con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Parámetros VIF

Los VIF tienen los siguientes parámetros:

- `uuid` (solo lectura) la referencia única de identificador/objeto para el VIF
- `vm-uuid` (solo lectura) la referencia única de identificador/objeto para la VM en la que reside este VIF
- `vm-name-label` (solo lectura) el nombre de la VM en la que reside este VIF
- `allowed-operations` (parámetro set de solo lectura) una lista de las operaciones permitidas en este estado
- `current-operations` (parámetro establecido de solo lectura) una lista de las operaciones que están actualmente en curso en este VIF
- `device` (solo lectura) etiqueta de entero de este VIF, que indica el orden en que se crearon los back-ends de VIF
- `MAC` (solo lectura) Dirección MAC de VIF, tal como se expone a la VM
- `MTU` (solo lectura) Unidad de transmisión máxima del VIF en bytes.

  Este parámetro es de solo lectura, pero puede anular la configuración de MTU con la clave `mtu` mediante el parámetro de asignación `other-config`. Por ejemplo, para restablecer la MTU en una NIC virtual para que use tramas gigantes:

  ```
  xe vif-param-set \
      uuid=<vif_uuid> \
      other-config:mtu=9000
  <!--NeedCopy-->
  ```

- `currently-attached` (solo lectura) true si el dispositivo está conectado
- `qos_algorithm_type` (lectura/escritura) Algoritmo de QoS a usar
- `qos_algorithm_params` (parámetro de mapa de lectura/escritura) parámetros para el algoritmo QoS elegido
- `qos_supported_algorithms` (parámetro establecido de solo lectura) algoritmos de QoS compatibles para este VIF
- `MAC-autogenerated` (solo lectura) True si la dirección MAC del VIF se generó automáticamente
- `other-config` (parámetro de mapa de lectura/escritura) pares `key:value` de configuración adicionales
- `other-config:ethtoolrx` (lectura/escritura) establecido en activado para activar la suma de comprobación de recepción, desactivado para inhabilitar

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- other-config:ethtooltx (lectura/escritura) establecido en activado para habilitar la suma de comprobación de transmisión, desactivado para inhabilitar
- other-config:ethtoolsg (lectura/escritura) se activa para habilitar la recopilación de dispersión, desactiva para inhabilitar
- other-config:ethtooltso (lectura/escritura) establecido en activado para habilitar la descarga de segmentación de TCP, desactivado para inhabilitar
- other-config:ethtoolufo (lectura/escritura) establecido en activado para habilitar la descarga de fragmentos UDP, desactivado para inhabilitar
- other-config:ethtoolgso (lectura/escritura) establecido en activado para habilitar la descarga de segmentación genérica, desactivado para inhabilitar
- other-config:promiscuous (lectura/escritura) true para que un VIF sea promiscuo en el puente, de modo que vea todo el tráfico a través del puente. Es útil para ejecutar un sistema de detección de intrusiones (IDS) o similar en una máquina virtual.
- network-uuid (solo lectura) la referencia única de identificador/objeto de la red virtual a la que está conectado este VIF
- network-name-**label** (solo lectura) el nombre descriptivo de la red virtual a la que está conectado este VIF
- io_read_kbs (solo lectura) velocidad de lectura promedio en kb/s para este VIF
- io_write_kbs (solo lectura) velocidad de escritura promedio en kb/s para este VIF
- locking_mode (lectura/escritura) Afecta a la capacidad de las VIF para filtrar el tráfico hacia/desde una lista de direcciones MAC e IP. Requiere parámetros adicionales.
- locking_mode:**default** (lectura/escritura) Varía según el modo de bloqueo predeterminado de la red VIF.

  Si el modo de bloqueo predeterminado está establecido en, disabledXenServer aplica una regla de filtrado para que el VIF no pueda enviar ni recibir tráfico. Si el modo de bloqueo predeterminado está establecido en, unlockedXenServer elimina todas las reglas de filtrado asociadas al VIF. Para obtener más información, consulte Comandos de red.
- locking_mode:locked (lectura/escritura) Solo se permite el tráfico enviado a o enviado desde las direcciones MAC e IP especificadas en el VIF. Si no se especifican direcciones IP, no se permite el tráfico.
- locking_mode:unlocked (lectura/escritura) No se aplican filtros a ningún tráfico que vaya hacia o desde el VIF.
- locking_mode:disabled (lectura/escritura) XenServer aplica una regla de filtrado para que el VIF elimine todo el tráfico.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

vif-create

```
xe vif-create vm-uuid=uuid_of_the_vm device=see below network-uuid=
    uuid_of_network_to_connect_to [mac=mac_address]
<!--NeedCopy-->
```

Cree una VIF en una VM.

Los valores apropiados para el campo `device` se enumeran en el parámetro `allowed-VIF-devices` de la máquina virtual especificada. Antes de que existan VIF, los valores permitidos son enteros de 0 a 15.

El parámetro `mac` es la dirección MAC estándar en forma `aa:bb:cc:dd:ee:ff`. Si lo deja sin especificar, se crea una dirección MAC aleatoria apropiada. También puede establecer explícitamente una dirección MAC aleatoria especificando `mac=random`.

vif-destroy

```
xe vif-destroy uuid=uuid_of_vif
<!--NeedCopy-->
```

Destruya una VIF.

vif-move

```
xe vif-move uuid=uuid network-uuid=network_uuid
<!--NeedCopy-->
```

Mueva la VIF a otra red.

vif-plug

```
xe vif-plug uuid=uuid_of_vif
<!--NeedCopy-->
```

Intente conectar el VIF mientras la máquina virtual se encuentra en estado de ejecución.

vif-unplug

```
xe vif-unplug uuid=uuid_of_vif
<!--NeedCopy-->
```

Intenta desconectar la VIF de la VM mientras se está ejecutando.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

vif-configure-ipv4

Configure los ajustes de IPv4 para esta interfaz virtual. Configure la configuración de IPv4 de la siguiente manera:

```
xe vif-configure-ipv4 uuid=uuid_of_vif mode=static address=CIDR_address
    gateway=gateway_address
<!--NeedCopy-->
```

Por ejemplo:

```
VIF.configure_ipv4(vifObject,"static", " 192.168.1.10/24", "
   192.168.1.1")
<!--NeedCopy-->
```

Limpie la configuración IPv4 de la siguiente manera:

```
xe vif-configure-ipv4 uuid=uuid_of_vif mode=none
<!--NeedCopy-->
```

vif-configure-ipv6

Configure los ajustes de IPv6 para esta interfaz virtual. Configure la configuración de IPv6 de la siguiente manera:

```
xe vif-configure-ipv6 uuid=uuid_of_vif mode=static address=IP_address
   gateway=gateway_address
<!--NeedCopy-->
```

Por ejemplo:

```
VIF.configure_ipv6(vifObject,"static", "fd06:7768:b9e5:8b00::5001/64",
   "fd06:7768:b9e5:8b00::1")
<!--NeedCopy-->
```

Limpie la configuración IPv6 de la siguiente manera:

```
xe vif-configure-ipv6 uuid=uuid_of_vif mode=none
<!--NeedCopy-->
```

Comandos de VLAN

Comandos para trabajar con VLAN (redes virtuales). Para enumerar y modificar interfaces virtuales, consulte los comandos PIF, que tienen un parámetro VLAN para indicar que tienen una red virtual asociada. Para obtener más información, consulte Comandos PIF. Por ejemplo, para enumerar las VLAN, utilice `xe pif-list`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

vlan-create

```
xe vlan-create pif-uuid=uuid_of_pif vlan=vlan_number network-uuid=
   uuid_of_network
<!--NeedCopy-->
```

Cree una VLAN en el host de XenServer.

pool-vlan-create

```
xe pool-vlan-create pif-uuid=uuid_of_pif vlan=vlan_number network-uuid=
   uuid_of_network
<!--NeedCopy-->
```

Cree una VLAN en todos los hosts de un grupo, determinando en qué interfaz (por ejemplo, `eth0`) se encuentra la red especificada (en cada host) y creando y conectando un nuevo objeto PIF en cada host en consecuencia.

vlan-destroy

```
xe vlan-destroy uuid=uuid_of_pif_mapped_to_vlan
<!--NeedCopy-->
```

Destruye una VLAN. Requiere el UUID del PIF que representa la VLAN.

Comandos de VM

Comandos para controlar las máquinas virtuales y sus atributos.

Selectores de VM

Varios de los comandos enumerados aquí tienen un mecanismo común para seleccionar una o más máquinas virtuales en las que realizar la operación. La forma más sencilla es proporcionar el argumento `vm=name_or_uuid`. Una forma sencilla de obtener el uuid de una máquina virtual real es, por ejemplo, ejecutarla `xe vm-list power-state=running`. (Obtenga la lista completa de campos que pueden coincidir mediante el comando `xe vm-list params=all`) Por ejemplo, al especificar `power-state=halted` se seleccionan las máquinas virtuales cuyo parámetro `power-state` es igual a `halted`. Si hay varias máquinas virtuales que coincidan, especifique la opción `--multiple` para realizar la operación. La lista completa de parámetros que se pueden hacer coincidir se describe al principio de esta sección.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Los objetos de VM se pueden enumerar con el comando de listado de objetos estándar (`xe vm-list`) y los parámetros manipulados con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

Parámetros VM

Las VM tienen los siguientes parámetros:

> **Nota:**
>
> Todos los valores de parámetros de VM grabables se pueden cambiar mientras la VM se está ejecutando, pero los nuevos parámetros *no* se aplican dinámicamente y no se pueden aplicar hasta que se reinicie la VM.

- `appliance` (lectura/escritura) el dispositivo/vApp a la que pertenece la VM
- `uuid` (solo lectura) la referencia única de identificador/objeto para la VM
- `name-label` (lectura/escritura) el nombre de la VM
- `name-description` (lectura/escritura) la cadena de descripción de la VM
- `order` (lectura/escritura) para el inicio o cierre de la vApp y para el inicio después de una conmutación por error de alta disponibilidad. Las máquinas virtuales con un valor de pedido de 0 (cero) se inician primero, luego las máquinas virtuales con un valor de pedido de 1, y así sucesivamente.
- `version` (solo lectura) el número de veces que se ha recuperado esta máquina virtual. Si quiere sobrescribir una máquina virtual nueva con una versión anterior, llame a `vm-recover`
- `user-version` (lectura/escritura) para creadores de máquinas virtuales y plantillas para poner información de versión
- `is-a-template` (lectura/escritura) False a menos que esta máquina virtual sea una plantilla. Las VM de plantilla nunca se pueden iniciar, solo se usan para clonar otras VM. Una vez que este valor se ha establecido en true, no se puede restablecer a false. Las máquinas virtuales de plantilla no se pueden convertir en máquinas virtuales con este parámetro.

  Puede convertir una máquina virtual en una plantilla con:

  ```
  xe vm-param-set uuid=<vm uuid> is-a-template=true
  <!--NeedCopy-->
  ```

- `is-control-domain` (solo lectura) True si se trata de un dominio de control (dominio 0 o un dominio de controlador)
- `power-state` (solo lectura) estado de alimentación actual

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- start-delay (lectura/escritura) el retraso de espera antes de que se produzca una llamada para iniciar la máquina virtual en segundos
- shutdown-delay (lectura/escritura) el retraso de espera antes de que una llamada para apagar la máquina virtual regrese en segundos
- memory-dynamic-max (lectura/escritura) máximo dinámico en bytes
- memory-dynamic-min (lectura/escritura) mínimo dinámico en bytes
- memory-**static**-max (lectura/escritura) establecido estáticamente como máximo (absoluto) en bytes. Si quiere cambiar este valor, la máquina virtual debe cerrarse.
- memory-**static**-min (lectura/escritura) establecido estáticamente como mínimo (absoluto) en bytes. Si quiere cambiar este valor, la máquina virtual debe cerrarse.
- suspend-VDI-uuid (solo lectura) la VDI en la que se almacena una imagen suspendida
- VCPUs-params (parámetro de mapa de lectura/escritura) para la directiva de vCPU seleccionada.

  Puede ajustar la fijación de una vCPU con

  ```
  1  xe vm-param-set uuid=<vm_uuid> VCPUs-params:mask=1,2,3
  2  <!--NeedCopy-->
  ```

  La VM seleccionada se ejecuta solo en las CPU físicas 1, 2 y 3.
  También puede ajustar la prioridad de la vCPU (programación xen) con los parámetros de límite y peso. Por ejemplo:

  ```
  1  xe vm-param-set uuid=<vm_uuid> VCPUs-params:weight=512 xe vm-
       param-set uuid=<vm_uuid> VCPUs-params:cap=100
  2  <!--NeedCopy-->
  ```

  Una máquina virtual con un peso de 512 obtiene el doble de CPU que un dominio con un peso de 256 en un host de XenServer en disputa. Los pesos legales varían de 1 a 65535 y el valor predeterminado es 256. El límite fija, de forma opcional, la cantidad máxima de CPU que una máquina virtual podrá consumir, incluso si el host XenServer tiene ciclos de CPU inactivos. El límite se expresa en porcentaje de una CPU física: 100 es 1 CPU física, 50 es media CPU, 400 son 4 CPU, etc. El valor predeterminado, 0, significa que no hay límite superior.
- VCPUs-max (lectura/escritura) número máximo de CPU virtuales.
- VCPUs-at-startup (lectura/escritura) número de arranque de CPU virtuales
- actions-after-crash (lectura/escritura) que se debe realizar si la máquina virtual se bloquea. Para los huéspedes de PV, los parámetros válidos son:
  - preserve (solo para análisis)
  - coredump_and_restart (grabar un volcado de núcleo y reiniciar la VM)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - `coredump_and_destroy` (grabar un volcado de núcleo y dejar la VM detenida)
  - `restart` (sin volcado de núcleo y reinicio de VM)
  - `destroy` (sin volcado de núcleo y dejar la VM detenida)

- `console-uuids` (parámetro establecido de solo lectura) dispositivos de consola virtual
- `platform` (parámetro de mapa de lectura/escritura) configuración específica de la plataforma

  Para inhabilitar el VDA para cambiar Windows 10 al modo Tableta:

```
xe vm-param-set uuid=<vm_uuid> platform:acpi_laptop_slate=0
<!--NeedCopy-->
```

  Para permitir que el VDA cambie Windows 10 al modo Tableta:

```
xe vm-param-set uuid=<vm_uuid> platform:acpi_laptop_slate=1
<!--NeedCopy-->
```

  Para comprobar el estado actual:

```
xe vm-param-get uuid=<vm_uuid> param-name=platform param-key=
   acpi_laptop_slate
<!--NeedCopy-->
```

- `allowed-operations` (parámetro de conjunto de solo lectura) lista de las operaciones permitidas en este estado
- `current-operations` (parámetro establecido de solo lectura) una lista de las operaciones que están actualmente en curso en la VM
- `allowed-VBD-devices` (parámetro conjunto de solo lectura) de identificadores VBD disponibles para su uso, representados por enteros del rango 0—15. Esta lista es solo informativa y se pueden usar otros dispositivos (pero es posible que no funcionen).
- `allowed-VIF-devices` (parámetro conjunto de solo lectura) de identificadores VIF disponibles para su uso, representados por enteros del rango 0—15. Esta lista es solo informativa y se pueden usar otros dispositivos (pero es posible que no funcionen).
- `HVM-boot-policy` (leer/escribir) la directiva de arranque para los huéspedes. Orden de BIOS o una cadena vacía.
- `HVM-boot-params` (parámetro del mapa de lectura/escritura) la tecla de orden controla el orden de arranque del invitado, representado como una cadena en la que cada carácter es un método de arranque: d para el CD/DVD, c para el disco raíz y n para el arranque PXE de red. El valor por defecto es dc.
- `HVM-shadow-multiplier` (lectura/escritura) Valor de punto flotante que controla la cantidad de sobrecarga de memoria instantánea que se debe conceder a la VM. El valor predeterminado es 1.0 (el valor mínimo) y solo cambia este valor si es un usuario avanzado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- PV-kernel (lectura/escritura) al núcleo
- PV-ramdisk (lectura/escritura) a la initrd
- PV-args (lectura/escritura) de argumentos de línea de comandos del núcleo
- PV-legacy-args (lectura/escritura) de argumentos para hacer que las máquinas virtuales heredadas arranquen
- PV-bootloader (lectura/escritura) nombre o ruta al gestor de arranque
- PV-bootloader-args (lectura/escritura) de argumentos varios para el gestor de arranque
- last-boot-CPU-flags (solo lectura) describe los indicadores de CPU en los que se inició la máquina virtual por última vez
- resident-on (solo lectura) el host de XenServer en el que reside una máquina virtual
- affinity (lectura/escritura) El host de XenServer en el que prefiere ejecutarse la máquina virtual. Utilizado por el comando xe vm-start para decidir dónde ejecutar la VM
- other-config (parámetro de mapa de lectura/escritura) Una lista de pares clave/valor que especifican parámetros de configuración adicionales para la máquina virtual.

  Por ejemplo, el par de clave/valor other-config de auto_poweron: **true** solicita iniciar la máquina virtual automáticamente después de que se inicie cualquier host del grupo. También debe establecer este parámetro en el de su agrupación other-config. Estos parámetros ahora están en desuso. Utilice el parámetro ha-restart-priority en su lugar.
- start-time (solo lectura) marca de tiempo de la fecha y hora en que se leyeron las métricas de la máquina virtual. Esta marca de tiempo tiene el formato yyyymmddThh:mm:ss z, donde z es el indicador de zona horaria militar de una sola letra, por ejemplo, Z para UTC (GMT)
- install-time (solo lectura) marca de tiempo de la fecha y hora en que se leyeron las métricas de la máquina virtual. Esta marca de tiempo tiene el formato yyyymmddThh:mm:ss z, donde z es el indicador de zona horaria militar de una sola letra, por ejemplo, Z para UTC (GMT)
- memory-actual (solo lectura) la memoria real que utiliza una VM
- VCPUs-number (solo lectura) el número de CPU virtuales asignadas a la VM para una VM Linux. Este número puede diferir de VCPUS-max y cambiarse sin necesidad de reiniciar la VM mediante el comando vm-vcpu-hotplug. Para obtener más información, consulte vm-vcpu-hotplug. Las máquinas virtuales de Windows siempre se ejecutan con el número de vCPU establecido en VCPUsmax y deben reiniciarse para cambiar este valor. El rendimiento disminuye drásticamente cuando se establece VCPUs-number en un valor superior al número de CPU físicas del host de XenServer.
- VCPUs-Utilization (parámetro de mapa de solo lectura) una lista de CPU virtuales y su peso

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- os-version (parámetro map de solo lectura) la versión del sistema operativo para la VM
- PV-drivers-version (parámetro de mapa de solo lectura) las versiones de los controladores paravirtualizados para la VM
- PV-drivers-detected (solo lectura) para la última versión de los controladores paravirtualizados para la VM
- memory (parámetro de mapa de solo lectura) métricas de memoria notificadas por el agente en la VM
- disks (parámetro de mapa de solo lectura) métricas de disco informadas por el agente en la VM
- networks (parámetro de mapa de solo lectura) métricas de red informadas por el agente en la VM
- other (parámetro de mapa de solo lectura) otras métricas notificadas por el agente en la VM
- guest-metrics-lastupdated (solo lectura) marca de tiempo cuando el agente invitado realizó la última escritura en estos campos. La marca de tiempo tiene el formato yyyymmddThh:mm:ss z, donde z es el indicador de zona horaria militar de una sola letra; por ejemplo, Z para UTC (GMT)
- actions-after-shutdown (lectura/escritura) que se debe realizar después de que la máquina virtual se haya apagado
- actions-after-reboot (lectura/escritura) que se debe realizar después de que la VM se haya reiniciado
- possible-hosts hosts potenciales de esta VM de solo lectura
- dom-id (solo lectura) ID de dominio (si está disponible, -1 en caso contrario)
- recommendations (solo lectura) Especificación XML de valores y rangos recomendados para las propiedades de esta máquina virtual
- xenstore-data (parámetro de asignación de lectura/escritura) Datos que se insertarán en el árbol xenstore (/local/domain/*domid*/vm-data) después de crear la máquina virtual
- is-a-snapshot (solo lectura) True si esta máquina virtual es una instantánea
- snapshot_of (solo lectura) el UUID de la máquina virtual de la que pertenece esta instantánea
- snapshots (solo lectura) los UUID de todas las instantáneas de esta VM
- snapshot_time (solo lectura) la marca de tiempo de la operación de instantánea que creó esta instantánea de VM

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- memory-target (solo lectura) la cantidad objetivo de memoria establecida para esta VM
- blocked-operations (parámetro de mapa de lectura/escritura) enumera las operaciones que no se pueden realizar en esta máquina virtual
- last-boot-record (solo lectura) de los últimos parámetros de arranque para esta plantilla, en formato XML
- ha-always-run (lectura/escritura) True si esta máquina virtual se reinicia siempre en otro host si se produce un error en el host en el que reside. Este parámetro ahora está en desuso. Utilice el parámetro ha-restart-priority en su lugar.
- ha-restart-priority (lectura/escritura) reinicio o lo mejor que se pueda hacer
- blobs (solo lectura) almacén de datos binarios
- live (solo lectura) True si la máquina virtual está en ejecución. False si HA sospecha que la VM no se está ejecutando.

vm-assert-can-be-recovered

```
1 xe vm-assert-can-be-recovered uuid [database] vdi-uuid
2 <!--NeedCopy-->
```

Comprueba si hay almacenamiento disponible para recuperar esta VM.

vm-call-plugin

```
1 xe vm-call-plugin vm-uuid=vm_uuid plugin=plugin fn=function [args:key=
     value]
2 <!--NeedCopy-->
```

Llama a la función dentro del complemento en la máquina virtual dada con argumentos opcionales (args:key=value). Para pasar una cadena de "valor"con caracteres especiales (por ejemplo, una línea nueva), se puede usar una sintaxis alternativa args:key:file=local_file, donde se recuperará el contenido de local_file y se asignará a "key"como un todo.

vm-cd-add

```
1 xe vm-cd-add cd-name=name_of_new_cd device=
     integer_value_of_an_available_vbd [vm-selector=vm_selector_value...]
2 <!--NeedCopy-->
```

Agregue un nuevo CD virtual a la máquina virtual seleccionada. Seleccione el parámetro device entre el valor del parámetro allowed-VBD-devices de la máquina virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

vm-cd-eject

```
xe vm-cd-eject [vm-selector=vm_selector_value...]
<!--NeedCopy-->
```

Expulse un CD de la unidad de CD virtual. Este comando solo funciona si hay exactamente un CD conectado a la VM. Cuando haya dos o más CD, use el comando `xe vbd-eject` y especifique el UUID del VBD.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

vm-cd-insert

```
xe vm-cd-insert cd-name=name_of_cd [vm-selector=vm_selector_value...]
<!--NeedCopy-->
```

Inserte un CD en la unidad de CD virtual. Este comando solo funciona si hay exactamente un dispositivo de CD vacío conectado a la VM. Cuando haya dos o más dispositivos de CD vacíos, utilice el comando `xe vbd-insert` y especifique los UUID del VBD y del VDI que se van a insertar.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

vm-cd-list

```
xe vm-cd-list [vbd-params] [vdi-params] [vm-selector=vm_selector_value
    ...]
<!--NeedCopy-->
```

Muestra los CD adjuntos a las máquinas virtuales especificadas.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

También puede seleccionar los parámetros VBD y VDI que quiere enumerar.

vm-cd-remove

```
xe vm-cd-remove cd-name=name_of_cd [vm-selector=vm_selector_value...]
<!--NeedCopy-->
```

Retire un CD virtual de las máquinas virtuales especificadas.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

vm-checkpoint

```
xe vm-checkpoint new-name-label=name_label [new-name-description=
    description]
<!--NeedCopy-->
```

Controle una VM existente, mediante la operación rápida de instantáneas de disco a nivel de almacenamiento cuando esté disponible.

vm-clone

```
xe vm-clone new-name-label=name_for_clone [new-name-description=
    description_for_clone] [vm-selector=vm_selector_value...]
<!--NeedCopy-->
```

Clone una VM existente, mediante la operación de clonación rápida de discos a nivel de almacenamiento, donde esté disponible. Especifique el nombre y la descripción opcional de la máquina virtual clonada resultante mediante los argumentos **new**-name-**label** y **new**-name-description.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

vm-compute-maximum-memory

```
xe vm-compute-maximum-memory total=
    amount_of_available_physical_ram_in_bytes [approximate=add overhead
    memory for additional vCPUS? true|false] [vm_selector=
    vm_selector_value...]
<!--NeedCopy-->
```

Calcule la cantidad máxima de memoria estática que se puede asignar a una VM existente, mediante la cantidad total de RAM física como límite superior. El parámetro opcional `approximate` reserva suficiente memoria adicional en el cálculo para tener en cuenta la adición de vCPU adicionales a la VM más adelante.

Por ejemplo:

```
xe vm-compute-maximum-memory vm=testvm total=`xe host-list params=
    memory-free --minimal`
<!--NeedCopy-->
```

Este comando usa el valor del parámetro `memory-free` devuelto por el comando `xe host-list` para establecer la memoria máxima de la máquina virtual denominada `testvm`.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

vm-compute-memory-overhead

```
xe vm-compute-memory-overhead
<!--NeedCopy-->
```

Calcula la sobrecarga de memoria de virtualización de una VM.

vm-copy

```
xe vm-copy new-name-label=name_for_copy [new-name-description=
    description_for_copy] [sr-uuid=uuid_of_sr] [vm-selector=
    vm_selector_value...]
<!--NeedCopy-->
```

Copie una VM existente, pero sin usar la operación de clonación rápida de disco a nivel de almacenamiento (incluso si esta opción está disponible). Se garantiza que las imágenes de disco de la máquina virtual copiada sean *imágenes completas*, es decir, que no formen parte de una cadena de copia en escritura (CoW).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Especifique el nombre y la descripción opcional de la máquina virtual copiada resultante mediante los argumentos **new**-name-**label** y **new**-name-description.

Especifique el SR de destino para la máquina virtual copiada resultante mediante el sr-uuid. Si no se especifica este parámetro, el destino es el mismo SR en el que se encuentra la máquina virtual original.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

vm-copy-bios-strings

```
xe vm-copy-bios-strings host-uuid=host_uuid
<!--NeedCopy-->
```

Copie las cadenas de BIOS del host dado en la VM.

> **Nota:**
>
> Después de iniciar una VM por primera vez, no puede cambiar sus cadenas de BIOS. Asegúrese de que las cadenas del BIOS sean correctas antes de iniciar la VM por primera vez.

vm-crashdump-list

```
xe vm-crashdump-list [vm-selector=vm selector value...]
<!--NeedCopy-->
```

Enumera los volcados de memoria asociados a las máquinas virtuales especificadas.

Cuando se usa el argumento opcional params, el valor de params es una cadena que contiene una lista de parámetros de este objeto que quiere mostrar. Como alternativa, puede usar la palabra clave all para mostrar todos los parámetros. Si params no se usa, la lista devuelta muestra un subconjunto predeterminado de todos los parámetros disponibles.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

vm-data-source-list

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe vm-data-source-list [vm-selector=vm selector value...]
<!--NeedCopy-->
```

Enumere las fuentes de datos que se pueden grabar para una VM.

Seleccione las máquinas virtuales en las que quiere realizar esta operación mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección. Si no se proporcionan parámetros para seleccionar hosts, la operación se lleva a cabo en todas las máquinas virtuales.

Las fuentes de datos tienen dos parámetros (`standard` y `enabled`) que puede ver en el resultado de este comando. Si un origen de datos tiene `enabled` establecido en **`true`**, las métricas se están registrando actualmente en la base de datos de rendimiento. Si un origen de datos tiene `standard` establecido en **`true`**, las métricas se registran en la base de datos de rendimiento de forma predeterminada (y también `enabled` se establece en **`true`** para este origen de datos). Si un origen de datos tiene `standard` establecido en **`false`**, las métricas *no* se registran en la base de datos de rendimiento de forma predeterminada (y también `enabled` se establece en **`false`** para este origen de datos).

Para empezar a registrar métricas de fuentes de datos en la base de datos de rendimiento, ejecute el comando `vm-data-source-record`. Este comando establece `enabled` en **`true`**. Para detener, ejecute el `vm-data-source-forget`. Este comando establece `enabled` en **`false`**.

vm-data-source-record

```
xe vm-data-source-record data-source=name_description_of_data-source [
   vm-selector=vm selector value...]
<!--NeedCopy-->
```

Registre la fuente de datos especificada para una VM.

Esta operación escribe la información de la fuente de datos en la base de datos de métricas de rendimiento persistentes de las máquinas virtuales especificadas. Por motivos de rendimiento, esta base de datos es distinta de la base de datos de agentes normal.

Seleccione las máquinas virtuales en las que quiere realizar esta operación mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección. Si no se proporcionan parámetros para seleccionar hosts, la operación se lleva a cabo en todas las máquinas virtuales.

vm-data-source-forget

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe vm-data-source-forget data-source=name_description_of_data-source [
    vm-selector=vm selector value...]
<!--NeedCopy-->
```

Deje de grabar la fuente de datos especificada para una VM y olvide todos los datos grabados.

Seleccione las máquinas virtuales en las que quiere realizar esta operación mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección. Si no se proporcionan parámetros para seleccionar hosts, la operación se lleva a cabo en todas las máquinas virtuales.

vm-data-source-query

```
xe vm-data-source-query data-source=name_description_of_data-source [vm
    -selector=vm_selector_value...]
<!--NeedCopy-->
```

Muestra la fuente de datos especificada para una VM.

Seleccione las máquinas virtuales en las que quiere realizar esta operación mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección. Si no se proporcionan parámetros para seleccionar hosts, la operación se lleva a cabo en todas las máquinas virtuales.

vm-destroy

```
xe vm-destroy uuid=uuid_of_vm
<!--NeedCopy-->
```

Destruye la VM especificada. Esto deja intacto el almacenamiento asociado a la VM. Para eliminar también el almacenamiento, use `xe vm-uninstall`.

vm-disk-add

```
xe vm-disk-add disk-size=size_of_disk_to_add device=uuid_of_device [vm-
    selector=vm_selector_value...]
<!--NeedCopy-->
```

Agregue un disco a las máquinas virtuales especificadas. Seleccione el parámetro `device` del valor del parámetro `allowed-VBD-devices` de las máquinas virtuales.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El parámetro `disk-size` se puede especificar en bytes o mediante los sufijos estándar IEC KiB, MiB, GiB y TiB.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

vm-disk-list

```
xe vm-disk-list [vbd-params] [vdi-params] [vm-selector=
    vm_selector_value...]
<!--NeedCopy-->
```

Enumera los discos conectados a las VM especificadas. Los parámetros `vbd-params` y `vdi-params` controlan los campos de los objetos respectivos que se van a emitir. Indique los parámetros como una lista separada por comas o la clave especial `all` para la lista completa.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

vm-disk-remove

```
xe vm-disk-remove device=integer_label_of_disk [vm-selector=
    vm_selector_value...]
<!--NeedCopy-->
```

Retire un disco de las máquinas virtuales especificadas y destrúyalo.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

vm-export

```
xe vm-export filename=export_filename [metadata=true|false] [vm-
    selector=vm_selector_value...]
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Exporte las máquinas virtuales especificadas (incluidas las imágenes de disco) a un archivo en la máquina local. Especifique el nombre de archivo al que exportar la máquina virtual mediante el parámetro `filename`. Por convención, el nombre del archivo tiene una `.xva` extensión.

Si el parámetro `metadata` es **`true`**, los discos no se exportan. Solo se escriben los metadatos de la VM en el archivo de salida. Use este parámetro cuando el almacenamiento subyacente se transfiera a través de otros mecanismos y permita que se vuelva a crear la información de la VM. Para obtener más información, consulte `vm-import`.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

vm-import

```
xe vm-import filename=export_filename [metadata=true|false] [preserve=
    true|false][sr-uuid=destination_sr_uuid]
<!--NeedCopy-->
```

Importe una VM desde un archivo exportado anteriormente. Si `preserve` se establece en **`true`**, se conserva la dirección MAC de la máquina virtual original. `sr-uuid` determina el SR de destino en el que se importará la VM. Si no se especifica este parámetro, se utiliza el SR predeterminado.

Si `metadata` es **`true`**, puede importar un conjunto de metadatos previamente exportado sin sus bloques de disco asociados. La importación solo de metadatos falla si no se puede encontrar ningún VDI (nombrado por SR y `VDI.location`) a menos que se especifique la opción `--force`, en cuyo caso la importación continúa independientemente. Si los discos se pueden duplicar o mover fuera de banda, la importación/exportación de metadatos es una forma rápida de mover las VM entre grupos separados. Por ejemplo, como parte de un plan de recuperación ante desastres.

> **Nota:**
>
> Las importaciones de varias máquinas virtuales se realizan más rápido en serie que en paralelo.

vm-install

```
xe vm-install new-name-label=name [template-uuid=
    uuid_of_desired_template] [template=template_uuid_or_name] [sr-uuid=
    sr_uuid | sr-name-label=name_of_sr][copy-bios-strings-from=host_uuid
    ]
<!--NeedCopy-->
```

Instale o clone una VM a partir de una plantilla. Especifique el nombre de la plantilla mediante el argumento `template-uuid` o `template`. Especifique un SR mediante el argumento `sr-uuid` o

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

sr-name-**label**. Especifique para instalar medios bloqueados por BIOS mediante el argumento copy-bios-strings-from.

> **Nota:**
>
> Al instalar desde una plantilla que tiene discos existentes, de forma predeterminada, los discos nuevos se crean en la misma SR que estos discos existentes. Cuando el SR lo admite, estos discos son copias rápidas. Si se especifica un SR diferente en la línea de comandos, los discos nuevos se crean allí. En este caso, no es posible realizar una copia rápida y los discos son copias completas.
>
> Cuando se instala desde una plantilla que no tiene discos existentes, cualquier disco nuevo se crea en el SR especificado o en el SR predeterminado del grupo cuando no se especifica un SR.

vm-is-bios-customized

```
xe vm-is-bios-customized
<!--NeedCopy-->
```

Indica si las cadenas de BIOS de la VM se han personalizado.

vm-memory-dynamic-range-set

```
xe vm-memory-dynamic-range-set min=min max=max
<!--NeedCopy-->
```

Configure el rango de memoria dinámica de una VM. El rango de memoria dinámica define límites inferiores y superiores suaves para la memoria de una VM. Es posible cambiar estos campos cuando una VM se está ejecutando o se detiene. El rango dinámico debe ajustarse al rango estático.

vm-memory-limits-set

```
xe vm-memory-limits-set static-min=static_min static-max=static_max
    dynamic-min=dynamic_min dynamic-max=dynamic_max
<!--NeedCopy-->
```

Configure los límites de memoria de una VM.

vm-memory-set

```
xe vm-memory-set memory=memory
<!--NeedCopy-->
```

Configure la asignación de memoria de una VM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

vm-memory-shadow-multiplier-set

```
xe vm-memory-shadow-multiplier-set [vm-selector=vm_selector_value...] [
   multiplier=float_memory_multiplier]
<!--NeedCopy-->
```

Configure el multiplicador de memoria instantánea para la máquina virtual especificada.

Se trata de una opción avanzada que modifica la cantidad de *memoria oculta* asignada a una máquina virtual asistida por hardware.

En algunas cargas de trabajo de aplicaciones especializadas, como Citrix Virtual Apps, se requiere memoria oculta adicional para lograr un rendimiento completo.

Esta memoria se considera una sobrecarga. Se separa de los cálculos de memoria normales para la memoria de cuentas de una máquina virtual. Cuando se invoca este comando, la cantidad de memoria de host libre disminuye según el multiplicador y el campo `HVM_shadow_multiplier` se actualiza con el valor que Xen ha asignado a la VM. Si no hay suficiente memoria libre en el host de XenServer, se devuelve un error.

Las máquinas virtuales en las que se realizará esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM.

vm-memory-static-range-set

```
xe vm-memory-static-range-set min=min max=max
<!--NeedCopy-->
```

Configure el rango de memoria estática de una VM. El rango de memoria estática define los límites inferior y superior duros para la memoria de una VM. Es posible cambiar estos campos solo cuando se detiene una VM. El rango estático debe abarcar el rango dinámico.

vm-memory-target-set

```
xe vm-memory-target-set target=target
<!--NeedCopy-->
```

Establezca el objetivo de memoria para una VM detenida o en ejecución. El valor dado debe estar dentro del rango definido por los valores memory_static_min y memory_static_max de la VM.

vm-migrate

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
xe vm-migrate [compress=true|false] [copy=true|false] [host-uuid=
    destination_host_uuid] [host=name_or_ uuid_of_destination_host] [
    force=true|false] [live=true|false] [vm-selector=vm_selector_value
    ...] [remote-master=destination_pool_master_uuid] [remote-username=
    destination_pool_username] [remote-password=
    destination_pool_password] [remote-network=
    destination_pool_network_uuid ][vif:source_vif_uuid=
    destination_network_uuid] [vdi:vdi_uuid=destination_sr_uuid]
<!--NeedCopy-->
```

Este comando migra las máquinas virtuales especificadas entre hosts físicos.

El `compress` parámetro anula el parámetro de `migration-compression` grupo de `xe pool-param-set`.

El `host` parámetro del comando `vm-migrate` puede ser el nombre o el UUID del host de XenServer. Por ejemplo, para migrar la VM a otro host del grupo, donde los discos de VM se encuentran en almacenamiento compartido por ambos hosts:

```
xe vm-migrate uuid=vm_uuid host-uuid=destination_host_uuid
<!--NeedCopy-->
```

Para mover máquinas virtuales entre hosts del mismo grupo que no comparten almacenamiento (migración de almacenamiento en vivo):

```
xe vm-migrate uuid=vm_uuid host-uuid=destination_host_uuid \
    remote-master=192.0.2.35 remote-username=username remote-password=
       password
<!--NeedCopy-->
```

Para la migración en vivo del almacenamiento, debe proporcionar el nombre de host o la dirección IP, el nombre de usuario y la contraseña del coordinador del grupo, incluso cuando esté migrando dentro del mismo grupo.

Puede elegir la SR en la que se almacena cada VDI:

```
xe vm-migrate uuid=vm_uuid remote-master=192.0.2.35 remote-username=
    username remote-password=password host-uuid=destination_host_uuid \
    vdi:vdi_1=destination_sr1_uuid \
    vdi:vdi_2=destination_sr2_uuid \
    vdi:vdi_3=destination_sr3_uuid
<!--NeedCopy-->
```

Además, puede elegir qué red quiere conectar la VM después de la migración:

```
xe vm-migrate uuid=vm_uuid \
    vdi1:vdi_1_uuid=destination_sr1_uuid \
    vdi2:vdi_2_uuid=destination_sr2_uuid \
    vdi3:vdi_3_uuid=destination_sr3_uuid \
    vif:source_vif_uuid=destination_network_uuid
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para la migración entre grupos:

```
xe vm-migrate uuid=vm_uuid remote-master=192.0.2.35 \
    remote-username=username remote-password=password \
    host-uuid=destination_host_uuid  \
    vif:source_vif_uuid=destination_network_uuid \
    vdi:vdi_uuid=destination_sr_uuid
<!--NeedCopy-->
```

Para obtener más información sobre la migración en vivo del almacenamiento, la migración en vivo y la migración de VDI en vivo, consulte Migración de máquinas virtuales.

> **Nota:**
>
> Si está actualizando desde una versión anterior de XenServer o Citrix Hypervisor, es posible que deba apagar y arrancar todas las máquinas virtuales después de migrarlas para asegurarse de que se incorporan las nuevas funciones de virtualización.

De forma predeterminada, la VM se suspende, migra y reanuda en el otro host. El parámetro `live` selecciona la migración en vivo. La migración en vivo mantiene la máquina virtual en funcionamiento mientras se realiza la migración, lo que minimiza el tiempo de inactividad de la máquina virtual. En algunas circunstancias, como las cargas de trabajo que consumen mucha memoria en la VM, la migración en vivo vuelve al modo predeterminado y suspende la VM durante un breve período antes de completar la transferencia de memoria.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

vm-pause

```
xe vm-pause
<!--NeedCopy-->
```

Ponga en pausa una VM en ejecución. Tenga en cuenta que esta operación no libera la memoria asociada (consulte `vm-suspend`).

vm-reboot

```
xe vm-reboot [vm-selector=vm_selector_value...] [force=true]
<!--NeedCopy-->
```

Reinicie las VM especificadas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

Use el argumento `force` para provocar un reinicio implacable. Donde el apagado es similar a desconectar un servidor físico.

vm-recover

```
xe vm-recover vm-uuid [database] [vdi-uuid] [force]
<!--NeedCopy-->
```

Recupera una VM de la base de datos contenida en la VDI suministrada.

vm-reset-powerstate

```
xe vm-reset-powerstate [vm-selector=vm_selector_value...] {
 force=true }

<!--NeedCopy-->
```

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

Se trata de un comando *avanzado* que solo se utiliza cuando un host miembro de un grupo se desactiva. Puede usar este comando para forzar al coordinador del grupo a restablecer el estado de energía de las máquinas virtuales `halted`. Básicamente, este comando fuerza el bloqueo de la máquina virtual y sus discos para que se pueda iniciar a continuación en otro host de grupo. Esta llamada *requiere que* se especifique la marca force y falla si no está en la línea de comandos.

vm-restart-device-models

```
xe vm-restart-device-models [vm-selector=vm_selector_value...]
<!--NeedCopy-->
```

Reinicie el modelo de dispositivo para esta máquina virtual en el host. Mientras se reinicia el modelo de dispositivo, no puede detener, iniciar ni migrar la máquina virtual. Es posible que el usuario final de la máquina virtual experimente una pausa leve y se reanude su sesión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Para que la acción de reinicio del modelo de dispositivo sea compatible con una máquina virtual Windows, la máquina virtual debe tener instalado XenServer VM Tools para Windows.

vm-resume

```
xe vm-resume [vm-selector=vm_selector_value...] [force=true|false] [on=
    host_uuid]
<!--NeedCopy-->
```

Reanude las máquinas virtuales especificadas.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

Si la máquina virtual está en un SR compartido en un grupo de hosts, utilice el argumento `on` para especificar en qué miembro del grupo se va a iniciar. De forma predeterminada, el sistema determina un host apropiado, que puede ser cualquiera de los miembros del grupo.

vm-retrieve-wlb-recommendations

```
xe vm-retrieve-wlb-recommendations
<!--NeedCopy-->
```

Recupere las recomendaciones de equilibrio de carga de trabajo para la VM seleccionada.

vm-shutdown

```
xe vm-shutdown [vm-selector=vm_selector_value...] [force=true|false]
<!--NeedCopy-->
```

Apague la VM especificada.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

Utilice el argumento `force` para provocar un apagado incorrecto, similar a tirar del enchufe en un servidor físico.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

vm-snapshot

```
xe vm-snapshot new-name-label=name_label [new-name-description+
    name_description]
<!--NeedCopy-->
```

Realice una instantánea de una VM existente, utilizando la operación de instantánea de disco rápida a nivel de almacenamiento cuando esté disponible.

vm-start

```
xe vm-start [vm-selector=vm_selector_value...] [force=true|false] [on=
    host_uuid] [--multiple]
<!--NeedCopy-->
```

Inicie las máquinas virtuales especificadas.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

Si las máquinas virtuales están en un SR compartido en un grupo de hosts, utilice el argumento on para especificar en qué miembro del grupo se van a iniciar las máquinas virtuales. De forma predeterminada, el sistema determina un host apropiado, que puede ser cualquiera de los miembros del grupo.

vm-suspend

```
xe vm-suspend [vm-selector=vm_selector_value...]
<!--NeedCopy-->
```

Suspenda la VM especificada.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

vm-uninstall

```
xe vm-uninstall [vm-selector=vm_selector_value...] [force=true|false]
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Desinstale una VM y destruya sus discos (los VDI marcados como RW y conectados a esta VM únicamente) además de su registro de metadatos. Para destruir solo los metadatos de la VM, use `xe vm-destroy`.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

vm-unpause

```
xe vm-unpause
<!--NeedCopy-->
```

Reanuda una VM en pausa.

vm-vcpu-hotplug

```
xe vm-vcpu-hotplug new-vcpus=new_total_vcpu_count [vm-selector=
   vm_selector_value...]
<!--NeedCopy-->
```

Ajuste dinámicamente la cantidad de vCPU disponibles para una VM Linux en ejecución. El número de CPU virtuales está limitado por el parámetro `VCPUs-max`. Las máquinas virtuales de Windows siempre se ejecutan con el número de vCPU establecido en `VCPUs-max` y deben reiniciarse para cambiar este valor.

Usa el **`new`**`-vcpus`parámetro para definir la nueva cantidad *total* de vCPU que deseas tener después de ejecutar este comando. No utilices este parámetro para pasar la cantidad de vCPU que deseas agregar. Por ejemplo, si ya tiene dos vCPU en su máquina virtual y desea agregar dos CPU virtuales más, especifíquelo**`new`**`-vcpus=4`.

Las máquinas virtuales Linux o Windows en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

> **Nota:**
>
> Cuando ejecute máquinas virtuales Linux sin las herramientas de máquinas virtuales de XenServer instaladas, ejecute el siguiente comando en la máquina virtual para asegurarse de que `root` se utilizan las vCPU recién conectadas en caliente: `# for i in /sys/devices /system/cpu/cpu[1-9]*/online; do if [ "$(cat $i)"= 0 ]; then echo`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  1 > $i; fi; done
```

vm-vif-list

```
1 xe vm-vif-list [vm-selector=vm_selector_value...]
2 <!--NeedCopy-->
```

Enumera las VIF de las máquinas virtuales especificadas.

La máquina virtual o las máquinas virtuales en las que se realiza esta operación se seleccionan mediante el mecanismo de selección estándar. Para obtener más información, consulte Selectores de VM. Los selectores funcionan en los registros de VM al filtrar, y *no* en los valores VIF. Los argumentos opcionales pueden ser cualquier número de los parámetros de VM enumerados al principio de esta sección.

Instantáneas programadas

Comandos para controlar las instantáneas programadas de VM y sus atributos.

Los objetos `vmss` se pueden enumerar con el comando estándar de listado de objetos (`xe vmss -list`) y los parámetros se pueden manipular con los comandos de parámetros estándar. Para obtener más información, consulte Comandos de parámetros de bajo nivel

vmss-create

```
1 xe vmss-create enabled=True/False name-label=name type=type frequency=
     frequency retained-snapshots=value name-description=description
     schedule:schedule
2 <!--NeedCopy-->
```

Crea una programación de instantáneas en el grupo.

Por ejemplo:

```
1 xe vmss-create retained-snapshots=9 enabled=true frequency=daily \
2     name-description=sample name-label=samplepolicy type=snapshot \
3     schedule:hour=10 schedule:min=30
4 <!--NeedCopy-->
```

Las programaciones de instantáneas tienen los siguientes parámetros:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del parámetro	Descripción	Tipo
name-**label**	Nombre de la programación de instantáneas.	Lectura/Escritura
name-description	Descripción de la programación de instantáneas.	Lectura/Escritura
type	Snapshot de disco o snapshot de memoria.	Lectura/Escritura
frequency	Cada hora; diaria; semanal	Lectura/Escritura
retained-snapshots	Instantáneas que se conservarán. Intervalo: 1-10.	Lectura/Escritura
schedule	schedule:days (de lunes a domingo), schedule:hours (de 0 a 23), schedule:minutes (0, 15, 30, 45)	Lectura/Escritura

vmss-destroy

```
xe vmss-destroy uuid=uuid
<!--NeedCopy-->
```

Destruye una programación de instantáneas en el grupo.

Paso a través de USB

La transferencia USB es compatible con las siguientes versiones de USB: 1.1, 2.0 y 3.0.

Activación/desactivación de paso a través de USB

```
xe pusb-param-set uuid=pusb_uuid passthrough-enabled=true/false
<!--NeedCopy-->
```

Habilitar/inhabilitar el paso a través de USB.

pusb-scan

```
xe pusb-scan host-uuid=host_uuid
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Escanee PUSB y actualice.

vusb-create

```
xe vusb-create usb-group-uuid=usb_group_uuid vm-uuid=vm_uuid
<!--NeedCopy-->
```

Crea un USB virtual en el grupo. Inicie la VM para pasar a través del USB a la VM.

vusb-unplug

```
xe vusb-unplug uuid=vusb_uuid
<!--NeedCopy-->
```

Desconecta el USB de la VM.

vusb-destroy

```
xe vusb-destroy uuid=vusb_uuid
<!--NeedCopy-->
```

Elimina la lista de USB virtuales de la VM.

---

layout: doc
description: Learn about the levels of support for XenServer and the logs that are available to help with troubleshooting.—

Solución de problemas

Si tiene problemas técnicos con el host de XenServer, esta sección le ayudará a resolver el problema si es posible. Si no es posible, use la información de esta sección para recopilar los registros de la aplicación y otros datos que puedan ayudar al servicio de asistencia a rastrear y resolver el problema.

En los artículos siguientes se proporciona información sobre la solución de problemas sobre áreas específicas del producto:

- Solución de problemas de
- Resolver problemas
- Solución de problemas de agrupaciones en clúisteres

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Solución de problemas de XenCenter
- Solución de problemas de Workload Balancing
- Solución de problemas de Conversion Manager

Solucionar problemas de conexiones entre XenCenter y el host de XenServer

Si tiene problemas para conectarse al host de XenServer con XenCenter, compruebe lo siguiente:

- ¿Su XenCenter es una versión anterior a la del host de XenServer al que intenta conectarse?

  XenCenter 8.2.7 y versiones anteriores no son compatibles con los hosts de XenServer 8. Para administrar los hosts o grupos de XenServer 8, necesita la versión más reciente de XenCenter con una versión con el formato aaaa.x.x.

  Para corregir este problema, instale la versión más reciente de XenCenter.

- ¿Está vigente su licencia?

  Puede ver la fecha de caducidad del código de acceso a la licencia en la ficha **General** del host de XenServer, en la sección **Detalles de licencia** de XenCenter.

  Para obtener más información sobre la licencia de un host, consulte Licencias.

- El host de XenServer se comunica con XenCenter mediante HTTPS a través de los siguientes puertos:

  - Puerto 443 (una conexión bidireccional para comandos y respuestas mediante la API de administración)
  - Puerto 5900 para conexiones VNC gráficas con máquinas virtuales Linux paravirtualizadas.

  Si tiene un firewall habilitado entre el host de XenServer y la máquina que ejecuta el software cliente, asegúrese de que permita el tráfico desde estos puertos. Para obtener más información, consulte Conectividad a Internet.

Recopile los registros de XenServer y XenCenter

Registros del host de XenServer

XenCenter se puede usar para recopilar información sobre el host de XenServer.

Haga clic en **Informe de estado del servidor** en el menú **Herramientas** para abrir la tarea **Informe de estado del servidor**. Puede seleccionar de una lista de diferentes tipos de información (varios registros, volcados de memoria, etc.). La información se compila y descarga en la máquina en la que se ejecuta XenCenter. Para obtener más información, consulte la documentación de XenCenter.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

De forma predeterminada, los archivos recopilados para un informe de estado del servidor pueden tener un tamaño limitado. Si necesita archivos de registro más grandes que los predeterminados, puede ejecutar el comando `xenserver-status-report -u` en la consola host de XenServer.

> **Importante:**
>
> Los registros del host de XenServer pueden contener información confidencial.

Enviar mensajes de registro de host a un servidor central En lugar de escribir los registros en el sistema de archivos del dominio de control, puede configurar el host de XenServer para que los escriba en un servidor remoto. El servidor remoto debe tener el demonio `syslogd` ejecutándose en él para recibir los registros y agregarlos correctamente. El demonio `syslogd` es una parte estándar de todos los tipos de Linux y Unix, y las versiones de terceros están disponibles para Windows y otros sistemas operativos.

Establezca el parámetro syslog_destination en el nombre de host o la dirección IP del servidor remoto en el que desea que se escriban los registros:

```
xe host-param-set uuid=host_uuid logging:syslog_destination=hostname
<!--NeedCopy-->
```

Ejecute el comando:

```
xe host-syslog-reconfigure uuid=host_uuid
<!--NeedCopy-->
```

Para hacer cumplir el cambio. (También puede ejecutar este comando de forma remota especificando el parámetro `host`).

Registros de XenCenter

XenCenter también tiene un registro del lado del cliente. Este archivo incluye una descripción completa de todas las operaciones y los errores que se producen al usar XenCenter. También contiene registros informativos de eventos que le proporcionan una pista de auditoría de varias acciones que se han producido. El archivo de registro de XenCenter se almacena en la carpeta de perfil en la siguiente ruta:. `%userprofile%\AppData\Roaming\XenServer\XenCenter\logs\XenCenter.log`

Para buscar los archivos de registro de XenCenter, por ejemplo, cuando quiera abrir el archivo de registro o enviarlo por correo electrónico, haga clic en **Ver archivos de registro de XenCenter** en el menú **Ayuda** de XenCenter.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Registros de la instalación

Si se produce un error desconocido durante la instalación, capture el archivo de registro de su host y envíelo al Soporte técnico.

Con un teclado conectado directamente a la máquina host (no conectado a través de un puerto serie), puede acceder a tres terminales virtuales durante la instalación:

- Presione **Alt+F1** para acceder al instalador principal de XenServer
- Presione **Alt+F2** para acceder a un shell local
- Presione **Alt+F3** para acceder al registro de eventos

Para capturar y guardar los archivos de registro:

1. Presione **Alt+F2** para acceder al shell local.
2. Escriba lo siguiente:

```
/opt/xensource/installer/report.py
<!--NeedCopy-->
```

3. Se le pedirá que elija dónde desea guardar el archivo de registro: **NFS**, **FTP**o **medios locales**.

   Seleccione **NFS** o **FTP** para copiar el archivo de registro en otro equipo de la red. Para hacerlo, las redes deben funcionar correctamente y debe tener acceso de escritura a una máquina remota.

   Seleccione **Medios locales** para guardar el archivo en un dispositivo de almacenamiento extraíble, como una unidad flash USB, en el equipo local.

   Una vez que haya hecho sus selecciones, el programa escribe el archivo de registro en la ubicación elegida. El nombre del archivo es `support.tar.bz2`.

---

layout: doc
description: Learn about the levels of support for XenServer—

Asistencia

Ofrecemos servicios de asistencia técnica a los clientes con una licencia de XenServer Premium Edition o Standard Edition. Para acceder a esta asistencia, puede abrir un caso en línea o contactar con el centro de asistencia por teléfono si tiene dificultades técnicas. Para obtener más información, consulte la página de asistencia de XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si usa XenServer Trial Edition (sin licencia), no podrá acceder a esta asistencia, pero valoramos sus comentarios. Para obtener más información, consulte Enviar comentarios sobre XenServer y XenCenter.

> **Nota:**
>
> Si instaló XenServer 8 durante el período de Technical Preview, debe aplicar las actualizaciones publicadas el 18 de marzo de 2024 o después para que su grupo alcance un nivel compatible con producción con derecho a asistencia técnica.

Actualizaciones frecuentes

XenServer 8 usa un modelo de actualización frecuente que ofrece funciones, correcciones y mejoras a los hosts. Esperamos que use estas actualizaciones en un plazo de seis meses por cuestiones de compatibilidad. Si el nivel de actualización de su grupo tiene más de seis meses, le pediremos que reproduzca el problema en el nivel de actualización más reciente.

Lista de verificación de asistencia

Esta sección le guía a través de las posibles acciones que puede tomar cuando se produce un problema en su entorno de XenServer. Al completar todos los pasos que pueda, nos ayudará a solucionar su problema más rápido.

Primeros pasos

Cuando observe el problema por primera vez, complete estos pasos:

1. Antes de llevar a cabo cualquier paso de recuperación, capture todos los registros que pueda del entorno:

   - Si el problema está relacionado con XenServer, capture un informe de estado del servidor (SSR) del host o grupo en el que se detectó el problema. Vaya al menú **Herramientas** de XenCenter y, a continuación, al **Informe de estado del servidor**.
   - Si el problema está relacionado con XenCenter:
     - Para obtener los archivos de registro de la aplicación, vaya al menú **Ayuda** de XenCenter y, a continuación, a **Ver los archivos de registro de XenCenter**.
     - Realice capturas de pantalla de las pantallas correspondientes.
   - Si el problema está relacionado con una máquina virtual, recopile todos los registros pertinentes del sistema operativo de la máquina virtual.

   Para obtener más información sobre cómo obtener información de registro, consulte Recopilar los registros de XenServer y XenCenter.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Anota la fecha de sincronización, la suma de comprobación de sincronización y la suma de comprobación de actualización del host o grupo. Para obtener más información, consulte Ver tareas pendientes.
3. Si es necesario, intente recuperar el entorno para que funcione.

Autoayuda

Proporcionamos información y orientación que pueden servirle de ayuda para diagnosticar y resolver los problemas que pueda tener.

1. Consulte esta documentación para obtener ayuda:
    - Problemas conocidos: en este artículo se enumeran los problemas conocidos de XenServer y, si corresponde, las soluciones alternativas que puede aplicar.
    - Acceso anticipado y normal: en estos artículos se enumeran las actualizaciones disponibles para XenServer. Es posible que se haya publicado recientemente una solución para su problema.
    - Solución de problemas: este artículo es un punto de entrada a la información de solución de problemas que se proporciona en la documentación.
    - Revise la sección de la documentación relacionada con la función que muestra el problema. Es posible que haya restricciones en esta función que estén causando el problema o que haya opciones de configuración que puedan servir de ayuda para solucionarlo.
2. Citrix Knowledge Center contiene muchos artículos escritos por nuestro equipo de asistencia técnica en los que se describen las soluciones a los problemas detectados anteriormente con XenServer.

Si realiza alguna acción de diagnóstico o cambia la configuración de su entorno como resultado de esta información, anótela y avísenos si se pone en contacto con el servicio de asistencia.

Actualizar a la versión más reciente

Si ya usa la versión más reciente de todos los componentes de XenServer, vaya a Capturar registros.

Si no ejecuta la versión más reciente de XenServer, XenCenter o un componente relacionado, es posible que la solución del problema esté incluida en la versión o el nivel de actualización más recientes. Le recomendamos que actualice su entorno a la versión más reciente, si es posible.

1. Actualice su grupo con la última actualización.
2. Actualice XenCenter a la versión más reciente.
3. Si el problema está relacionado con una máquina virtual Windows, actualice XenServer VM Tools para Windows a la versión más reciente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Si el problema está relacionado con una máquina virtual Linux, asegúrese de que esté instalada la versión más reciente de XenServer VM Tools para Linux. Estas herramientas están disponibles en https://xenserver.com/downloads.
5. Si el problema está relacionado con Workload Balancing o con XenServer Conversion Manager, asegúrese de utilizar la última versión disponible en https://xenserver.com/downloads.

Reproducir el problema en la última versión

Si actualizó alguno de los componentes de su entorno desde que se produjo el problema, intente reproducir el problema ahora.

Registros de captura

- Si el problema está relacionado con XenServer, capture un informe de estado del servidor (SSR) del host o grupo en el que se encontró el problema. Vaya al menú **Herramientas** de XenCenter y, a continuación, al **Informe de estado del servidor**.
- Si el problema está relacionado con XenCenter:
  - Para obtener los archivos de registro de la aplicación, vaya al menú **Ayuda** de XenCenter y, a continuación, a **Ver los archivos de registro de XenCenter**.
  - Realice capturas de pantalla de las pantallas correspondientes.
- Si el problema está relacionado con una máquina virtual, recopile todos los registros pertinentes del sistema operativo de la máquina virtual.

Contactar con asistencia técnica

Para conocer los métodos para ponerse en contacto con nosotros, consulte la página de asistencia de XenServer.

Proporcione la siguiente información para obtener asistencia:

- Fecha y hora en que se detectó el problema
- Canal de actualización de la agrupación (acceso anticipado o normal)
- Nombre del coordinador de la agrupación
- Fecha y hora en que la agrupación se sincronizó por última vez
- Suma de verificación de sincronización para el coordinador del grupo
- Fecha y hora en que se actualizó la agrupación por última vez
- Suma de comprobación de actualización para todos los hosts del grupo

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Cualquier captura de pantalla relevante que ayude a describir el problema
- Cualquier cambio o evento que pueda haber provocado el problema
- Cualquier solución alternativa conocida
- Cualquier medida de diagnóstico que ya haya tomado
- El SSR para el grupo con problemas
- Si corresponde, los registros de XenCenter

> **Nota:**
>
> Si no puede reproducir el problema en un grupo actualizado, adjunte el SSR que capturó cuando se produjo el problema por primera vez y explique por qué no pudo aplicar todas las actualizaciones.

Proporcionar comentarios sobre XenServer y XenCenter

Ayúdenos a mejorar nuestro producto proporcionando comentarios sobre las funciones y la usabilidad de nuestra nueva versión. Para enviar comentarios, no se ponga en contacto con el servicio de asistencia técnica; envíe un correo electrónico de comentarios. Los usuarios de la edición de prueba pueden informar de un error a través del portal de errores.

Enviar un correo electrónico de comentarios

Envíe sus comentarios y consultas por correo electrónico a feedback@xenserver.com. Para ayudarnos a entender el contexto completo de su situación, asegúrese de incluir la siguiente información en su correo electrónico de comentarios:

- Su nombre completo
- Su empresa o negocio
- Su ubicación geográfica
- Su tipo de licencia
- La cantidad de hosts de su implementación de producción
- El sistema operativo invitado en el que se produjo el problema (Windows o Linux)

No utilice esta dirección de correo electrónico para solicitar asistencia técnica.

Informar de un error (usuarios de la edición Trial Edition)

> **Nota:**
>
> Si eres cliente de las ediciones Premium o Standard, no utilice el portal de errores para solicitar

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> ayuda. Su problema se solucionará más rápido poniéndose en contacto con el servicio de asistencia técnica. Para obtener más información, consulte la página de asistencia de XenServer.

Para informar de un error, envíe un ticket mediante el portal de errores de XenServer 8.

- Cree una cuenta en el portal de errores de XenServer 8. Al crear su cuenta, asegúrese de utilizar un correo electrónico de contacto válido. Aunque nuestro objetivo es responderte en el tíquet, a veces puede ser necesario que nos pongamos en contacto con usted directamente por correo electrónico.
- Para registrar un error en el portal de errores de XenServer 8, haga clic en **Informar de un problema en XenServer**.

Los problemas que surgen a través del portal de errores de XenServer 8 se clasifican y es posible que nos comuniquemos con usted si el problema merece una investigación.

Avisos legales de terceros

August 24, 2023

Esta versión de XenServer incluye software de terceros con licencia de varias licencias diferentes.

Para extraer la información de licencias del producto y los componentes de XenServer instalados, consulte las instrucciones en Licencias y atribuciones de código abierto de XenServer.

Además, tenga en cuenta la siguiente información:

- Este producto incluye software desarrollado por OpenSSL Project para su uso en OpenSSL Toolkit. (http://www.openssl.org/)
- Este producto incluye software criptográfico escrito por Eric Young (eay@cryptsoft.com).
- XenServer High Availability funciona con everRun, una marca comercial registrada de Stratus Technologies Bermuda, Limited.

Licencias y atribución de código abierto de XenServer

April 10, 2024

El producto XenServer es una recopilación de paquetes de software. Cada paquete se rige por su propia licencia. Los términos de licencia completos aplicables a un paquete determinado se pueden encontrar en el RPM de origen del paquete, a menos que el paquete esté cubierto por una

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

licencia propietaria que no permita la redistribución de fuentes, en cuyo caso no hay RPM de origen disponible.

La distribución de XenServer contiene contenido de CentOS Linux y CentOS Stream. Cuando el Proyecto CentOS posee derechos de autor en los paquetes que componen las distribuciones CentOS Linux o CentOS Stream, esos derechos de autor se licencian bajo la licencia GPLv2, a menos que se indique lo contrario. Para obtener más información, consulte https://www.centos.org/legal/licensing-policy/.

Extraer información de atribución y licencia en un host XenServer instalado

Este artículo proporciona un método para extraer la información de licencias de todos los paquetes RPM incluidos en la instalación de XenServer.

Obtenga información general

Para enumerar todos los RPM y sus licencias:

1. Conéctese a la consola host de XenServer mediante SSH o mediante XenCenter.
2. En la línea de comandos de la consola, ejecute el siguiente comando:

```
rpm -qa --qf '%{
 name }
 -%{
 version }
 : %{
 license }
 \n'
```

Este comando enumera todos los componentes instalados y las licencias con las que se distribuyen. La salida tiene el siguiente formato:

```
readline-6.2: GPLv3+
gnupg2-2.0.22: GPLv3+
libdb-5.3.21: BSD and LGPLv2 and Sleepycat
rpm-python-4.11.3: GPLv2+
sqlite-3.7.17: Public Domain
qrencode-libs-3.4.1: LGPLv2+
libselinux-2.5: Public Domain
ustr-1.0.4: MIT or LGPLv2+ or BSD
gdbm-1.10: GPLv3+
procps-ng-3.3.10: GPL+ and GPLv2 and GPLv2+ and GPLv3+ and LGPLv2+
p11-kit-trust-0.23.5: BSD
device-mapper-libs-1.02.149: LGPLv2
xenserver-release-8.2.50: GPLv2
elfutils-libs-0.170: GPLv2+ or LGPLv3+
xz-libs-5.2.2: LGPLv2+
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
dbus-1.10.24: (GPLv2+ or AFL) and GPLv2+
elfutils-libelf-0.170: GPLv2+ or LGPLv3+
systemd-sysv-219: LGPLv2+
jemalloc-3.6.0: BSD
<!--NeedCopy-->
```

Obtenga información detallada

Para obtener una lista más completa de información sobre cada componente instalado:

1. Conéctese a la consola host de XenServer mediante SSH o mediante XenCenter.
2. En la línea de comandos de la consola, ejecute el siguiente comando:

   ```
   rpm -qai | sed '/^Name /i\\n'
   ```

   La salida tiene el siguiente formato:

   ```
   Name: host-upgrade-plugin
   Version     : 2.2.6
   Release     : 1.xs8
   Architecture: noarch
   Install Date: Wed 23 Aug 2023 01:54:25 PM UTC
   Group: Unspecified
   Size: 101626
   License     : GPL
   Signature   : RSA/SHA256, Tue 30 May 2023 10:01:44 AM UTC, Key ID
      5259d0b0f6529a4e
   Source RPM  : host-upgrade-plugin-2.2.6-1.xs8.src.rpm
   Build Date  : Fri 26 May 2023 03:05:49 AM UTC
   Build Host  : cf27e1dd25c54cbb8cef79726ed2bf2c
   Relocations : (not relocatable)
   Packager    : Koji
   Vendor      : Cloud Software Group, Inc.
   Summary     : Host upgrade plugin
   Description :
   Host upgrade plugin.

   Name        : m4
   Version     : 1.4.16
   Release     : 10.el7
   Architecture: x86_64
   Install Date: Wed 23 Aug 2023 01:52:31 PM UTC
   Group       : Applications/Text
   Size        : 525707
   License     : GPLv3+
   Signature   : RSA/SHA256, Tue 09 May 2023 02:53:25 PM UTC, Key ID
      5259d0b0f6529a4e
   Source RPM  : m4-1.4.16-10.el7.src.rpm
   Build Date  : Fri 20 Nov 2015 07:28:07 AM UTC
   Build Host  : worker1.bsys.centos.org
   Relocations : (not relocatable)
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
Packager    : CentOS BuildSystem <http://bugs.centos.org>
Vendor      : CentOS
URL         : http://www.gnu.org/software/m4/
Summary     : The GNU macro processor
Description :
A GNU implementation of the traditional UNIX macro processor.  M4 is
useful for writing text files which can be logically parsed, and is used
by many programs as part of their build process.  M4 has built-in
functions for including files, running shell commands, doing arithmetic,
etc.  The autoconf program needs m4 for generating configure scripts, but
not for running configure scripts.
<!--NeedCopy-->
```

Obtenga más información

En la mayoría de los casos, se instala más información sobre cada componente y el texto completo de la licencia en `/usr/share/doc/` o en `/usr/share/licenses`.

Por ejemplo, puede encontrar más información sobre el componente `jemalloc-3.6.0` ejecutando el siguiente comando:

```
ls -l /usr/share/doc/jemalloc-3.6.0/

total 120
-rw-r--r--. 1 root root   1703 Mar 31  2014 COPYING
-rw-r--r--. 1 root root 109739 Mar 31  2014 jemalloc.html
-rw-r--r--. 1 root root   1084 Mar 31  2014 README
-rw-r--r--. 1 root root     50 Mar 31  2014 VERSION
```

Sin embargo, para algunos componentes distribuidos por CentOS, el texto de la licencia no está instalado en el producto XenServer. Para ver el texto de licencia de estos componentes, puede mirar dentro de los RPM de origen. Hacemos que los RPM de origen del host de XenServer estén disponibles en las siguientes ubicaciones:

- Para la versión inicial del producto, los archivos fuente se proporcionan en la página de descargas de XenServer.
- Para cualquier actualización o parche rápido de la versión inicial, los archivos fuente actualizados se proporcionan en el artículo correspondiente en el sitio de soporte de Citrix.

El nombre del archivo de origen para un componente específico viene dado por el valor de "RPM de origen"en la salida de información detallada. Por ejemplo:

```
Source RPM : m4-1.4.16-10.el7.src.rpm
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Licencias múltiples

Algunos componentes del producto XenServer contienen varias licencias. Por ejemplo, `procps-ng-3.3.10`contiene las siguientes partes:

- algunas piezas que tienen licencia con la GPL original (o cualquier versión posterior)
- algunas piezas que tienen licencia de la GPL versión 2 (únicamente)
- algunas partes que tienen licencia de la GPL versión 2 (o cualquier versión posterior)
- algunas partes que tienen licencia de la GPL versión 3 (o cualquier versión posterior)
- algunas piezas que tienen licencia con la versión 2 de la LGPL (o cualquier versión posterior)

En este caso, inspeccione la documentación de `/usr/share/doc/procps-ng-3.3.10` para obtener más información o, si es necesario, el RPM de origen correspondiente.

Otros componentes de XenServer

Paquetes suplementarios

Los paquetes complementarios se instalan en el host de XenServer. Si tiene paquetes adicionales instalados en su host, la información sobre sus RPM se incluye al completar los pasos de la sección anterior de este artículo.

Los archivos fuente de los paquetes complementarios también se proporcionan en la página de descargas de XenServer.

XenCenter

Para ver información sobre los componentes de terceros incluidos en XenCenter, lleve a cabo los siguientes pasos:

1. En XenCenter, vaya a **Ayuda > Acerca de XenCenter**.
2. Haga clic en **Ver avisos legales**.

Herramientas de máquinas virtuales de XenServer para Windows

Las herramientas de máquinas virtuales de XenServer para Windows incluyen los siguientes componentes:

- El agente de administración, que está cubierto por una licencia propietaria.
- Los controladores de E/S de Windows, que están cubiertos por la licencia BSD2. Derechos de autor: Cloud Software Group, Inc.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La información de licencia se incluye en el archivo INF de cada controlador. Cuando Windows Update o el instalador del agente de administración instalan los controladores en el sistema Windows, los archivos INF se almacenan como archivos `C:\Windows\INF\OEM*.inf`. El instalador del agente de administración también coloca los archivos INF en `C:\Program Files\XenServer\XenTools\Drivers\***.inf`.

No se proporciona el código fuente para XenServer VM Tools para Windows.

Herramientas de máquinas virtuales de XenServer para Linux

Las herramientas de máquinas virtuales de XenServer para Linux están cubiertas por la licencia BSD2. Derechos de autor: Cloud Software Group, Inc.

El archivo comprimido que se proporciona en la página de descarga del producto contiene el archivo de licencia y los archivos de origen de las herramientas.

Dispositivos virtuales

Los siguientes dispositivos virtuales se proporcionan como componentes opcionales para su entorno XenServer:

- Dispositivo virtual XenServer Conversion Manager
- Dispositivo virtual de equilibrio de carga de

Estos dispositivos virtuales también se basan en CentOS. Puede usar los mismos comandos que se proporcionan para el host de XenServer para obtener información general e información detallada sobre los paquetes de código abierto incluidos en los dispositivos virtuales.

En la consola del dispositivo virtual, ejecute los siguientes comandos:

- Para obtener información general: `rpm -qa --qf '%{ name } -%{ version } : %{ license } \n'`
- Para obtener información detallada: `rpm -qai | sed '/^Name /i\\n'`

Además, el dispositivo virtual XenServer Conversion Manager y el dispositivo virtual Workload Balancing utilizan de forma dinámica algunos componentes de terceros.

- Para el dispositivo virtual XenServer Conversion Manager, los archivos de licencia de estos componentes se encuentran en la siguiente ruta `/opt/vpxxcm/conversion`:.
- Para el dispositivo virtual Equilibrio de carga de trabajo, los archivos de licencia de estos componentes se encuentran en la siguiente ruta: `/opt/vpx/wlb`.

Los archivos fuente de los dispositivos virtuales se proporcionan en la página de descargas de XenServer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Reglamentación de datos

April 10, 2024

En este artículo se proporciona información sobre la recopilación, el almacenamiento y la retención de registros por parte de XenServer.

XenServer es una plataforma de virtualización de servidores que permite al cliente crear y administrar una implementación de máquinas virtuales. XenCenter es la interfaz de usuario de administración de XenServer. XenServer y XenCenter pueden recopilar y almacenar datos de clientes como parte de las siguientes funciones:

- **Telemetría** : la funcionalidad de telemetría transmite información básica de licencias sobre un grupo de XenServer. XenServer recopila estos datos básicos de licencias según sea necesario para sus intereses legítimos, incluido el cumplimiento de las licencias.
- **Informes**de estado del servidor : se puede generar un informe de estado del servidor a petición y cargarlo en Citrix Insight Services o proporcionarlo al servicio de asistencia. El informe de estado del servidor contiene información que puede ayudar a diagnosticar problemas en su entorno.
- **Actualizaciones automáticas para el agente de administración: el agente** de administración se ejecuta en máquinas virtuales alojadas en un host o grupo de XenServer. Si el servidor o el grupo tienen licencia, el agente de administración puede buscar y aplicar actualizaciones a sí mismo y a los controladores de E/S de la máquina virtual. Como parte de la búsqueda de actualizaciones, la función de actualización automática realiza una solicitud web a Cloud Software Group que puede identificar la máquina virtual en la que se ejecuta el agente de administración.
- **Comprobar si hay actualizaciones en XenCenter** : esta función determina si hay revisiones, actualizaciones acumulativas o nuevas versiones disponibles para los hosts y grupos de XenServer que administra XenCenter. Como parte de la búsqueda de actualizaciones, esta función realiza una solicitud web a Citrix que incluye telemetría. Esta telemetría no es específica del usuario y se usa para estimar el número total de instancias de XenCenter en todo el mundo.
- **Alertas por correo electrónico de XenCenter**: XenCenter se puede configurar para enviar notificaciones por correo electrónico cuando se superen los umbrales de alertas. Para enviar estas alertas por correo electrónico, XenCenter recopila y almacena la dirección de correo electrónico de destino.

La información de telemetría recibida por Cloud Software Group se trata de acuerdo con nuestros acuerdos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Telemetría

La funcionalidad de telemetría de XenServer recopila información básica sobre las licencias de los grupos de XenServer.

Cuando instala XenServer, el coordinador de su grupo recopila datos de telemetría y los carga semanalmente en un entorno de nube de Microsoft Azure ubicado en los Estados Unidos. Estos datos no identifican a personas ni clientes y se envían de forma segura a través de HTTPS en el puerto 443 a `https://telemetry.ops.xenserver.com/`. No se recopila ni transmite ninguna información que no sea la de los cuatro elementos identificados a continuación.

El acceso a estos datos está restringido a los miembros de los equipos de operaciones y administración de productos de XenServer.

La información de telemetría recibida por Cloud Software Group se trata de acuerdo con nuestros acuerdos.

Telemetría recopilada

Para cada grupo de XenServer, el coordinador del grupo recopila los siguientes datos:

Datos recopilados	Descripción
UUID	Un identificador único aleatorio para los datos de telemetría de este grupo. Este UUID no es el mismo que el UUID del grupo ni ningún otro identificador existente. No se recopila en los informes de estado del servidor.
Versión del producto	La versión de XenServer instalada en este grupo.
Enchufes (por host)	El número de sockets que tiene este host.
Edición (por anfitrión)	El tipo de licencia de este host.

Estos datos no identifican a las personas ni a los clientes y no contienen información de identificación personal.

Visualización de los datos de telemetría

Los datos que envía XenServer se registran en el coordinador del grupo. `/var/telemetry/telemetry.data` Este archivo no se recopila en los registros de estado del servidor.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Informes de estado del servidor

Durante el transcurso de la operación, un host de XenServer recopila y registra información diversa en el servidor en el que está instalado XenServer. Estos registros se pueden recopilar como parte de un informe de estado del servidor.

Se puede generar un informe de estado del servidor bajo demanda. Puede cargar estos informes en Citrix Insight Services o proporcionarlos a Support. El informe de estado del servidor contiene información que puede ayudar a diagnosticar problemas en su entorno.

Los informes de estado del servidor que se cargan en Citrix Insight Services se almacenan en entornos de Amazon S3 ubicados en los Estados Unidos.

XenServer y XenCenter recopilan información de las siguientes fuentes de datos:

- XenCenter
- Hosts y grupos de XenServer
- VM alojadas

Puede seleccionar qué elementos de datos se incluyen en los informes de estado del servidor. También puede eliminar cualquier informe de estado del servidor que esté cargado en su cuenta de MyCitrix en Citrix Insight Services.

Citrix Insight Services no implementa una retención automática de datos para los informes de estado del servidor cargados por el cliente. El cliente determina la directiva de retención de datos. Puede optar por eliminar cualquier informe de estado del servidor que esté cargado en su cuenta de MyCitrix en Citrix Insight Services.

Datos recopilados

Un informe de estado del servidor puede contener los siguientes archivos de registro:

Tipo de registro	¿Contiene PII?
`device-model`	sí
`fcoe`	sí
`firstboot`	sí
`network-status`	sí
`process-list`	sí
`xapi`	sí
`xenserver-databases`	sí

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Tipo de registro	¿Contiene PII?
control-slice	quizás
disk-info	quizás
hardware-info	quizás
high-availability	quizás
host-crashdump-logs	quizás
kernel-info	quizás
loopback-devices	quizás
message-**switch**	quizás
multipath	quizás
system-logs	quizás
v6d	quizás
xapi-clusterd	quizás
xapi-debug	quizás
xcp-rrdd-plugins	quizás
xen-info	quizás
xenopsd	quizás
xenserver-config	quizás
xenserver-install	quizás
xenserver-logs	quizás
xha-liveset	quizás
yum	si se personaliza
network-config	si se personaliza
cron	si se personaliza
blobs	no
block-scheduler	no
boot-loader	no
conntest	no
CVSM	no
pam	no

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Tipo de registro	¿Contiene PII?
system-services	no
tapdisk-logs	no
VM-snapshot-schedule	no
xapi-subprocess	no
xen-bugtool	no
xenserver-domains	no

Actualizaciones automáticas de Management Agent

El agente de administración se ejecuta en máquinas virtuales alojadas en un host o grupo de XenServer. Si el host o el grupo tienen licencia, el agente de administración puede comprobar si hay actualizaciones y aplicarlas a sí mismo y a los controladores de E/S de la máquina virtual. Como parte de la búsqueda de actualizaciones, la función de actualización automática nos envía una solicitud web que puede identificar la máquina virtual en la que se ejecuta el agente de administración.

Los registros web capturados de las solicitudes realizadas por la función de actualizaciones automáticas del agente de administración se encuentran en un entorno de nube de Microsoft Azure ubicado en los Estados Unidos. Estos registros se copian en un servidor de administración de registros en el Reino Unido.

Las solicitudes web realizadas por la función de actualizaciones automáticas del agente de administración se realizan a través de HTTPS. Los archivos de registro web se transmiten de forma segura al servidor de administración de registros.

Puede seleccionar si su VM usa la función de actualización automática del agente de administración. Si elige usar la función de actualización automática del agente de administración, también puede elegir si la solicitud web incluye la información de identificación de la máquina virtual.

Los registros web que contienen información de las solicitudes web realizadas por la función de actualizaciones automáticas del agente de administración y la función de comprobación de actualizaciones de XenCenter se pueden conservar indefinidamente.

Datos recopilados

Las solicitudes web de actualizaciones automáticas de Management Agent pueden contener los siguientes puntos de datos:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datos recopilados	Descripción	Para qué se utiliza
Dirección IP	La dirección IP de la máquina virtual donde está instalado el agente de administración	
UUID parcial de máquina virtual	Los primeros cuatro caracteres del identificador de usuario único de la máquina virtual en la que está instalado el agente de administración	

Búsqueda de actualizaciones en XenCenter

Esta función determina si hay revisiones, actualizaciones acumulativas o nuevas versiones disponibles para los hosts y grupos de XenServer que administra XenCenter. Como parte de la búsqueda de actualizaciones, esta función realiza una solicitud web a Cloud Software Group que incluye telemetría. Esta telemetría no identifica personalmente a los usuarios y se usa para estimar el número total de instancias de XenCenter en todo el mundo.

Los registros web capturados a partir de las solicitudes realizadas por la función de comprobación de actualizaciones de XenCenter se encuentran en un entorno de nube de Microsoft Azure ubicado en los Estados Unidos. Estos registros se copian en un servidor de administración de registros en el Reino Unido.

Las solicitudes web realizadas por la función de comprobación de actualizaciones de XenCenter se realizan a través de HTTPS. Los archivos de registro web se transmiten de forma segura al servidor de administración de registros.

La función Buscar actualizaciones de XenCenter está habilitada de forma predeterminada. Puede optar por desactivar esta función.

Datos recopilados

Las solicitudes web de la función de búsqueda de actualizaciones contienen los siguientes puntos de datos:

Datos recopilados	Descripción	Para qué se utiliza
Dirección IP	La dirección IP del equipo host de XenCenter	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datos recopilados	Descripción	Para qué se utiliza
Versión de XenCenter	La versión de XenCenter que realiza la solicitud	

Alertas por correo de XenCenter

XenCenter se puede configurar para enviar notificaciones por correo electrónico cuando se superen los umbrales de alerta. Para enviar estas alertas por correo electrónico, XenCenter recopila y almacena la dirección de correo electrónico de destino.

La dirección de correo electrónico que XenCenter usa para enviar alertas por correo electrónico se almacena en la máquina donde instaló XenCenter.

Puede eliminar las alertas de correo electrónico configuradas en XenCenter para eliminar la información de correo electrónico almacenada.

XenCenter conserva la información de correo electrónico que se utiliza para proporcionar alertas por correo electrónico durante la vigencia de la notificación por correo electrónico. Al eliminar la alerta de correo electrónico configurada, se eliminan los datos.

Datos recopilados

Para proporcionar alertas por correo electrónico, XenCenter almacena los siguientes puntos de datos:

Datos recopilados	Descripción	Para qué se utiliza
Dirección de correo electrónico	La dirección de correo electrónico para las alertas	Para enviar correos electrónicos de alertas y notificaciones a
Servidor SMTP	El servidor SMTP que se va a utilizar	Para enviar las alertas por correo electrónico al destinatario

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).