

Guía de configuración segura

3 de mayo de 2018
vRealize Automation 7.4



vmware®

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

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

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

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

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.: + 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Copyright © 2015–2018 VMware, Inc. Todos los derechos reservados. [Copyright e información de marca registrada.](#)

Contenido

- 1 Configuración segura 5**
- 2 Descripción general de la línea de base segura de vRealize Automation 6**
- 3 Comprobar la integridad de los medios de instalación 8**
- 4 Proteger la infraestructura de software del sistema de VMware 9**
 - Proteger el entorno de VMware vSphere® 9
 - Proteger el host de infraestructura como servicio 9
 - Proteger Microsoft SQL Server 10
 - Proteger Microsoft .NET 10
 - Proteger Microsoft Internet Information Services (IIS) 10
- 5 Revisar el software instalado 12**
- 6 Avisos de seguridad y revisiones de VMware 13**
- 7 Configuración segura 14**
 - Proteger el dispositivo de vRealize Automation 14
 - Cambiar la contraseña raíz 14
 - Comprobar la complejidad y el hash de la contraseña raíz 15
 - Comprobar historial de contraseñas raíz 16
 - Administrar la caducidad de las contraseñas 16
 - Administrar Secure Shell y cuentas administrativas 17
 - Cambiar el usuario de la interfaz de administración de dispositivos virtuales 22
 - Configurar la autenticación del cargador de arranque 23
 - Configurar NTP 23
 - Configurar TLS para datos en tránsito del dispositivo de vRealize Automation 24
 - Comprobar la seguridad de datos en reposo 33
 - Configurar recursos de aplicación de vRealize Automation 34
 - Personalizar configuración de proxy de la consola 37
 - Configurar encabezados de respuesta de servidor 39
 - Establecer el tiempo de espera de sesión de Dispositivo de vRealize Automation 40
 - Administrar software no esencial 41
 - Proteger el componente de infraestructura como servicio 45
 - Deshabilitar el servicio Hora de Windows 45
 - Configurar TLS para datos en tránsito de infraestructura como servicio 46
 - Configurar conjuntos de cifrados TLS 48

- Comprobar seguridad del servidor host 48
- Proteger recursos de aplicación 49
- Proteger la máquina host de infraestructura como servicio 50

8 Configurar la seguridad de la red del host 51

- Configurar ajustes de red para dispositivos de VMware 51
 - Evitar el control de usuario de las interfaces de red 51
 - Establecer el tamaño de cola de trabajo pendiente de TCP 52
 - Denegar ecos de ICMPv4 a direcciones de difusión 52
 - Deshabilitar ARP de proxy de IPv4 53
 - Denegar mensajes de redirección de ICMP IPv4 53
 - Denegar mensajes de redirección de ICMP IPv6 54
 - Registrar paquetes de datos con marcadores sospechosos IPv4 55
 - Utilizar el filtrado de rutas inversas IPv4 55
 - Denegar reenvío de IPv4 56
 - Denegar el reenvío de IPv6 57
 - Usar cookies SYN de TCP IPv4 57
 - Denegar anuncios de enrutador IPv6 58
 - Denegar solicitudes de enrutador IPv6 59
 - Denegar la preferencia de enrutador IPv6 en solicitudes de enrutador 60
 - Denegar prefijos de enrutador IPv6 60
 - Denegar opciones de límite de saltos de anuncio de enrutador IPv6 61
 - Denegar opciones de configuración automática de anuncios de enrutador IPv6 62
 - Denegar solicitudes de vecino de IPv6 63
 - Restringir la cantidad máxima de direcciones IPv6 63
- Configurar ajustes de red para el host de infraestructura como servicio 64
- Configurar puertos y protocolos 64
 - Puertos de usuario necesarios 65
 - Puertos de administrador necesarios 65

9 Auditoría y registro 68

Configuración segura

Configuración segura permite a los usuarios evaluar y optimizar la configuración segura de las implementaciones de vRealize Automation.

Configuración segura describe la verificación y la configuración de implementaciones seguras de entornos de vRealize Automation típicos. Además, proporciona información y procedimientos para ayudar a los usuarios a tomar decisiones informadas sobre la configuración de seguridad.

Público objetivo

Esta información está destinada a los administradores del sistema de vRealize Automation y otros usuarios que son responsables de la configuración y el mantenimiento de la seguridad del sistema.

Glosario de publicaciones técnicas de VMware

El departamento de Publicaciones técnicas de VMware ofrece un glosario con términos que quizá usted desconozca. Para consultar las definiciones de términos tal como se utilizan en la documentación técnica de VMware, visite <http://www.vmware.com/es/support/pubs>.

Descripción general de la línea de base segura de vRealize Automation

2

VMware proporciona recomendaciones integrales para permitirle comprobar y configurar una línea de base segura para el sistema de vRealize Automation.

Utilice las herramientas y los procedimientos adecuados, según lo especifica VMware, para comprobar y mantener una configuración de línea de base segura y protegida para el sistema de vRealize Automation. Algunos componentes de vRealize Automation están instalados en un estado protegido o parcialmente protegido, pero debería verificar la configuración de cada componente en función de las recomendaciones de seguridad de VMware, las políticas de seguridad de la empresa y las amenazas conocidas.

Posición de seguridad de vRealize Automation

La posición de seguridad de vRealize Automation supone un entorno seguro en general, con base en la configuración del sistema y la red, las políticas de seguridad de la organización y los procedimientos recomendados de seguridad.

Al comprobar y configurar la protección de un sistema de vRealize Automation, tenga en cuenta cada una de las siguientes áreas de acuerdo con las recomendaciones de protección de VMware.

- Implementación segura
- Configuración segura
- Seguridad de red

Para asegurarse de que su sistema está realmente protegido, tenga en cuenta las recomendaciones de VMware y las políticas de seguridad locales que se relacionan con cada una de estas áreas conceptuales.

Componentes del sistema

Al pensar en la protección y en la configuración segura del sistema de vRealize Automation, asegúrese de que conoce todos los componentes y comprende cómo funcionan juntos para respaldar la funcionalidad del sistema.

Tenga en cuenta los siguientes componentes al planificar e implementar un sistema seguro.

- Dispositivo de vRealize Automation

- Componente de IaaS

Para familiarizarse con vRealize Automation y saber cómo se complementan los componentes, consulte *Fundamentos y conceptos* en el centro de documentación de vRealize Automation de VMware. Para obtener información sobre las implementaciones y la arquitectura típicas de vRealize Automation, consulte *Arquitectura de referencia*.

Comprobar la integridad de los medios de instalación

3

Los usuarios siempre deben comprobar la integridad de los medios de instalación antes de instalar un producto de VMware.

Revise siempre el hash SHA1 después de descargar una ISO, un paquete sin conexión o una revisión para garantizar la integridad y la autenticidad de los archivos descargados. Si obtiene los soportes físicos de VMware y el sello de seguridad está roto, devuelva el software a VMware para su reemplazo.

Después de descargar los medios, utilice el valor de suma MD5/SHA1 para comprobar la integridad de la descarga. Compare la salida del hash MD5/SHA1 con el valor publicado en el sitio web de VMware. El hash SHA1 o MD5 debe coincidir.

Para obtener más información acerca de cómo comprobar la integridad de los medios de instalación, consulte <http://kb.vmware.com/kb/1537>.

Proteger la infraestructura de software del sistema de VMware

4

Como parte del proceso de protección, evalúe la infraestructura de software implementada que admite el sistema de VMware y compruebe que cumpla con las directrices de protección de VMware.

Antes de proteger el sistema de VMware, revise y solucione las deficiencias de seguridad en la infraestructura del software de apoyo para crear un entorno totalmente protegido. Los elementos de la infraestructura de software que se deben considerar incluyen componentes del sistema operativo, software de apoyo y software de base de datos. Solucione los problemas de seguridad en estos y en otros componentes de acuerdo con las recomendaciones del fabricante y otros protocolos de seguridad pertinentes.

Este capítulo cubre los siguientes temas:

- [Proteger el entorno de VMware vSphere®](#)
- [Proteger el host de infraestructura como servicio](#)
- [Proteger Microsoft SQL Server](#)
- [Proteger Microsoft .NET](#)
- [Proteger Microsoft Internet Information Services \(IIS\)](#)

Proteger el entorno de VMware vSphere®

Evalúe el entorno de VMware vSphere® y compruebe que se aplique y se mantenga el nivel apropiado de instrucciones de protección de vSphere.

Para obtener más instrucciones relacionadas con la protección, consulte <http://www.vmware.com/security/hardening-guides.html>.

Como parte de un entorno totalmente protegido, la infraestructura de VMware vSphere® debe cumplir con las directrices de seguridad que VMware define.

Proteger el host de infraestructura como servicio

Compruebe que la máquina host de Microsoft Windows de infraestructura como servicio esté protegida según las directrices de VMware.

Revise las recomendaciones establecidas en las directrices apropiadas de procedimientos recomendados seguros y de protección de Microsoft Windows, y asegúrese de que el host de Windows Server esté protegido correctamente. Si no se siguen las recomendaciones de protección, puede quedar expuesto a vulnerabilidades de seguridad conocidas de los componentes inseguros de las versiones de Windows.

Para comprobar que la versión es compatible, consulte la [matriz de soporte de vRealize Automation](#).

Pregunte a su proveedor de Microsoft acerca de las directrices correctas de los procedimientos de protección de los productos de Microsoft.

Proteger Microsoft SQL Server

Compruebe que la base de datos de Microsoft SQL Server cumpla con las directrices de seguridad establecidas por Microsoft y VMware.

Revise las recomendaciones establecidas en las directrices apropiadas de procedimientos recomendados seguros y de protección de Microsoft SQL Server. Revise todos los boletines de seguridad de Microsoft con respecto a la versión instalada de Microsoft SQL Server. Si no sigue las recomendaciones de protección, puede quedar expuesto a vulnerabilidades de seguridad conocidas de los componentes inseguros de las versiones de Microsoft SQL Server.

Para comprobar que se admite la versión de Microsoft SQL Server, consulte la [matriz de soporte de vRealize Automation](#).

Póngase en contacto con el proveedor de Microsoft para obtener consejos sobre la prácticas de protección de los productos de Microsoft.

Proteger Microsoft .NET

Como parte de un entorno totalmente protegido, Microsoft .NET debe cumplir con las directrices de seguridad establecidas por Microsoft y VMware.

Revise las recomendaciones establecidas en las directrices apropiadas de procedimientos recomendados seguros y de protección de .NET. Además, revise todos los boletines de seguridad de Microsoft sobre la versión de Microsoft SQL Server que está utilizando. Si no se siguen las recomendaciones de protección, puede quedar expuesto a vulnerabilidades de seguridad conocidas de los componentes inseguros de Microsoft.NET.

Para comprobar que su versión de Microsoft.NET es compatible, consulte la [matriz de soporte de vRealize Automation](#).

Póngase en contacto con su proveedor de Microsoft para obtener consejos sobre las prácticas de protección de los productos de Microsoft.

Proteger Microsoft Internet Information Services (IIS)

Compruebe que Microsoft Internet Information Services (IIS) cumpla con todas las directrices de seguridad de Microsoft y de VMware.

Revise las recomendaciones establecidas en las directrices apropiadas de procedimientos recomendados seguros y de protección de Microsoft IIS. Además, revise todos los boletines de seguridad de Microsoft sobre la versión de IIS que está utilizando. Si no se siguen las recomendaciones de protección, puede quedar expuesto a vulnerabilidades de seguridad conocidas.

Para comprobar que la versión es compatible, consulte la [matriz de soporte de vRealize Automation](#).

Póngase en contacto con su proveedor de Microsoft para obtener consejos sobre las prácticas de protección de los productos de Microsoft.

Revisar el software instalado

Debido a que las vulnerabilidades del software de terceros y del software no utilizado aumentan el riesgo de accesos no autorizados al sistema y de interrupciones de disponibilidad, es importante revisar todo el software instalado en las máquinas host de VMware y evaluar su uso.

No instale ningún software que no sea necesario para el funcionamiento seguro del sistema en las máquinas host de VMware. Desinstale el software irrelevante o que no se utiliza.

Realizar un inventario del software instalado no compatible

Evalúe la implementación de VMware y realice un inventario de los productos instalados para asegurarse de que no se haya instalado ningún software irrelevante y no compatible.

Para obtener más información acerca de las políticas de soporte para productos de terceros, consulte el artículo de soporte de VMware, en <https://www.vmware.com/support/policies/thirdparty.html>.

Comprobar el software de terceros

VMware no admite ni recomienda la instalación de software de terceros que no se haya probado y verificado. El software de terceros no seguro, no revisado o sin autenticar que se instale en las máquinas host de VMware puede causar accesos no autorizados e interrupción de la disponibilidad. Si debe usar software de terceros no compatible, pida al proveedor externo la configuración segura y los requisitos de revisiones.

Avisos de seguridad y revisiones de VMware

6

Para mantener la máxima seguridad en el sistema, siga los avisos de seguridad de VMware y aplique todas las revisiones correspondientes.

VMware publica avisos de seguridad relacionados con los productos. Supervise estos avisos para asegurarse de que su producto está protegido contra las amenazas conocidas.

Evalúe la instalación, las revisiones y el historial de actualizaciones de vRealize Automation, y compruebe que los avisos de seguridad de VMware publicados se sigan y se apliquen.

Para obtener más información sobre los avisos de seguridad de VMware actuales, consulte <http://www.vmware.com/security/advisories/>.

Configuración segura

Compruebe y actualice la configuración de seguridad de los dispositivos virtuales de vRealize Automation y del componente de infraestructura como servicio según corresponda para la configuración del sistema. Asimismo, compruebe y actualice la configuración de otros componentes y aplicaciones.

La configuración segura de una instalación de vRealize Automation implica abordar la configuración de cada componente de forma individual y cuando están trabajando juntos. Considere la configuración de los componentes de todos los sistemas en conjunto para lograr una línea de base razonablemente segura.

Este capítulo cubre los siguientes temas:

- [Proteger el dispositivo de vRealize Automation](#)
- [Proteger el componente de infraestructura como servicio](#)

Proteger el dispositivo de vRealize Automation

Compruebe y actualice la configuración de seguridad del dispositivo de vRealize Automation como corresponda para la configuración del sistema.

Configure los ajustes de seguridad para los dispositivos virtuales y sus sistemas operativos host. Además, establezca o compruebe la configuración de aplicaciones y componentes relacionados adicionales. En algunos casos, debe comprobar la configuración existente, mientras que en otros casos debe cambiar o agregar valores para realizar la configuración de forma adecuada.

Cambiar la contraseña raíz

Puede cambiar la contraseña raíz para que Dispositivo de vRealize Automation cumpla con los requisitos de seguridad correspondientes.

Cambie la contraseña raíz en el Dispositivo de vRealize Automation mediante la interfaz de administración de dispositivos virtuales. Compruebe que la contraseña raíz cumpla con los requisitos de complejidad de contraseña corporativa de la organización.

Procedimiento

- 1 Abra la interfaz de administración de dispositivos virtuales de Dispositivo de vRealize Automation.
<https://vRealizeAppliance-ur1:5480>

- 2 Seleccione la pestaña **Administración** en la interfaz de administración de dispositivos virtuales.
- 3 Seleccione el submenú **Administración**.
- 4 Introduzca la contraseña existente en el cuadro de texto **Contraseña de administrador actual**.
- 5 Introduzca la nueva contraseña en el cuadro de texto **Contraseña de administrador nueva**.
- 6 Introduzca la nueva contraseña en el cuadro de texto **Volver a escribir la nueva contraseña de administrador**.
- 7 Haga clic en **Guardar configuración** para guardar los cambios.

Comprobar la complejidad y el hash de la contraseña raíz

Compruebe que la contraseña raíz cumpla con los requisitos de complejidad de contraseña corporativa de la organización.

Es necesario validar la complejidad de la contraseña raíz debido a que el usuario raíz sorte la comprobación de complejidad de la contraseña del módulo pam_cracklib que se aplica a las cuentas de usuario.

La contraseña de la cuenta debe comenzar con \$6\$, lo que indica un hash sha512. Este es el hash estándar para todos los dispositivos protegidos.

Procedimiento

- 1 Para comprobar el hash de la contraseña raíz, inicie sesión como usuario raíz y ejecute el comando `# more /etc/shadow`.

Se muestra la información del hash.

Figura 7-1. Resultados del hash de la contraseña

```
vcac148-084-111:~ # more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870:0:60:7:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870:0:60:7:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KzK4SS44UEHPfAtgs
P/:16346:0:365:7:::
```

- 2 Si la contraseña raíz no contiene un hash sha512, ejecute el comando `passwd` para cambiarla.

Todos los dispositivos protegidos habilitan `enforce_for_root` en el módulo `pw_history`, que se encuentra en el archivo `etc/pam.d/common-password`. El sistema recuerda las últimas cinco contraseñas de forma predeterminada. Las contraseñas antiguas de cada usuario se almacenan en el archivo `/etc/securetty/passwd`.

Comprobar historial de contraseñas raíz

Compruebe que el historial de contraseñas se aplique a la cuenta raíz.

Todos los dispositivos protegidos habilitan `enforce_for_root` en el módulo `pw_history`, que se encuentra en el archivo `etc/pam.d/common-password`. El sistema recuerda las últimas cinco contraseñas de forma predeterminada. Las contraseñas antiguas de cada usuario se almacenan en el archivo `/etc/securetty/passwd`.

Procedimiento

- 1 Ejecute el siguiente comando:

```
cat /etc/pam.d/common-password-vmware.local | grep pam_pwhistory.so
```

- 2 Asegúrese de que `enforce_for_root` aparezca en los resultados devueltos.

```
password required pam_pwhistory.so enforce_for_root remember=5 retry=3
```

Administrar la caducidad de las contraseñas

Configure la caducidad de todas las contraseñas de cuenta en conformidad con las políticas de seguridad de la organización.

De forma predeterminada, todas las cuentas del dispositivo virtual protegido de VMware definen la caducidad de contraseña en 60 días. En la mayoría de los dispositivos protegidos, la caducidad de la contraseña de la cuenta raíz es de 365 días. Se recomienda comprobar que la fecha de caducidad de todas las cuentas cumpla con los estándares de requisitos de seguridad y funcionamiento.

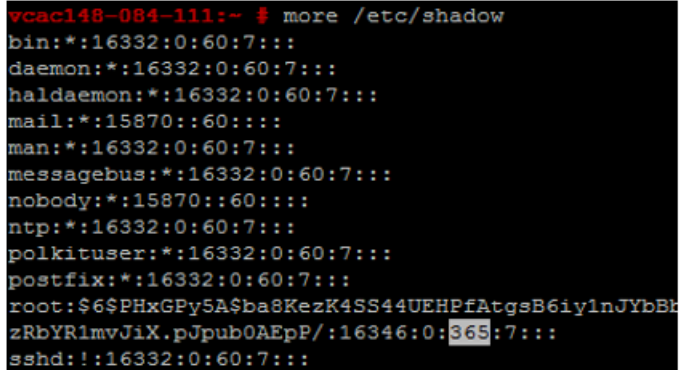
Si la contraseña raíz caduca, no podrá reactivarla. Debe implementar políticas específicas de sitio para evitar que las contraseñas administrativas y de usuario raíz caduquen.

Procedimiento

- 1 Inicie sesión en las máquinas del dispositivo virtual como usuario raíz y ejecute el siguiente comando para comprobar la caducidad de contraseña en todas las cuentas.

```
# cat /etc/shadow
```

La caducidad de contraseña es el quinto campo del archivo de sombra (los campos están separados por dos puntos). La caducidad de la raíz se establece en días.

Figura 7-2. Campo de caducidad de contraseña


```
vcac148-084-111:~ # more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPy5A$ba8KzK4SS44UEHPfAtgsB6iy1nJYbBk
zRbYR1mvJiX.pJpub0AEpP/:16346:0:365:7:::
sshd:!:16332:0:60:7:::
```

- 2 Para modificar la caducidad de la cuenta raíz, ejecute un comando con el siguiente formato.

```
# passwd -x 365 root
```

En este comando, 365 especifica el número de días que deben transcurrir antes de que caduque la contraseña. Puede utilizar el mismo comando para modificar cualquier usuario. Tan solo debe sustituir "root" por la cuenta específica y reemplazar el número de días para cumplir con los estándares de caducidad de la organización.

Administrar Secure Shell y cuentas administrativas

Para las conexiones remotas, todos los dispositivos protegidos incluyen el protocolo Secure Shell (SSH). Utilice SSH solo cuando sea necesario y adminístrelo correctamente para mantener la seguridad del sistema.

SSH es un entorno de línea de comandos interactivo que admite conexiones remotas con los dispositivos virtuales de VMware. De forma predeterminada, el acceso a SSH requiere credenciales de cuenta de usuario con privilegios elevados. Por lo general, las actividades de SSH del usuario raíz sortean el control de acceso basado en funciones (role-based access control, RBAC) y los controles de auditoría de los dispositivos virtuales.

Se recomienda deshabilitar SSH en un entorno de producción y habilitarlo solo para solucionar los problemas que no se puedan resolver por otros medios. Manténgalo habilitado solo mientras sea necesario para un propósito específico y en conformidad con las políticas de seguridad de la organización. En el dispositivo de vRealize Automation, SSH está deshabilitado de forma predeterminada. En función de la configuración de vSphere, puede habilitar o deshabilitar SSH al implementar la plantilla de Open Virtualization Format (OVF).

Para determinar de manera sencilla si SSH está habilitado en una máquina, intente abrir una conexión mediante SSH. Si la conexión se abre y se solicitan credenciales, SSH está habilitado y disponible para las conexiones.

Cuenta de usuario raíz de Secure Shell

Debido a que los dispositivos de VMware no incluyen cuentas de usuario preconfiguradas, la cuenta raíz puede usar SSH para iniciar sesión directamente de forma predeterminada. Deshabilite SSH como usuario raíz tan pronto como sea posible.

Para cumplir con los estándares de cumplimiento de manera que no haya rechazo, el servidor SSH de todos los dispositivos protegidos está preconfigurado con la entrada de wheel AllowGroups para restringir el acceso SSH al wheel del grupo secundario. Para separar las obligaciones, puede modificar la entrada de wheel AllowGroups en el archivo `/etc/ssh/sshd_config` para usar otro grupo, como `sshd`.

El grupo wheel está habilitado con el módulo `pam_wheel` para acceso de superusuarios, de modo que los miembros de grupo wheel puedan usar el comando `su-root`, en el que se requiere la contraseña raíz. La separación de grupos permite a los usuarios utilizar SSH en el dispositivo, pero no el comando `su to root`. Para garantizar el correcto funcionamiento del dispositivo, no quite ni modifique otras entradas del campo AllowGroups. Después de realizar un cambio, debe reiniciar el daemon SSH ejecutando el comando `# service sshd restart`.

Habilitar o deshabilitar Secure Shell en los dispositivos de vRealize Automation

Habilite Secure Shell (SSH) en el dispositivo de vRealize Automation solo para solucionar problemas. Deshabilite SSH en estos componentes durante la operación normal de producción.

Puede habilitar o deshabilitar SSH en el dispositivo de vRealize Automation mediante la consola de administración de dispositivos virtuales.

Procedimiento

- 1 Desplácese hasta la consola de administración de dispositivos virtuales del dispositivo de vRealize Automation.
: `https://vRealizeAppliance url:5480`
- 2 Haga clic en la pestaña **Administración**.
- 3 Haga clic en el submenú **Administración**.
- 4 Active la casilla de verificación **Habilitar servicio SSH** para habilitar SSH o desactívela para deshabilitar SSH.
- 5 Haga clic en **Guardar configuración** para guardar los cambios.

Crear una cuenta de administrador local para Secure Shell

Como procedimiento de seguridad recomendado, cree y configure cuentas administrativas locales de Secure Shell (SSH) en las máquinas host del dispositivo virtual. Además, también se recomienda quitar el acceso SSH raíz después de crear las cuentas apropiadas.

Cree cuentas administrativas locales para SSH o miembros del grupo wheel secundario, o ambos. Antes de deshabilitar el acceso directo a la raíz, compruebe que los administradores autorizados puedan acceder a SSH usando AllowGroups y que puedan recurrir a `su to root` utilizando el grupo wheel.

Procedimiento

- 1 Inicie sesión en el dispositivo virtual como usuario raíz y ejecute los siguientes comandos con el nombre de usuario adecuado.

```
# useradd -g users <username> -G wheel -m -d /home/username
# passwd username
```

Wheel es el grupo especificado en AllowGroups para el acceso a SSH. Para agregar varios grupos secundarios, utilice `-G wheel, sshd`.

- 2 Cambie al usuario y proporcione una contraseña nueva para aplicar la comprobación de complejidad de contraseña.

```
# su -username
# username@hostname:~>passwd
```

Si se cumple con la complejidad de contraseña, la contraseña se actualiza. Si no se cumple con la complejidad de contraseña, se revierte a la contraseña original, y debe volver a ejecutar el comando de contraseña.

- 3 Para quitar el inicio de sesión directo en SSH, modifique el archivo `/etc/ssh/sshd_config` reemplazando `(#)PermitRootLogin yes` por `PermitRootLogin no`.

Opcionalmente, se puede habilitar o deshabilitar SSH en la interfaz de administración de dispositivos virtuales (VAMI) activando o desactivando la casilla de verificación **Inicio de sesión de SSH de administrador habilitado** en la pestaña **Administración**.

Qué hacer a continuación

Deshabilite los inicios de sesión directos como raíz. De forma predeterminada, los dispositivos protegidos permiten realizar el inicio de sesión directo como raíz mediante la consola. Después de crear cuentas administrativas de manera que no haya rechazo y de probarlas para el acceso de wheel de su-root, deshabilite los inicios de sesión raíz directos editando el archivo `/etc/security` como usuario raíz y reemplazando la entrada `tty1` por `console`.

- 1 Abra el archivo `/etc/security` en un editor de texto.
- 2 Busque `tty1` y reemplácelo por `console`.
- 3 Guarde el archivo y ciérrelo.

Restringir el acceso a Secure Shell

Como parte del proceso de protección del sistema, restrinja el acceso a Secure Shell (SSH) configurando correctamente el paquete `tcp_wrappers` en todas las máquinas host del dispositivo virtual de VMware. Mantenga también los permisos de archivo de claves de SSH necesarios en los dispositivos.

Todos los dispositivos virtuales de VMware incluyen el paquete `tcp_wrappers` para que los daemons compatibles con TCP puedan controlar las subredes de red que pueden acceder a los daemons en bibliotecas `libwrap`. De forma predeterminada, el archivo `/etc/hosts.allow` contiene una entrada genérica (`Sshd: ALL : ALLOW`) que permite el acceso total a Secure Shell. Restrinja este acceso según corresponda en su organización.

Procedimiento

- 1 En un editor de texto, abra el archivo `/etc/hosts.allow` en la máquina host del dispositivo virtual.
- 2 Cambie la entrada genérica en el entorno de producción para que incluya solo las entradas de host local y la subred de la red de administración de operaciones seguras.

```
sshd:127.0.0.1 : ALLOW
sshd: [::1] : ALLOW
sshd: 10.0.0.0 :ALLOW
```

En este ejemplo, se permiten todas las conexiones de host local y las conexiones que los clientes establecen en la subred 10.0.0.0.

- 3 Añada todos los datos de identificación de máquina necesarios; por ejemplo, el nombre de host, la dirección IP, el nombre de dominio completo (fully qualified domain name, FQDN) y el bucle invertido.
- 4 Guarde el archivo y ciérrelo.

Proteger la configuración del servidor de Secure Shell

Siempre que sea posible, todos los dispositivos de VMware tienen una configuración de protección predeterminada. Los usuarios pueden comprobar si su configuración está protegida adecuadamente examinando la configuración del servicio del cliente y el servidor en la sección de opciones globales del archivo de configuración.

Si es posible, restrinja el uso del servidor de SSH a una subred de administración en el archivo `/etc/hosts.allow`.

Procedimiento

- 1 Abra el archivo de configuración del servidor `/etc/ssh/sshd_config` en el dispositivo de VMware y compruebe que la configuración sea correcta.

Configuración	Estado
Protocolo de daemon de servidor	Protocol 2
Cifrados de CBC	aes256-ctr y aes128-ctr
Reenvío de TCP	AllowTCPForwarding no
Puertos de puerta de enlace de servidor	Gateway Ports no
Reenvío de X11	X11Forwarding no
Servicio SSH	Utilice el campo <code>AllowGroups</code> y especifique un acceso de grupo permitido. Agregue los miembros adecuados a este grupo.
Autenticación de GSSAPI	GSSAPIAuthentication no, si no se utiliza.

Configuración	Estado
Autenticación Kerberos	KeberosAuthentication no, si no se utiliza.
Variables locales (opción AcceptEnv global)	Establecido como desactivado por conversión a comentario o habilitado para las variables LC_* o LANG.
Configuración de túnel	PermitTunnel no
Sesiones de red	MaxSessions 1
Conexiones simultáneas de usuario	Establecido como 1 para raíz y cualquier otro usuario. El archivo <code>/etc/security/limits.conf</code> también debe configurarse con los mismos ajustes.
Comprobación en modo estricto	Strict Modes yes
Separación de privilegios	UsePrivilegeSeparation yes
Autenticación RSA de rhosts	RhostsESAAuthentication no
Compresión	Compression delayed o Compression no
Código de autenticación de mensaje	MACs hmac-sha1
Restricción de acceso de usuario	PermitUserEnvironment no

- 2 Guarde los cambios y cierre el archivo.

Proteger la configuración del cliente de Secure Shell

Como parte del proceso de protección del sistema, compruebe la protección del cliente de SSH examinando el archivo de configuración del cliente de SSH en las máquinas host del dispositivo virtual para asegurarse de que esté configurado según las directrices de VMware.

Procedimiento

- 1 Abra el archivo de configuración del cliente de SSH, `/etc/ssh/ssh_config`, y compruebe que la configuración en la sección de opciones globales sea correcta.

Configuración	Estado
Protocolo de cliente	Protocol 2
Puertos de puerta de enlace de cliente	Gateway Ports no
Autenticación de GSSAPI	GSSAPIAuthentication no
Variables locales (opción SendEnv global)	Proporcionar solo las variables LC_* o LANG
Cifrados de CBC	Solo aes256-ctr y aes128-ctr
Códigos de autenticación de mensaje	Solo en la entrada MACs hmac-sha1

- 2 Guarde los cambios y cierre el archivo.

Comprobar los permisos de archivo de claves de shell seguro

Para minimizar la posibilidad de ataques malintencionados, mantenga los permisos de archivo de claves SSH críticos en las máquinas host del dispositivo virtual.

Después de ajustar o actualizar la configuración de SSH, asegúrese de comprobar que los siguientes permisos de archivo de claves de SSH no hayan cambiado.

- Los archivos de claves de host público ubicados en `/etc/ssh/*key.pub` son propiedad del usuario raíz y tienen los permisos establecidos en 0644 (`-rw-r--r--`).
- Los archivos de claves de host privado ubicados en `/etc/ssh/*key` son propiedad del usuario raíz y tienen los permisos establecidos en 0600 (`-rw-----`).

Comprobar los permisos de archivo de clave SSH

Compruebe que se aplican permisos de SSH a los archivos de clave tanto pública como privada.

Procedimiento

- 1 Ejecute el siguiente comando para comprobar los archivos de clave pública SSH: `ls -l /etc/ssh/*key.pub`
- 2 Compruebe que el propietario es root, que el propietario del grupo es root y que los archivos tienen los permisos establecidos en 0644 (`-rw-r--r--`).
- 3 Ejecute los siguientes comandos para resolver los problemas que haya.


```
chown root /etc/ssh/*key.pub
chgrp root /etc/ssh/*key.pub
chmod 644 /etc/ssh/*key.pub
```
- 4 Ejecute el siguiente comando para comprobar los archivos de clave privada SSH: `ls -l /etc/ssh/*key`
- 5 Ejecute los siguientes comandos para resolver los problemas que haya.


```
chown root /etc/ssh/*key
chgrp root /etc/ssh/*key
chmod 644 /etc/ssh/*key
```

Cambiar el usuario de la interfaz de administración de dispositivos virtuales

Puede añadir y eliminar usuarios en la interfaz de administración de dispositivos virtuales para lograr el nivel de seguridad adecuado.

La cuenta de usuario raíz de la interfaz de administración de dispositivos virtuales utiliza PAM para la autenticación, por lo que también se usan los niveles de recorte establecidos por PAM. Si la interfaz de administración de dispositivos virtuales no se ha aislado correctamente, podría producirse un bloqueo de la cuenta raíz del sistema en caso de que un atacante trate de iniciar sesión mediante fuerza bruta. Además, cuando la cuenta raíz no sea suficiente para que no haya rechazo a través más de una persona de la organización, habrá que cambiar el usuario administrador de la interfaz de administración.

Prerequisitos

Procedimiento

- 1 Ejecute el siguiente comando para crear un usuario y añadirlo al grupo de interfaz de administración de dispositivos virtuales.

```
useradd -G vami,root usuario
```

- 2 Cree una contraseña para el usuario.

```
passwd usuario
```

- 3 (Opcional) Ejecute el siguiente comando para deshabilitar el acceso raíz en la interfaz de administración de dispositivos virtuales.

```
usermod -R vami root
```

NOTA: Cuando se deshabilita el acceso raíz en la interfaz de administración de dispositivos virtuales, también se deshabilita la posibilidad de actualizar la contraseña del administrador (o raíz) en la pestaña Administración.

Configurar la autenticación del cargador de arranque

Para proporcionar un nivel de seguridad adecuado, configure la autenticación del cargador de arranque en los dispositivos virtuales de VMware.

Si el cargador de arranque del sistema no requiere autenticación, los usuarios con acceso a la consola del sistema pueden modificar la configuración de arranque del sistema o arrancar el sistema en el modo de usuario único o de mantenimiento, lo que puede provocar la denegación de servicio o el acceso no autorizado al sistema. Debido a que la autenticación del cargador de arranque no se establece de forma predeterminada en los dispositivos virtuales de VMware, debe crear una contraseña GRUB para configurarla.

Procedimiento

- 1 Para comprobar si existe una contraseña de arranque, busque la línea `password --md5 <password-hash>` en el archivo `/boot/grub/menu.lst` en los dispositivos virtuales.

- 2 Si no existe ninguna contraseña, ejecute el comando `# /usr/sbin/grub-md5-crypt` en el dispositivo virtual.

Se genera una contraseña MD5 y el comando proporciona la salida del hash md5.

- 3 Añada la contraseña al archivo `menu.lst`; para ello, ejecute el comando `# password --md5 <hash from grub-md5-crypt>`.

Configurar NTP

Para el aprovisionamiento de tiempo crítico, deshabilite la sincronización de hora del host y utilice el protocolo de tiempo de redes (Network Time Protocol, NTP) en el dispositivo de vRealize Automation.

El daemon de NTP en el dispositivo de vRealize Automation proporciona servicios de hora sincronizada. De forma predeterminada, NTP está deshabilitado, por lo que deberá configurarlo manualmente. Si es posible, utilice NTP en entornos de producción para realizar un seguimiento de las acciones del usuario y detectar posibles intrusiones y ataques malintencionados mediante la auditoría y la generación de logs precisas. Para obtener información sobre los avisos de seguridad de NTP, consulte el sitio web de NTP.

El archivo de configuración de NTP se encuentra en la carpeta `/etc/` de cada dispositivo. Puede habilitar el servicio de NTP para el dispositivo de vRealize Automation y añadir servidores horarios en la pestaña **Administración** de la interfaz de administración de dispositivos virtuales.

Procedimiento

- 1 Abra el archivo de configuración `/etc/ntp.conf` en un editor de texto de la máquina host del dispositivo virtual.
- 2 Establezca la propiedad del archivo en **root:root**.
- 3 Establezca los permisos en **0640**.
- 4 Para reducir el riesgo de un ataque de amplificación por denegación de servicio en el servicio NTP, abra el archivo `/etc/ntp.conf` y asegúrese de que las líneas de restricción aparezcan en el archivo.

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

- 5 Guarde los cambios y cierre los archivos.

Configurar TLS para datos en tránsito del dispositivo de vRealize Automation

Asegúrese de que la implementación de vRealize Automation use protocolos TLS seguros para proteger los canales de transmisión de los componentes del dispositivo de vRealize Automation.

Por motivos de rendimiento, no se habilita TLS para las conexiones de localhost entre algunos servicios de aplicación. Cuando una defensa más robusta sea una preocupación, habilite TLS en todas las comunicaciones de localhost.

IMPORTANTE: Al finalizar TLS en el equilibrador de carga, deshabilite protocolos no seguros (como SSLv2, SSLv3 y TLS 1.0) en todos los equilibradores de carga.

Habilitar TLS en la configuración de localhost

De manera predeterminada, algunas comunicaciones de localhost no utilizan TLS. Puede habilitar TLS en todas las conexiones de localhost para proporcionar una mayor seguridad.

Procedimiento

- 1 Conéctese con el Dispositivo de vRealize Automation mediante SSH.
- 2 Defina permisos para el almacén de claves de vCAC mediante la ejecución de los siguientes comandos.

```
usermod -A vco,coredump,pivotal vco
chown vcac.pivotal /etc/vcac/vcac.keystore
chmod 640 /etc/vcac/vcac.keystore
```

- 3 Actualice la configuración de HAProxy.
 - a Abra el archivo de configuración de HAProxy ubicado en `/etc/haproxy/conf.d` y elija el servicio `20-vcac.cfg`.

- b Busque las líneas que contengan la siguiente cadena:

`server local 127.0.0.1...` y añada lo siguiente al final de estas líneas: `ssl verify none`

Esta sección contiene otras líneas como la siguiente:

backend-horizon	backend-vro
backend-vra	backend-artifactory
backend-vra-health	

- c Cambie el puerto de backend-horizon de 8080 a 8443.

- 4 Obtenga la contraseña de keystorePass.

- a Busque la propiedad `certificate.store.password` en el archivo `/etc/vcac/security.properties`.

Por ejemplo, `certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

- b Descifre el valor con el siguiente comando:

`vcac-config prop-util -d --p VALUE`

Por ejemplo, `vcac-config prop-util -d --p s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

- 5 Configure el servicio de vRealize Automation.

- a Abra el archivo `/etc/vcac/server.xml`.
 - b Agregue el siguiente atributo a la etiqueta Connector, reemplazando `certificate.store.password` con el valor de contraseña del almacén de certificados que se encuentra en `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS"
keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache"
keystorePass="certificate.store.password"
```

6 Configure el servicio de vRealize Orchestrator.

- a Abra el archivo `/etc/vco/app-server.xml`.
- b Agregue el siguiente atributo a la etiqueta `Connector`, reemplazando `certificate.store.password` con el valor de contraseña del almacén de certificados que se encuentra en `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS"
keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache"
keystorePass="certificate.store.password"
```

7 Reinicie los servicios de HAProxy, de vRealize Orchestrator y de vRealize Automation.

```
service vcac-server restart
service vco-server restart
service haproxy restart
```

NOTA: Si `vco-server` no se reinicia, reinicie el equipo host.

8 Configure la interfaz de administración de dispositivos virtuales.

- a Abra el archivo `/opt/vmware/share/htdocs/service/café-services/services.py`.
- b Para aumentar la seguridad, cambie la línea `conn = httplib.HTTP()` por `conn = httplib.HTTPS()`.

Habilitar el cumplimiento con el Estándar federal de procesamiento de información (Federal Information Processing Standard, FIPS) 140-2

El dispositivo de vRealize Automation ahora utiliza la versión de OpenSSL certificada por el FIPS 140-2 para los datos en tránsito en TLS en todo el tráfico de red entrante y saliente.

Puede habilitar o deshabilitar el modo FIPS en la interfaz de administración del dispositivo de vRealize Automation. También puede configurar el FIPS desde la línea de comandos después de iniciar sesión como raíz con los siguientes comandos:

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

Si está habilitado, el tráfico de red entrante y saliente del Dispositivo de vRealize Automation en el puerto 443 utiliza el cifrado que cumple con FIPS 140–2. Independientemente de la configuración de FIPS, vRealize Automation utiliza AES–256 para la protección de los datos almacenados en el dispositivo de vRealize Automation.

NOTA: Actualmente, vRealize Automation solo habilita parcialmente el cumplimiento del estándar FIPS porque algunos componentes internos no utilizan todavía módulos criptográficos certificados. En los casos en los que todavía no se hayan implementado módulos certificados, el cifrado basado en AES-256 se utiliza en todos los algoritmos criptográficos.

NOTA: Con el siguiente procedimiento se reiniciará la máquina física cuando la configuración se altere.

Procedimiento

- 1 Inicie sesión como raíz en la interfaz de administración del dispositivo de vRealize Automation.
`https:// vrealize-automation-appliance-FQDN:5480`
- 2 Seleccione **Configuración de vRA > Configuración del host**.
- 3 Para habilitar o deshabilitar FIPS, haga clic en el botón que se encuentra debajo del encabezado Acciones en la parte superior derecha.
- 4 Haga clic en **Sí** para reiniciar el dispositivo de vRealize Automation.

Comprobar que SSLv3, TLS 1.0 y TLS 1.1 estén deshabilitados

Como parte del proceso de protección, asegúrese de que la instancia implementada de Dispositivo de vRealize Automation utiliza canales de transmisión seguros.

Prerequisitos

Complete el procedimiento [Habilitar TLS en la configuración de localhost](#).

Procedimiento

- 1 Compruebe que SSLv3, TLS 1.0 y TLS 1.1 estén deshabilitados en los controladores https de HAProxy en Dispositivo de vRealize Automation.

Revisar este archivo	Asegurarse de que lo siguiente esté presente	Asegurarse de que esté en la línea adecuada tal como se muestra
/etc/haproxy/conf.d/20-vcac.cfg	no-ssl3 no-tls10 no-tls11 force-tls12	bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11
/etc/haproxy/conf.d/30-vro-config.cfg	no-ssl3 no-tls10 no-tls11 force-tls12	bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11

- 2 Reinicie el servicio.

```
service haproxy restart
```

- 3 Abra el archivo /opt/vmware/etc/lighttpd/lighttpd.conf y compruebe que aparezcan las entradas de deshabilitación correctas.

NOTA: No hay ninguna directiva para deshabilitar TLS 1.0 o TLS 1.1 en Lighttpd. La restricción en el uso de TLS 1.0 y TLS 1.1 puede mitigarse parcialmente aplicando OpenSSL para que no utilice los conjuntos de cifrado de TLS 1.0 y TLS 1.1.

```
ssl.use-ssl2 = "disable"
ssl.use-ssl3 = "disable"
```

- 4 Compruebe que SSLv3, TLS 1.0 y TLS 1.1 estén deshabilitados para el proxy de la consola en Dispositivo de vRealize Automation.
 - a Edite el archivo /etc/vcac/security.properties mediante la adición o la modificación de la siguiente línea:

```
consoleproxy.ssl.server.protocols = TLSv1.2
```
 - b Reinicie el servidor ejecutando el siguiente comando:

```
service vcac-server restart
```

5 Compruebe que SSLv3, TLS 1.0 y TLS 1.1 estén deshabilitados para el servicio vCO.

- a Busque la etiqueta <Connector> en el archivo /etc/vco/app-server/server.xml y agregue el siguiente atributo:

```
sslEnabledProtocols = "TLSv1.2"
```

- b Ejecute el siguiente comando para reiniciar el servicio vCO.

```
service vco-server restart
```

6 Compruebe que SSLv3, TLS 1.0 y TLS 1.1 estén deshabilitados para el servicio vRealize Automation.

- a Añada los siguientes atributos a la etiqueta <Connector> en el archivo /etc/vcac/server.xml:

```
sslEnabledProtocols = "TLSv1.2"
```

- b Ejecute el siguiente comando para reiniciar el servicio vRealize Automation:

```
service vcac-server restart
```

7 Compruebe que SSLv3, TLS 1.0 y TLS 1.1 estén deshabilitados para RabbitMQ.

Abra el archivo /etc/rabbitmq/rabbitmq.config y compruebe que {versions, ['tlsv1.2', 'tlsv1.1']} aparezca en las secciones ssl y ssl_options.

```
[
  {ssl, [
    {versions, ['tlsv1.2', 'tlsv1.1']},
    {ciphers, ["AES256-SHA", "AES128-SHA"]}
  ]},
  {rabbit, [
    {tcp_listeners, [{"127.0.0.1", 5672}]},
    {frame_max, 262144},
    {ssl_listeners, [5671]},
    {ssl_options, [
      {cacertfile, "/etc/rabbitmq/certs/ca/cacert.pem"},
      {certfile, "/etc/rabbitmq/certs/server/cert.pem"},
      {keyfile, "/etc/rabbitmq/certs/server/key.pem"},
      {versions, ['tlsv1.2', 'tlsv1.1']},
      {ciphers, ["AES256-SHA", "AES128-SHA"]},
      {verify, verify_peer},
      {fail_if_no_peer_cert, false}
    ]},
    {mnesia_table_loading_timeout, 600000},
    {cluster_partition_handling, autoheal},
    {heartbeat, 600}
  ]},
  {kernel, [{net_ticktime, 120}]}
].
```

8 Reinicie el servidor de RabbitMQ.

```
# service rabbitmq-server restart
```

- 9 Compruebe que SSLv3, TLS 1.0 y TLS 1.1 estén deshabilitados para el servicio vIDM.

Abra el archivo `opt/vmware/horizon/workspace/conf/server.xml` para cada instancia del conector que contenga `SSLEnabled="true"` y asegúrese de que la siguiente línea esté presente.

```
sslEnabledProtocols="TLSv1.2"
```

Configurar conjuntos de cifrados TLS para los componentes de vRealize Automation

Para lograr la máxima seguridad, debe configurar los componentes de vRealize Automation para que utilicen cifrados seguros.

Los cifrados que se negocian entre el servidor y el navegador determinan el nivel de cifrado que se utiliza durante una sesión de TLS.

Para asegurarse de que se seleccionen solo cifrados seguros, deshabilite los cifrados no seguros en los componentes de vRealize Automation. Configure el servidor para que admita solo cifrados seguros y para que utilice tamaños de clave lo suficientemente grandes. Además, configure todos los cifrados en un orden adecuado.

Deshabilite los conjuntos de cifrados que no ofrezcan autenticación, como los conjuntos de cifrados NULL, aNULL o eNULL. Deshabilite también el intercambio de claves Diffie-Hellman anónimo (ADH), los cifrados de nivel de exportación (EXP, cifrados que contienen DES), los tamaños de clave inferiores a 128 bits para el cifrado del tráfico de carga, el uso de MD5 como un mecanismo de hash del tráfico de carga, los conjuntos de cifrados IDEA y los conjuntos de cifrados RC4. Asegúrese también de que el conjunto de cifrados que usa el intercambio de claves Diffie-Hellman (DHE) está deshabilitado.

Deshabilitar cifrados no seguros en HAProxy

Compare los cifrados del servicio HAProxy del dispositivo de vRealize Automation con la lista de cifrados aceptados y deshabilite todos los que no considere seguros.

Deshabilite los conjuntos de cifrados que no ofrezcan autenticación, como los conjuntos de cifrados NULL, aNULL o eNULL. Deshabilite también el intercambio de claves Diffie-Hellman anónimo (ADH), los cifrados de nivel de exportación (EXP, cifrados que contienen DES), los tamaños de clave inferiores a 128 bits para el cifrado del tráfico de carga, el uso de MD5 como un mecanismo de hash del tráfico de carga, los conjuntos de cifrados IDEA y los conjuntos de cifrados RC4.

Procedimiento

- 1 Revise la entrada de cifrados del archivo `/etc/haproxy/conf.d/20-vcac.cfg` de la directiva de enlace y deshabilite aquellos que no considere seguros.

```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH
+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-
tls10 no-tls11
```

- 2 Revise la entrada de cifrados del archivo `/etc/haproxy/conf.d/30-vro-config.cfg` de la directiva de enlace y deshabilite aquellos que no considere seguros.

```
bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH
no-sslsv3 no-tlsv10 no-tlsv11
```

Deshabilitar cifrados no seguros del servicio de proxy de la consola del dispositivo de Dispositivo de vRealize Automation

Compare los cifrados del servicio de proxy de la consola del dispositivo de vRealize Automation con la lista cifrados aceptados y deshabilite todos los que no considere seguros.

Deshabilite los conjuntos de cifrados que no ofrezcan autenticación, como los conjuntos de cifrados NULL, aNULL o eNULL. Deshabilite también el intercambio de claves Diffie-Hellman anónimo (ADH), los cifrados de nivel de exportación (EXP, cifrados que contienen DES), los tamaños de clave inferiores a 128 bits para el cifrado del tráfico de carga, el uso de MD5 como un mecanismo de hash del tráfico de carga, los conjuntos de cifrados IDEA y los conjuntos de cifrados RC4.

Procedimiento

- 1 Abra el archivo `/etc/vcac/security.properties` en un editor de texto.
- 2 Agregue una línea al archivo para deshabilitar los conjuntos de cifrados no deseados.

Utilice una variación de la siguiente línea:

```
consoleproxy.ssl.ciphers.disallowed=cipher_suite_1, cipher_suite_2, etc.
```

Por ejemplo, para deshabilitar los conjuntos de claves de cifrado AES 128 y AES 256, añada la siguiente línea:

```
consoleproxy.ssl.ciphers.disallowed=TLS_DH_DSS_WITH_AES_128_CBC_SHA,
TLS_DH_DSS_WITH_AES_256_CBC_SHA, TLS_DH_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

- 3 Reinicie el servidor mediante el siguiente comando.

```
service vcac-server restart
```

Deshabilitar cifrados no seguros en el servicio vCO de Dispositivo de vRealize Automation

Compare los cifrados del servicio vCO de Dispositivo de vRealize Automation con la lista de cifrados aceptados y deshabilite todos los que se consideren no seguros.

Deshabilite los conjuntos de cifrados que no ofrezcan autenticación, como los conjuntos de cifrados NULL, aNULL o eNULL. Deshabilite también el intercambio de claves Diffie-Hellman anónimo (ADH), los cifrados de nivel de exportación (EXP, cifrados que contienen DES), los tamaños de clave inferiores a 128 bits para el cifrado del tráfico de carga, el uso de MD5 como un mecanismo de hash del tráfico de carga, los conjuntos de cifrados IDEA y los conjuntos de cifrados RC4.

Procedimiento

- 1 Busque la etiqueta <Connector> en el archivo /etc/vco/app/server/server.xml.
- 2 Edite o añada el atributo de cifrado para utilizar los conjuntos de claves cifrado deseados.

Consulte el siguiente ejemplo:

```
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
```

Deshabilitar cifrados no seguros en el servicio RabbitMQ de Dispositivo de vRealize Automation

Compare los cifrados del servicio RabbitMQ de Dispositivo de vRealize Automation con la lista de cifrados aceptados y deshabilite todos los que considere no seguros.

Deshabilite los conjuntos de cifrados que no ofrezcan autenticación, como los conjuntos de cifrados NULL, aNULL o eNULL. Deshabilite también el intercambio de claves Diffie-Hellman anónimo (ADH), los cifrados de nivel de exportación (EXP, cifrados que contienen DES), los tamaños de clave inferiores a 128 bits para el cifrado del tráfico de carga, el uso de MD5 como un mecanismo de hash del tráfico de carga, los conjuntos de cifrados IDEA y los conjuntos de cifrados RC4.

Procedimiento

- 1 Para analizar los conjuntos de cifrados compatibles, ejecute el comando
/usr/sbin/rabbitmqctl eval 'ssl:cipher_suites().'

Los cifrados que se devuelven en el siguiente ejemplo representan solo los cifrados compatibles. El servidor de RabbitMQ no utiliza ni anuncia estos cifrados, a menos que esté configurado para hacerlo en el archivo rabbitmq.config.

```
["ECDHE-ECDSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-GCM-SHA384",  
"ECDHE-ECDSA-AES256-SHA384", "ECDHE-RSA-AES256-SHA384",  
"ECDH-ECDSA-AES256-GCM-SHA384", "ECDH-RSA-AES256-GCM-SHA384",  
"ECDH-ECDSA-AES256-SHA384", "ECDH-RSA-AES256-SHA384",  
"DHE-RSA-AES256-GCM-SHA384", "DHE-DSS-AES256-GCM-SHA384",  
"DHE-RSA-AES256-SHA256", "DHE-DSS-AES256-SHA256", "AES256-GCM-SHA384",  
"AES256-SHA256", "ECDHE-ECDSA-AES128-GCM-SHA256",  
"ECDHE-RSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES128-SHA256",  
"ECDHE-RSA-AES128-SHA256", "ECDH-ECDSA-AES128-GCM-SHA256",  
"ECDH-RSA-AES128-GCM-SHA256", "ECDH-ECDSA-AES128-SHA256",  
"ECDH-RSA-AES128-SHA256", "DHE-RSA-AES128-GCM-SHA256",  
"DHE-DSS-AES128-GCM-SHA256", "DHE-RSA-AES128-SHA256", "DHE-DSS-AES128-SHA256",  
"AES128-GCM-SHA256", "AES128-SHA256", "ECDHE-ECDSA-AES256-SHA",  
"ECDHE-RSA-AES256-SHA", "DHE-RSA-AES256-SHA", "DHE-DSS-AES256-SHA",  
"ECDH-ECDSA-AES256-SHA", "ECDH-RSA-AES256-SHA", "AES256-SHA",  
"ECDHE-ECDSA-DES-CBC3-SHA", "ECDHE-RSA-DES-CBC3-SHA", "EDH-RSA-DES-CBC3-SHA",
```



```
"EDH-DSS-DES-CBC3-SHA", "ECDH-ECDSA-DES-CBC3-SHA", "ECDH-RSA-DES-CBC3-SHA",
"DES-CBC3-SHA", "ECDHE-ECDSA-AES128-SHA", "ECDHE-RSA-AES128-SHA",
"DHE-RSA-AES128-SHA", "DHE-DSS-AES128-SHA", "ECDH-ECDSA-AES128-SHA",
"ECDH-RSA-AES128-SHA", "AES128-SHA"]
```

- 2 Seleccione los cifrados compatibles que cumplan con los requisitos de seguridad de su organización.

Por ejemplo, para permitir solo ECDHE-ECDSA-AES128-GCM-SHA256 & ECDHE-ECDSA-AES256-GCM-SHA384, revise el archivo `/etc/rabbitmq/rabbitmq.config` y agregue la siguiente línea a `ssl_options`.

```
{ciphers, ["ECDHE-ECDSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES256-GCM-SHA384"]}
```

- 3 Reinicie el servidor de RabbitMQ con el siguiente comando.

```
service rabbitmq-server restart
```

Comprobar la seguridad de datos en reposo

Compruebe la seguridad de los usuarios y las cuentas de la base de datos con vRealize Automation.

Usuario de Postgres

La cuenta de usuario de Postgres Linux está vinculada a la función de cuenta de superusuario de la base de datos de Postgres, la cual es una cuenta bloqueada de forma predeterminada. Esta es la configuración más segura para este usuario, ya que solo es accesible desde la cuenta de usuario raíz. No desbloquee esta cuenta de usuario.

Funciones de cuenta de usuario de base de datos

Las funciones predeterminadas de la cuenta de usuario de Postgres no deben utilizarse al margen de la funcionalidad de la aplicación. Para poder admitir actividades de generación de informes o revisión de base de datos no predeterminadas, debe crearse una cuenta adicional que esté protegida con una contraseña apropiada.

Ejecute el siguiente script en la línea de comandos:

```
vcac-vami add-db-user newUsername newPassword
```

Esto agregará un nuevo usuario y una contraseña proporcionada por el usuario.

NOTA: Este script debe ejecutarse en la base de datos de Postgres principal en los casos donde existe una configuración de Postgres de HA principal-esclavo.

Configurar autenticación de cliente de PostgreSQL

Asegúrese de que la autenticación de confianza local no esté configurada en la base de datos PostgreSQL del dispositivo de vRealize Automation. Esta configuración permite que cualquier usuario local, incluido el superusuario de base de datos, se conecte como cualquier usuario de PostgreSQL sin una contraseña.

NOTA: La cuenta de superusuario de Postgres debe permanecer como de confianza local.

Se recomienda el método de autenticación md5, ya que envía contraseñas cifradas.

La configuración de autenticación de cliente se encuentra en el archivo `/storage/db/pgdata/pg_hba.conf`.

```
# TYPE  DATABASE  USER          ADDRESS        METHOD

# "local" is for Unix domain socket connections only
local    all             postgres              trust
# IPv4 local connections:
#host    all             all              127.0.0.1/32      md5
hostssl  all             all              127.0.0.1/32      md5
# IPv6 local connections:
#host    all             all              ::1/128           md5
hostssl  all             all              ::1/128           md5

# Allow remote connections for VCAC user.
#host    vcac             vcac             0.0.0.0/0          md5
hostssl  vcac             vcac             0.0.0.0/0          md5
hostssl  vcac             vcac             ::0/0              md5
# Allow remote connections for VCAC replication user.
#host    vcac             vcac_replication 0.0.0.0/0          md5
hostssl  vcac             vcac_replication 0.0.0.0/0          md5
hostssl  vcac             vcac_replication ::0/0              md5
# Allow replication connections by a user with the replication privilege.
#host    replication      vcac_replication 0.0.0.0/0          md5
hostssl  replication      vcac_replication 0.0.0.0/0          md5
hostssl  replication      vcac_replication ::0/0              md5
```

Si edita el archivo `pg_hba.conf`, debe reiniciar el servidor de Postgres ejecutando los siguientes comandos para que los cambios surtan efecto.

```
# cd /opt/vmware/vpostgres/9.2/bin
# su postgres
# ./pg_ctl restart -D /storage/db/pgdata/ -m fast
```

Configurar recursos de aplicación de vRealize Automation

Revise los recursos de aplicación de vRealize Automation y restrinja los permisos de archivo.

Procedimiento

- 1 Ejecute el siguiente comando para comprobar que los archivos con bits SUID y GUID estén definidos correctamente.

```
find / -path /proc -prune -o -type f -perm +6000 -ls
```

Debería aparecer la siguiente lista.

```
2197357  24 -rwsr-xr-x  1 polkituser root      23176 Mar 31  2015 /usr/lib/PolicyKit/polkit-
set-default-helper
2197354  16 -rwxr-sr-x  1 root      polkituser  14856 Mar 31  2015 /usr/lib/PolicyKit/polkit-
read-auth-helper
2197353  12 -rwsr-x---  1 root      polkituser  10744 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper-pam
2197352  20 -rwxr-sr-x  1 root      polkituser  19208 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper
2197351  20 -rwxr-sr-x  1 root      polkituser  19008 Mar 31  2015 /usr/lib/PolicyKit/polkit-
explicit-grant-helper
2197356  24 -rwxr-sr-x  1 root      polkituser  23160 Mar 31  2015 /usr/lib/PolicyKit/polkit-
revoke-helper
2188203 460 -rws--x--x  1 root      root      465364 Apr 21 22:38 /usr/lib64/ssh/ssh-keysign
2138858  12 -rwxr-sr-x  1 root      tty       10680 May 10  2010 /usr/sbin/utempter
2142482 144 -rwsr-xr-x  1 root      root      142890 Sep 15  2015 /usr/bin/passwd
2142477 164 -rwsr-xr-x  1 root      shadow    161782 Sep 15  2015 /usr/bin/chage
2142467 156 -rwsr-xr-x  1 root      shadow    152850 Sep 15  2015 /usr/bin/chfn
1458298 364 -rwsr-xr-x  1 root      root      365787 Jul 22  2015 /usr/bin/sudo
2142481  64 -rwsr-xr-x  1 root      root      57776 Sep 15  2015 /usr/bin/newgrp
1458249  40 -rwsr-x---  1 root      trusted   40432 Mar 18  2015 /usr/bin/crontab
2142478 148 -rwsr-xr-x  1 root      shadow    146459 Sep 15  2015 /usr/bin/chsh
2142480 156 -rwsr-xr-x  1 root      shadow    152387 Sep 15  2015 /usr/bin/gpasswd
2142479  48 -rwsr-xr-x  1 root      shadow    46967 Sep 15  2015 /usr/bin/expiry
311484  48 -rwsr-x---  1 root      messagebus 47912 Sep 16  2014 /lib64/dbus-1/dbus-daemon-
launch-helper
876574  36 -rwsr-xr-x  1 root      shadow    35688 Apr 10  2014 /sbin/unix_chkpwd
876648  12 -rwsr-xr-x  1 root      shadow    10736 Dec 16  2011 /sbin/unix2_chkpwd
 49308  68 -rwsr-xr-x  1 root      root      63376 May 27  2015 /opt/likewise/bin/ksu
1130552  40 -rwsr-xr-x  1 root      root      40016 Apr 16  2015 /bin/su
1130511  40 -rwsr-xr-x  1 root      root      40048 Apr 15  2011 /bin/ping
1130600 100 -rwsr-xr-x  1 root      root      94808 Mar 11  2015 /bin/mount
1130601  72 -rwsr-xr-x  1 root      root      69240 Mar 11  2015 /bin/umount
1130512  36 -rwsr-xr-x  1 root      root      35792 Apr 15  2011 /bin/ping6
2012 /lib64/dbus-1/dbus-daemon-launch-helper
```

- 2 Ejecute el siguiente comando para comprobar que todos los archivos del dispositivo virtual tienen un propietario.

```
find / -path /proc -prune -o -nouser -o -nogroup
```

- 3 Ejecute el siguiente comando para verificar los permisos de todos los archivos en el dispositivo virtual para comprobar que ninguno de ellos puede ser modificado por cualquier usuario.

```
find / -name ".*" -type f -perm -a+w | xargs ls -ldb
```

- 4 Ejecute el siguiente comando para comprobar que solo el usuario vcac es el propietario de los archivos correctos.

```
find / -name "proc" -prune -o -user vcac -print | egrep -v -e "*/vcac/*" | egrep -v -e "*/vmware-vcac/*"
```

Si se devuelve ningún resultado, todos los archivos correctos son propiedad exclusiva del usuario vcac.

- 5 Compruebe que solo el usuario vcac tenga permiso para escribir en los siguientes archivos.

```
/etc/vcac/vcac/security.properties
/etc/vcac/vcac/solution-users.properties
/etc/vcac/vcac/sso-admin.properties
/etc/vcac/vcac/vcac.keystore
/etc/vcac/vcac/vcac.properties
```

Compruebe también los siguientes archivos y sus subdirectorios:

```
/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*
```

- 6 Compruebe que solo el usuario raíz o el usuario vcac pueden leer los archivos correctos en los siguientes directorios y sus subdirectorios.

```
/etc/vcac/*
/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*
```

- 7 Compruebe que los archivos correctos son propiedad exclusiva del usuario raíz o el usuario vco, como se muestra en los siguientes directorios y sus subdirectorios.

```
/etc/vco/*
/var/log/vco/*
/var/lib/vco/*
/var/cache/vco/*
```

- 8 Compruebe que solo el usuario raíz o el usuario vco pueden escribir en los archivos correctos, como se muestra en los siguientes directorios y sus subdirectorios.

```
/etc/vco/*
/var/log/vco/*
```

`/var/lib/vco/*`

`/var/cache/vco/*`

- 9 Compruebe que solo el usuario raíz o el usuario vco pueden leer los archivos correctos, como se muestra en los siguientes directorios y sus subdirectorios.

`/etc/vco/*`

`/var/log/vco/*`

`/var/lib/vco/*`

`/var/cache/vco/*`

Personalizar configuración de proxy de la consola

Puede personalizar la configuración de la consola remota para que vRealize Automation facilite la solución de problemas y las prácticas recomendadas organizativas.

Al instalar, configurar o mantener vRealize Automation, puede cambiar algunas opciones para habilitar la solución de problemas y la depuración de la instalación. Catalogue y audite cada uno de los cambios que realice para asegurarse de que los componentes aplicables estén protegidos correctamente según su uso requerido. No pase a la etapa de producción si no está seguro de que los cambios de configuración están protegidos correctamente.

Personalizar la caducidad de ticket de VMware Remote Console

Puede personalizar el período de validez de los tickets de consola remota que se utilizan para establecer conexiones de VMware Remote Console.

Cuando un usuario establece conexiones de VMware Remote Console, el sistema crea y devuelve una credencial única que establece una conexión específica con una máquina virtual. Puede establecer la caducidad de ticket para un período de tiempo especificado en minutos.

Procedimiento

- 1 Abra el archivo `/etc/vcac/security.properties` en un editor de texto.
- 2 Agregue una línea al archivo con el formato `consoleproxy.ticket.validitySec=30`.
En esta línea, el valor numérico especifica la cantidad de minutos que debe transcurrir antes de que caduque el ticket.
- 3 Guarde el archivo y ciérrelo.
- 4 Reinicie el servidor vCAC mediante el comando `/etc/init.d/vcac-server restart`.

El valor de caducidad de ticket se restablece en el período de tiempo especificado en minutos.

Personalizar el puerto del servidor proxy de la consola

Puede personalizar el puerto en el que el proxy de la consola VMware Remote Console escucha los mensajes.

Procedimiento

- 1 Abra el archivo `/etc/vcac/security.properties` en un editor de texto.
- 2 Agregue una línea al archivo con el formato `consoleproxy.service.port=8445`.

El valor numérico especifica el número de puerto del servicio de proxy de la consola (en este caso, 8445).

- 3 Guarde el archivo y ciérrelo.
- 4 Reinicie el servidor vCAC mediante el comando `/etc/init.d/vcac-server restart`.

El puerto del servicio de proxy cambia al número de puerto especificado.

Configurar encabezado de respuesta X-XSS-Protection

Agregue el encabezado de respuesta X-XSS-Protection al archivo de configuración de HAProxy.

Procedimiento

- 1 Abra `/etc/haproxy/conf.d/20-vcac.cfg` para editarlo.
- 2 Añada las siguientes líneas en una sección de front-end:

```
rspdel X-XSS-Protection:\ 1;\ mode=block
rspadd X-XSS-Protection:\ 1;\ mode=block
```

- 3 Vuelva a cargar la configuración de HAProxy mediante el siguiente comando.
`/etc/init.d/haproxy reload`

Configurar encabezado de respuesta de seguridad de transporte estricto de HTTP

Agregue el encabezado de respuesta de transporte estricto de HTTP (HSTS) a la configuración de HAProxy.

Procedimiento

- 1 Abra `/etc/haproxy/conf.d/20-vcac.cfg` para editarlo.
- 2 Añada las siguientes líneas en una sección de front-end:

```
rspdel Strict-Transport-Security:\ max-age=31536000
rspadd Strict-Transport-Security:\ max-age=31536000
```

- 3 Vuelva a cargar la configuración de HAProxy mediante el siguiente comando.
`/etc/init.d/haproxy reload`

Configurar encabezado de respuesta X-Frame-Options

El encabezado de respuesta X-Frame-Options puede aparecer dos veces en algunos casos.

El encabezado de respuesta X-Frame-Options puede aparecer dos veces debido a que el servicio de vIDM agrega este encabezado tanto al back-end como a HAProxy. Puede evitar que aparezca dos veces si se configura de forma adecuada.

Procedimiento

- 1 Abra `/etc/haproxy/conf.d/20-vcac.cfg` para editarlo.
- 2 En la sección de front-end, busque la siguiente línea:
`rspadd X-Frame-Options:\ SAMEORIGIN`
- 3 Agregue las siguientes líneas antes de la línea que ha encontrado en el paso anterior:
`rspdel X-Frame-Options:\ SAMEORIGIN`
- 4 Vuelva a cargar la configuración de HAProxy mediante el siguiente comando.
`/etc/init.d/haproxy reload`

Configurar encabezados de respuesta de servidor

Como procedimiento de seguridad recomendado, configure el sistema de vRealize Automation para limitar la información que está disponible para los posibles atacantes.

En la medida que sea posible, reduzca la cantidad de información que el sistema comparte sobre su identidad y su versión. Los piratas informáticos y los agentes malintencionados pueden utilizar esta información para realizar ataques contra su versión o su servidor web específicos.

Configurar encabezado de respuesta del servidor Lighttpd

Se recomienda crear un encabezado de servidor en blanco para el servidor Lighttpd del dispositivo de vRealize Automation.

Procedimiento

- 1 Abra el archivo `/opt/vmware/etc/lighttpd/lighttpd.conf` en un editor de texto.
- 2 Añada `server.tag = " "` al archivo.
- 3 Guarde los cambios y cierre el archivo.
- 4 Reinicie el servidor Lighttpd ejecutando el comando `# /opt/vmware/etc/init.d/vami-lighttpd restart`.

Configurar el encabezado de respuesta de TCServer para el dispositivo de vRealize Automation

Se recomienda crear un encabezado de servidor en blanco personalizado para el encabezado de respuesta de TCServer que se utiliza con el dispositivo de vRealize Automation con el fin de limitar la posibilidad de que un atacante malintencionado obtenga información valiosa.

Procedimiento

- 1 Abra el archivo `/etc/vco/app-server/server.xml` con un editor de texto.

- 2 En cada elemento <Connector>, agregue `server=" "`.

Por ejemplo, <Connector protocol="HTTP/1.1" server="" />.

- 3 Guarde los cambios y cierre el archivo.
- 4 Reinicie el servidor mediante el siguiente comando.

```
service vco-server restart
```

Configurar el encabezado de respuesta del servidor de Internet Information Services

Se recomienda crear un encabezado de servidor en blanco personalizado para el servidor de Internet Information Services (IIS) que se utiliza con Identity Appliance para limitar la posibilidad de que atacantes malintencionados obtengan información valiosa.

Procedimiento

- 1 Abra el archivo `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini` en un editor de texto.
- 2 Busque `RemoveServerHeader=0` y cámbielo por `RemoveServerHeader=1..`
- 3 Guarde los cambios y cierre el archivo.
- 4 Reinicie el servidor ejecutando el comando `iisreset`.

Qué hacer a continuación

Deshabilite el encabezado "IIS X-Powered by" mediante la eliminación de los encabezados de respuesta HTTP de la lista en la consola de Administrador de IIS.

- 1 Abra la consola de Administrador de IIS.
- 2 Abra el encabezado de respuesta HTTP y quítelo de la lista.
- 3 Reinicie el servidor ejecutando el comando `iisreset`.

Establecer el tiempo de espera de sesión de Dispositivo de vRealize Automation

Configure el tiempo de espera de sesión en Dispositivo de vRealize Automation de acuerdo con la política de seguridad de la empresa.

El tiempo de espera de sesión predeterminado de Dispositivo de vRealize Automation para la inactividad del usuario es de 30 minutos. Para ajustar este valor de tiempo de espera de modo que cumpla con la política de seguridad de la organización, edite el archivo `web.xml` en la máquina host de Dispositivo de vRealize Automation.

Procedimiento

- 1 Abra el archivo `/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml` en un editor de texto.

- 2 Busque `session-config` y establezca el valor de tiempo de espera de sesión. Consulte el siguiente código de ejemplo.

```
<!-- 30 minutes session expiration time -->
<session-config>
  <session-timeout>30</session-timeout>
  <tracking-mode>COOKIE</tracking-mode>
  <cookie-config>
    <path>/</path>
  </cookie-config>
</session-config>
```

- 3 Reinicie el servidor ejecutando el siguiente comando.

```
service vcac-server restart
```

Administrar software no esencial

Para minimizar los riesgos de seguridad, quite o configure el software no esencial de las máquinas host de vRealize Automation.

Configure todo el software que no haya quitado en función de las recomendaciones del fabricante y los procedimientos recomendados de seguridad para minimizar las posibilidades de que genere infracciones de seguridad.

Proteger el controlador de almacenamiento USB

Proteja el controlador de almacenamiento USB para evitar que se utilice como controlador de dispositivo USB con las máquinas host del dispositivo virtual de VMware. Los posibles atacantes pueden aprovechar este controlador para poner en peligro el sistema.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.
- 2 Asegúrese de que la línea `install usb-storage /bin/true` aparezca en el archivo.
- 3 Guarde el archivo y ciérrelo.

Proteger el controlador del protocolo Bluetooth

Proteja el controlador del protocolo Bluetooth en las máquinas host del dispositivo virtual para evitar que los posibles atacantes lo aprovechen.

La vinculación del protocolo Bluetooth con la pila de red es innecesaria y puede incrementar la superficie del host expuesta a ataques.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.

- 2 Asegúrese de que la línea siguiente aparezca en el archivo.

```
install bluetooth /bin/true
```

- 3 Guarde el archivo y ciérrelo.

Proteger el protocolo Stream Control Transmission Protocol

Evite que el protocolo Stream Control Transmission Protocol (SCTP) se cargue en el sistema de forma predeterminada. Los posibles atacantes podrían aprovechar este protocolo para poner en peligro el sistema.

Configure el sistema para evitar que se cargue el módulo de Stream Control Transmission Protocol (SCTP), a menos que sea absolutamente necesario. SCTP es un protocolo de capa de transporte estandarizado por IETF que no se utiliza. Al vincular este protocolo con la pila de red, se incrementa la superficie del host expuesta a ataques. Los procesos locales sin privilegios podrían causar que el kernel cargue un controlador de protocolo de manera dinámica abriendo un socket mediante el protocolo.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.

- 2 Asegúrese de que la línea siguiente aparezca en el archivo.

```
install sctp /bin/true
```

- 3 Guarde el archivo y ciérrelo.

Proteger protocolo de congestión de datagramas

Como parte de las actividades de protección del sistema, evite que el protocolo de congestión de datagramas (Datagram Congestion Protocol, DCCP) se cargue en las máquinas host del dispositivo virtual de forma predeterminada. Los posibles atacantes pueden aprovechar este protocolo para poner en peligro el sistema.

Evite cargar el protocolo de control de congestión de datagramas (Datagram Congestion Control Protocol, DCCP), a menos que sea absolutamente necesario. DCCP es un protocolo de capa de transporte propuesto que no se utiliza. Al vincular este protocolo con la pila de red, se incrementa la superficie del host expuesta a ataques. Los procesos locales sin privilegios pueden causar que el kernel cargue un controlador de protocolo de manera dinámica mediante el protocolo para abrir un socket.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.

- 2 Asegúrese de que las líneas de DCCP aparezcan en el archivo.

```
install dccp/bin/true
install dccp_ipv4/bin/true
install dccp_ipv6/bin/true
```

- 3 Guarde el archivo y ciérrelo.

Proteger el puente de red

Evite que el módulo de puente de red se cargue en el sistema de forma predeterminada. Los posibles atacantes podrían aprovecharlo para poner en peligro el sistema.

Configure el sistema para evitar que se cargue la red, a menos que sea absolutamente necesario. Los posibles atacantes podrían aprovecharla para sortear la seguridad y las particiones de red.

Procedimiento

- 1 Ejecute el siguiente comando en todas las máquinas host del dispositivo virtual de VMware.

```
# rmmod bridge
```

- 2 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.

- 3 Asegúrese de que la línea siguiente aparezca en el archivo.

```
install bridge /bin/false
```

- 4 Guarde el archivo y ciérrelo.

Proteger el protocolo Reliable Datagram Sockets

Como parte de las actividades de protección del sistema, evite que el protocolo Reliable Datagram Sockets (RDS) se cargue en las máquinas host del dispositivo virtual de forma predeterminada. Los posibles atacantes pueden aprovechar este protocolo para poner en peligro el sistema.

Al vincular el protocolo Reliable Datagram Sockets (RDS) con la pila de red, se incrementa la superficie del host expuesta a ataques. Los procesos locales sin privilegios pueden causar que el sistema cargue un controlador de protocolo de manera dinámica mediante el protocolo para abrir un socket.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.

- 2 Asegúrese de que la línea `install rds /bin/true` aparezca en el archivo.

- 3 Guarde el archivo y ciérrelo.

Proteger el protocolo de comunicación transparente entre procesos

Como parte de las actividades de protección del sistema, evite que el Protocolo de comunicación transparente entre procesos (Transparent Inter-Process Communication Protocol, TIPC) se cargue en las máquinas host de dispositivo virtual de forma predeterminada. Los posibles atacantes pueden aprovechar este protocolo para poner en peligro el sistema.

Vincular el TIPC a la pila de red aumenta la superficie del host expuesta a ataques. Los procesos locales sin privilegios pueden causar que el kernel cargue un controlador de protocolo de manera dinámica mediante el protocolo para abrir un socket.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.

- 2 Asegúrese de que la línea `install tipc /bin/true` aparezca en el archivo.
- 3 Guarde el archivo y ciérrelo.

Proteger el protocolo Internetwork Packet Exchange

Evite que el protocolo Internetwork Packet Exchange (IPX) se cargue en el sistema de forma predeterminada. Los posibles atacantes podrían aprovechar este protocolo para poner en peligro el sistema.

Evite cargar el módulo del protocolo Internetwork Packet Exchange (IPX), a menos que sea absolutamente necesario. El protocolo IPX es un protocolo de nivel de red obsoleto. Al vincular este protocolo con la pila de red, se incrementa la superficie del host expuesta a ataques. Los procesos locales sin privilegios podrían causar que el sistema cargue un controlador de protocolo de manera dinámica mediante el protocolo para abrir un socket.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.
- 2 Asegúrese de que la línea siguiente aparezca en el archivo.
`install ipx /bin/true`
- 3 Guarde el archivo y ciérrelo.

Proteger el protocolo Appletalk

Evite que el protocolo Appletalk se cargue en el sistema de forma predeterminada. Los posibles atacantes podrían aprovechar este protocolo para poner en peligro el sistema.

Evite cargar el módulo del protocolo Appletalk, a menos que sea absolutamente necesario. Al vincular este protocolo con la pila de red, se incrementa la superficie del host expuesta a ataques. Los procesos locales sin privilegios podrían causar que el sistema cargue un controlador de protocolo de manera dinámica mediante el protocolo para abrir un socket.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.
- 2 Asegúrese de que la línea siguiente aparezca en el archivo.
`install appletalk /bin/true`
- 3 Guarde el archivo y ciérrelo.

Proteger el protocolo DECnet

Evite que el protocolo DECnet se cargue en el sistema de forma predeterminada. Los posibles atacantes podrían aprovechar este protocolo para poner en peligro el sistema.

Evite cargar el módulo del protocolo DECnet, a menos que sea absolutamente necesario. Al vincular este protocolo con la pila de red, se incrementa la superficie del host expuesta a ataques. Los procesos locales sin privilegios podrían causar que el sistema cargue un controlador de protocolo de manera dinámica mediante el protocolo para abrir un socket.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` del protocolo DECnet en un editor de texto.
- 2 Asegúrese de que la línea siguiente aparezca en el archivo.
`install decnet /bin/true`
- 3 Guarde el archivo y ciérrelo.

Asegurar el módulo Firewire

Evite que el módulo Firewire se cargue en el sistema de forma predeterminada. Los posibles atacantes podrían aprovechar este protocolo para poner en peligro el sistema.

Evite cargar el módulo Firewire, a menos que sea absolutamente necesario.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.
- 2 Asegúrese de que la línea siguiente aparezca en el archivo.
`install ieee1394 /bin/true`
- 3 Guarde el archivo y ciérrelo.

Proteger el componente de infraestructura como servicio

Al proteger el sistema, ofrezca seguridad al componente de infraestructura como servicio (Infrastructure as a Service, IaaS) de vRealize Automation y su máquina host para evitar que posibles atacantes aprovechen esa vulnerabilidad.

Debe configurar la seguridad del componente de IaaS de vRealize Automation y el host en el que reside. Debe establecer o comprobar la configuración de los demás componentes y aplicaciones relacionados. En algunos casos, puede comprobar la configuración existente; en otros casos, debe cambiar o añadir ajustes para que la configuración sea adecuada.

Deshabilitar el servicio Hora de Windows

Como procedimiento de seguridad recomendado, use servidores horarios autorizados en lugar de la sincronización de hora del host en un entorno de producción de vRealize Automation.

En un entorno de producción, deshabilite la sincronización de hora del host y utilice los servidores horarios autorizados para permitir el seguimiento preciso de las acciones de usuario y la identificación de posibles intrusiones y ataques malintencionados a través de auditoría y registro.

Configurar TLS para datos en tránsito de infraestructura como servicio

Asegúrese de que la implementación de vRealize Automation use protocolos de TLS seguros para proteger los canales de transmisión de los componentes de infraestructura como servicio.

El protocolo Capa de sockets seguros (Secure Sockets Layer, SSL) y el protocolo Seguridad de la capa de transporte (Transport Layer Security, TLS) más reciente son protocolos criptográficos que permiten garantizar la seguridad del sistema durante las comunicaciones de red entre los diferentes componentes del sistema. Como SSL es un estándar más antiguo, muchos de sus implementos ya no ofrecen un nivel de protección adecuado contra posibles ataques. Se han identificado vulnerabilidades importantes en los protocolos SSL anteriores, incluidos SSLv2 y SSLv3. Estos protocolos ya no se consideran seguros.

Según las políticas de seguridad de la organización, puede que también sea recomendable deshabilitar TLS 1.0.

NOTA: Al finalizar TLS en el equilibrador de carga, deshabilite también los protocolos poco seguros, como SSLv2, SSLv3, así como TLS 1.0 si es necesario.

Deshabilitar SSLv3 en Internet Information Services

Como procedimiento de seguridad recomendado, deshabilite SSLv3 en Internet Information Services (IIS) en la máquina del servidor host de infraestructura como servicio (Infrastructure as a Service, IaaS).

Procedimiento

- 1 Ejecute el editor del Registro de Windows como administrador.
- 2 Desplácese hasta `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\` en la ventana del Registro.
- 3 Haga clic con el botón derecho en **Protocolos** y seleccione **Nuevo > Clave**.
- 4 Introduzca **SSL 3.0**.
- 5 En el árbol de navegación, haga clic con el botón derecho en la clave de **SSL 3.0** recientemente creada y, en el menú emergente, seleccione **Nuevo > Clave** e introduzca **Cliente**.
- 6 En el árbol de navegación, haga clic con el botón derecho en la clave de **SSL 3.0** recientemente creada y, en el menú emergente, seleccione **Nuevo > Clave** e introduzca **Servidor**.
- 7 En el árbol de navegación, en SSL 3.0, haga clic con el botón derecho en **Cliente**, seleccione **Nuevo > Valor DWORD (32 bits)** e introduzca **DisabledByDefault**.
- 8 En el árbol de navegación, en SSL 3.0, seleccione **Cliente** y, en el panel derecho, haga doble clic en **DisabledByDefault** e introduzca **1**.
- 9 En el árbol de navegación, en SSL 3.0, haga clic con el botón derecho en **Servidor**, seleccione **Nuevo > Valor DWORD (32 bits)** e introduzca **Habilitado**.

- 10 En el árbol de navegación, en SSL 3.0, seleccione **Servidor** y, en el panel derecho, haga doble clic en la instancia habilitada de **DWORD** e introduzca **0**.
- 11 Reinicie Windows Server.

Deshabilitar TLS 1.0 para IaaS

Para proporcionar máxima seguridad, configure IaaS para que utilice la limitación de peticiones y deshabilite TLS 1.0.

Para obtener más información, consulte el artículo de Microsoft Knowledge Base <https://support.microsoft.com/en-us/kb/245030>.

Procedimiento

- 1 Configure IaaS para utilizar la limitación de peticiones en lugar de sockets web.
 - a Actualice el archivo de configuración de Manager Service C:\Archivos de programa (x86)\VMware\VCAC\Server\ManagerService.exe.config agregando los siguientes valores en la sección <appSettings>.
- ```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```
- b Reinicie Manager Service (VMware vCloud Automation Center Service).
  - 2 Compruebe que TLS 1.0 esté deshabilitado en el servidor de IaaS.
    - a Ejecute el editor del Registro como administrador.
    - b En la ventana del Registro, desplácese hasta HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\.
    - c Haga clic con el botón derecho en Protocolos y seleccione **Nuevo > Clave** y, a continuación, introduzca **TLS 1.0**.
    - d En el árbol de navegación, haga clic con el botón derecho en la clave de TLS 1.0 que acaba de crear y, en el menú emergente, seleccione **Nuevo > Clave** e introduzca **Cliente**.
    - e En el árbol de navegación, haga clic derecho en la clave de TLS 1.0 que acaba de crear y, en el menú emergente, seleccione **Nuevo > Clave** e introduzca **Servidor**.
    - f En el árbol de navegación, en TLS 1.0, haga clic con el botón derecho en **Cliente** y, a continuación, haga clic en **Nuevo > Valor DWORD (32 bits)** e introduzca **DisabledByDefault**.
    - g En el árbol de navegación, en TLS 1.0, seleccione **Cliente** y en el panel derecho, haga doble clic en el DWORD **DisabledByDefault** e introduzca **1**.
    - h En el árbol de navegación, TLS 1.0, haga clic con el botón derecho en **Servidor** y seleccione **Nuevo > Valor DWORD (32 bits)** e introduzca **Habilitado**.

- i En el árbol de navegación, en TLS 1.0, seleccione **Servidor** y en el panel derecho, haga doble clic en el DWORD **Habilitado** e introduzca **0**.
- j Reinicie Windows Server.

## Configurar conjuntos de cifrados TLS

Para lograr la máxima seguridad, debe configurar los componentes de vRealize Automation para que utilicen cifrados seguros. Los cifrados que se negocian entre el servidor y el navegador determinan el nivel de cifrado que se utiliza durante una sesión de TLS. Para asegurarse de que se seleccionen solo cifrados seguros, deshabilite los cifrados no seguros en los componentes de vRealize Automation. Configure el servidor para que admita solo cifrados seguros y para que utilice tamaños de clave lo suficientemente grandes. Además, configure todos los cifrados en un orden adecuado.

### Conjuntos de cifrados que no son aceptables

Deshabilite los conjuntos de cifrados que no ofrezcan autenticación, como los conjuntos de cifrados NULL, aNULL o eNULL. Deshabilite también el intercambio de claves Diffie-Hellman anónimo (ADH), los cifrados de nivel de exportación (EXP, cifrados que contienen DES), los tamaños de clave inferiores a 128 bits para el cifrado del tráfico de carga, el uso de MD5 como un mecanismo de hash del tráfico de carga, los conjuntos de cifrados IDEA y los conjuntos de cifrados RC4. Asegúrese también de que estén deshabilitados los conjuntos de cifrados que usen el intercambio de claves Diffie-Hellman (DHE).

## Comprobar seguridad del servidor host

Como procedimiento recomendado de seguridad, compruebe la configuración de seguridad de las máquinas de servidor host de infraestructura como servicio (Infrastructure as a Service, IaaS).

Microsoft proporciona varias herramientas para ayudarle a comprobar la seguridad en las máquinas de servidor host. Para obtener instrucciones acerca del uso más adecuado de estas herramientas, póngase en contacto con su proveedor de Microsoft.

### Comprobar la línea base segura del servidor host

Ejecute Microsoft Baseline Security Analyzer (MBSA) para confirmar rápidamente que el servidor tiene las actualizaciones o las correcciones más recientes. Puede usar MBSA para instalar las revisiones de seguridad de Microsoft que falten y mantener el servidor actualizado con las recomendaciones de seguridad de Microsoft.

Descargue la versión más reciente de la herramienta MBSA del sitio web de Microsoft.

### Comprobar la configuración de seguridad del servidor host

Utilice el Asistente para configuración de seguridad (Security Configuration Wizard, SCW) de Windows y el kit de herramientas de Microsoft Security Compliance Manager (SCM) para comprobar que el servidor host está configurado de forma segura.



Ejecute el SCW desde las herramientas administrativas del servidor de Windows. Esta herramienta puede identificar las funciones del servidor y las características instaladas, incluidas las redes, los firewalls de Windows y la configuración del registro. Compare el informe con las directrices de protección más recientes del SCM relevante para el servidor de Windows. En función de los resultados, puede ajustar la configuración de seguridad de cada característica (como los servicios de red, la configuración de cuenta y los firewalls de Windows) y aplicar la configuración a su servidor.

Puede encontrar más información acerca de la herramienta SCW en el sitio web de Microsoft Technet.

## Proteger recursos de aplicación

Como procedimiento de seguridad recomendado, asegúrese de que todos los archivos pertinentes de infraestructura como servicio tengan los permisos correspondientes.

Revise los archivos de infraestructura como servicio en la instalación de infraestructura como servicio. En la mayoría de los casos, las subcarpetas y los archivos de cada carpeta deben tener la misma configuración que la carpeta.

Directorio o archivo	Grupo o usuarios	Control total	Modificación	Lectura y ejecución	Lectura	Escritura
VMware\vCAC\Agents\<agent_name> \logs	SISTEMA	X	X	X	X	X
	Administrador	X	X	X	X	X
	Administradores	X	X	X	X	X
VMware\vCAC\Agents\<agent_name> \temp	SISTEMA	X	X	X	X	X
	Administrador	X	X	X	X	X
	Administradores	X	X	X	X	X
VMware\vCAC\Agents\	SISTEMA	X	X	X	X	X
	Administradores	X	X	X	X	X
	Usuarios			X	X	
VMware\vCAC\Distributed Execution Manager\	SISTEMA	X	X	X	X	X
	Administradores	X	X	X	X	X
	Usuarios			X	X	
VMware\vCAC\Distributed Execution Manager\DEM\Log	SISTEMA	X	X	X	X	X
	Administrador	X	X	X	X	X
	Administradores	X	X	X	X	X
VMware\vCAC\Distributed Execution Manager\DEO\Log	SISTEMA	X	X	X	X	X
	Administrador	X	X	X	X	X
	Administradores	X	X	X	X	X
VMware\vCAC\Management Agent\	SISTEMA	X	X	X	X	X
	Administradores	X	X	X	X	X
	Usuarios			X	X	

Directorio o archivo	Grupo o usuarios	Control total	Modificación	Lectura y ejecución	Lectura	Escritura
VMware\vCAC\Server\	SISTEMA	X	X	X	X	X
	Administradores	X	X	X	X	X
	Usuarios			X	X	
VMware\vCAC\Web API	SISTEMA	X	X	X	X	X
	Administradores	X	X	X	X	X
	Usuarios			X	X	

## Proteger la máquina host de infraestructura como servicio

Como procedimiento de seguridad recomendado, revise la configuración básica en su máquina host de infraestructura como servicio (Infrastructure as a Service, IaaS) para asegurarse de que cumpla con las directrices de seguridad.

Proteja cuentas, aplicaciones, puertos y servicios varios en la máquina host de IaaS.

### Comprobar la configuración de la cuenta de usuario de servidor

Compruebe que no existan cuentas de usuario locales y de dominio, ni parámetros de configuración que no sean necesarios. Restrinja las cuentas de usuario que no estén relacionadas con las funciones de aplicación a aquellas que sean necesarias para la administración, el mantenimiento y la solución de problemas. Además, restrinja el acceso remoto de cuentas de usuario de dominio al mínimo necesario para mantener el servidor, y controle y audite estas cuentas de manera estricta.

### Eliminar aplicaciones innecesarias

Elimine todas las aplicaciones innecesarias de los servidores host. Las aplicaciones innecesarias aumentan el riesgo de exposición debido a vulnerabilidades desconocidas o no revisadas.

### Deshabilitar servicios y puertos innecesarios

Revise el firewall del servidor host para obtener la lista de puertos abiertos. Bloquee todos los puertos que no sean necesarios para el funcionamiento crítico del sistema o el componente de IaaS. Consulte [Configurar puertos y protocolos](#). Audite los servicios que se ejecutan en el servidor host y desactive aquellos que no sean necesarios.

# Configurar la seguridad de la red del host

## 8

Para proporcionar la máxima protección frente a amenazas de seguridad conocidas, configure los ajustes de comunicación e interfaz de red en todas las máquinas host de VMware.

Como parte de un plan de seguridad integral, configure los ajustes de seguridad de la interfaz de red de los componentes de infraestructura como servicio y los dispositivos virtuales de VMware de acuerdo con las directrices de seguridad establecidas.

Este capítulo cubre los siguientes temas:

- [Configurar ajustes de red para dispositivos de VMware](#)
- [Configurar ajustes de red para el host de infraestructura como servicio](#)
- [Configurar puertos y protocolos](#)

## Configurar ajustes de red para dispositivos de VMware

Para garantizar que las máquinas host del dispositivo virtual de VMware admitan únicamente comunicaciones esenciales y seguras, revise y edite su configuración de comunicación de red.

Examine la configuración del protocolo IP de red de las máquinas host de VMware y configure los ajustes de red en función de las directrices de seguridad. Deshabilite todos los protocolos de comunicación que no sean esenciales.

## Evitar el control de usuario de las interfaces de red

Como procedimiento de seguridad recomendado, conceda a los usuarios solo los privilegios de sistema que necesitan para realizar su trabajo en las máquinas host del dispositivo de VMware.

Si se permite que las cuentas de usuario con privilegios manipulen interfaces de red, es posible que se sorteen los mecanismos de seguridad de red o se deniegue el servicio. Restrinja la capacidad de los usuarios con privilegios para cambiar la configuración de interfaces de red.

### Procedimiento

- 1 Ejecute el siguiente comando en cada máquina host del dispositivo de VMware.

```
grep -i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*
```

- 2 Asegúrese de que cada interfaz esté establecida en NO.

## Establecer el tamaño de cola de trabajo pendiente de TCP

Para proporcionar un cierto nivel de defensa contra ataques malintencionados, configure un tamaño de cola de trabajo pendiente de TCP en las máquinas host de dispositivo VMware.

Defina los tamaños de cola de trabajo pendiente de TCP en un tamaño predeterminado adecuado para mitigar los ataques de denegación de servicio de TCP. La configuración predeterminada recomendada es 1280.

### Procedimiento

- 1 Ejecute el siguiente comando en cada máquina del host de dispositivo de VMware.

```
cat /proc/sys/net/ipv4/tcp_max_syn_backlog
```

- 2 Abra el archivo `/etc/sysctl.conf` en un editor de texto.

- 3 Establezca el tamaño predeterminado de cola de trabajo pendiente de TCP añadiendo la siguiente entrada al archivo.

```
net.ipv4.tcp_max_syn_backlog=1280
```

- 4 Guarde los cambios y cierre el archivo.

## Denegar ecos de ICMPv4 a direcciones de difusión

Como procedimiento de seguridad recomendado, compruebe que las máquinas host del dispositivo de VMware omitan las solicitudes de eco de direcciones de difusión de ICMP.

Las respuestas a ecos del Protocolo de mensajes de control de Internet (Internet Control Message Protocol, ICMP) de difusión proporcionan un vector de ataque para ataques de amplificación y pueden facilitar la asignación de redes por parte de agentes malintencionados. La configuración de las máquinas host del dispositivo para que omitan los ecos de ICMPv4 protege contra este tipo de ataques.

### Procedimiento

- 1 Ejecute el comando `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` en las máquinas host del dispositivo virtual de VMware para confirmar que deniegan las solicitudes de ecos de direcciones de difusión de IPv4.

Si se configuran las máquinas host para que denieguen las redirecciones de IPv4, este comando devolverá 0 para `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`.

- 2 Si desea configurar una máquina host del dispositivo virtual para que deniegue solicitudes de ecos de direcciones de difusión de ICMPv4, abra el archivo de `/etc/sysctl.conf` de las máquinas host de Windows en un editor de texto.
- 3 Busque la entrada que rece `net.ipv4.icmp_echo_ignore_broadcasts=0` . Si el valor para esta entrada no es 0 o si no existe la entrada, agréguela o actualice la entrada existente según corresponda.
- 4 Guarde los cambios y cierre el archivo.

## Deshabilitar ARP de proxy de IPv4

Compruebe que el ARP de proxy de IPv4 está deshabilitado si no es necesario en las máquinas host del dispositivo de VMware para evitar el uso compartido de información sin autorización.

El ARP de proxy de IPv4 permite a un sistema enviar respuestas a solicitudes de ARP en una interfaz en nombre de los hosts conectados a otra interfaz. Deshabilite esta opción si no es necesaria para evitar que se filtre información de direccionamiento entre los segmentos de red asociados.

### Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp | egrep "default|all"` en las máquinas host del dispositivo virtual de VMware para comprobar que el ARP de proxy de IPv4 está deshabilitado.

Si el ARP de proxy de IPv6 está deshabilitado en las máquinas host, este comando devolverá 0.

```
/proc/sys/net/ipv4/conf/all/proxy_arp:0
/proc/sys/net/ipv4/conf/default/proxy_arp:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar el ARP de proxy de IPv6 en las máquinas host, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv4.conf.default.proxy_arp=0
net.ipv4.conf.all.proxy_arp=0
```

Si las entradas no existen o si sus valores no son 0, agréguelas o actualice las entradas existentes según corresponda.

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

## Denegar mensajes de redirección de ICMP IPv4

Como procedimiento de seguridad recomendado, compruebe que las máquinas host del dispositivo virtual de VMware deniegan los mensajes de redirección de ICMP IPv4.

Los enrutadores utilizan mensajes de redirección de ICMP para indicar a los hosts que existe una ruta más directa a un destino. Un mensaje de redirección de ICMP malintencionado puede facilitar un ataque de tipo "Man in the middle". Estos mensajes modifican la tabla de rutas del host y no están autenticados. Asegúrese de que su sistema está configurado para omitirlos si no se necesitan por algún otro motivo.

**Procedimiento**

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects | egrep "default|all"` en las máquinas host del dispositivo de VMware para confirmar que deniegan los mensajes de redirección de IPv4.

Si las máquinas host están configuradas para denegar las redirecciones de IPv4, este comando devuelve lo siguiente:

```
/proc/sys/net/ipv4/conf/all/accept_redirects:0
```

```
/proc/sys/net/ipv4/conf/default/accept_redirects:0
```

- 2 Si necesita configurar una máquina host del dispositivo virtual para denegar los mensajes de redirección de IPv4, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe los valores de las líneas que comiencen con `net.ipv4.conf`.

Si los valores de las siguientes entradas no son 0 o si las entradas no existen, agréguelas al archivo o actualice las entradas existentes según corresponda.

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

- 4 Guarde los cambios realizados y cierre el archivo.

## Denegar mensajes de redirección de ICMP IPv6

Como procedimiento de seguridad recomendado, compruebe que las máquinas host del dispositivo virtual de VMware denieguen los mensajes de redirección de ICMP IPv6.

Los enrutadores utilizan mensajes de redirección de ICMP para indicar a los hosts que existe una ruta más directa a un destino. Un mensaje de redirección de ICMP malintencionado puede facilitar un ataque de tipo "Man in the middle". Estos mensajes modifican la tabla de rutas del host y no están autenticados. Asegúrese de que el sistema esté configurado para omitirlos si no se necesitan por algún otro motivo.

**Procedimiento**

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | egrep "default|all"` en las máquinas host del dispositivo virtual de VMware para confirmar que deniegan los mensajes de redirección de IPv6.

Si las máquinas host están configuradas para denegar las redirecciones de IPv6, este comando devuelve lo siguiente:

```
/proc/sys/net/ipv6/conf/all/accept_redirects:0
```

```
/proc/sys/net/ipv6/conf/default/accept_redirects:0
```

- 2 Para configurar una máquina host del dispositivo virtual para que se denieguen mensajes de redirección de IPv4, abra el archivo `/etc/sysctl.conf` en un editor de texto.

- 3 Compruebe los valores de las líneas que comiencen con `net.ipv6.conf`.

Si los valores de las siguientes entradas no son 0 o si las entradas no existen, agréguelas al archivo o actualice las entradas existentes según corresponda.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 Guarde los cambios y cierre el archivo.

## Registrar paquetes de datos con marcadores sospechosos IPv4

Como procedimiento de seguridad recomendado, compruebe que las máquinas host del dispositivo virtual de VMware registren paquetes de datos con marcadores sospechosos IPv4.

Los paquetes de datos con marcadores sospechosos contienen direcciones que el sistema sabe que no son válidas. Configure las máquinas host para registrar estos mensajes, de modo que pueda identificar configuraciones incorrectas o ataques en curso.

### Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que registran paquetes de datos con marcadores sospechosos IPv4.

Si las máquinas virtuales están configuradas para registrar paquetes de datos con marcadores sospechosos, devuelven lo siguiente:

```
/proc/sys/net/ipv4/conf/all/log_martians:1
/proc/sys/net/ipv4/conf/default/log_martians:1
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar máquinas virtuales para que registren paquetes de datos con marcadores sospechosos IPv4, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe los valores de las líneas que comienzan con `net.ipv4.conf`.

Si el valor de las siguientes entradas no es igual a 1 o si las entradas no existen, agréguelas al archivo o actualice las entradas existentes según corresponda.

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

- 4 Guarde los cambios y cierre el archivo.

## Utilizar el filtrado de rutas inversas IPv4

Como procedimiento de seguridad recomendado, compruebe que las máquinas host del dispositivo virtual de VMware utilicen el filtrado de rutas inversas IPv4.

El filtrado de rutas inversas protege contra las direcciones de origen suplantado haciendo que el sistema descarte los paquetes con direcciones de origen que no tengan una ruta o que tengan una que no apunte a la interfaz de origen. Configure las máquinas host de manera que utilicen el filtrado de rutas inversas siempre que sea posible. En algunos casos, según la función del sistema, el filtrado de rutas inversas puede hacer que el sistema descarte tráfico legítimo. Si encuentra problemas como este, es posible que deba utilizar un modo más permisivo o deshabilitar por completo el filtrado de rutas inversas.

### Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter | egrep "default|all"` en las máquinas host del dispositivo virtual de VMware para asegurarse de que utilicen el filtrado de rutas inversas IPv4.

Si las máquinas virtuales utilizan el filtrado de rutas inversas IPv4, el comando devuelve lo siguiente:

```
/proc/sys/net/ipv4/conf/all/rp_filter:1
/proc/sys/net/ipv4/conf/default/rp_filter:1
```

Si las máquinas virtuales se configuran correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar el filtrado de rutas inversas IPv4 en las máquinas host, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe los valores de las líneas que comiencen con `net.ipv4.conf`.

Si los valores de las siguientes entradas no se establecen como 1 o si no existen, agréguelas al archivo o actualice las entradas existentes según corresponda.

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

- 4 Guarde los cambios y cierre el archivo.

## Denegar reenvío de IPv4

Compruebe que las máquinas host del dispositivo de VMware deniegan el reenvío de IPv4.

Si el sistema está configurado para el reenvío de IP y no es un enrutador designado, los atacantes podrían utilizarlo para sortear la seguridad de red proporcionando una ruta de acceso para comunicación no filtrada por dispositivos de red. Para evitar el riesgo, configure las máquinas host del dispositivo virtual para que denieguen el reenvío de IPv4.

### Procedimiento

- 1 Ejecute el comando `# cat /proc/sys/net/ipv4/ip_forward` en las máquinas host del dispositivo de VMware para confirmar que deniegan el reenvío de IPv4.

Si las máquinas host están configuradas para denegar el reenvío de IPv4, este comando devolverá 0 para `/proc/sys/net/ipv4/ip_forward`. Si las máquinas virtuales están configuradas correctamente, no se necesita ninguna otra acción.



- 2 Si desea configurar una máquina host del dispositivo virtual para que deniegue el reenvío de IPv4, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Busque la entrada que rece `net.ipv4.ip_forward=0`. Si el valor para esta entrada no es 0 actualmente o si la entrada no existe, agréguela o actualice la entrada existente según corresponda.
- 4 Guarde todos los cambios y cierre el archivo.

## Denegar el reenvío de IPv6

Como procedimiento de seguridad recomendado, compruebe que los sistemas host del dispositivo de VMware denieguen el reenvío de IPv6.

Si el sistema está configurado para el reenvío de IP y no es un enrutador designado, los atacantes podrían utilizarlo para sortear la seguridad de red proporcionando una ruta de acceso para comunicación no filtrada por dispositivos de red. Configure las máquinas host del dispositivo virtual para que denieguen el reenvío de IPv6 para no correr este riesgo.

### Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding | grep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que deniegan el reenvío de IPv6.

Si las máquinas host están configuradas para denegar el reenvío de IPv6, este comando devolverá lo siguiente:

```
/proc/sys/net/ipv6/conf/all/forwarding:0
/proc/sys/net/ipv6/conf/default/forwarding:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar una máquina host para que deniegue el reenvío de IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe los valores de las líneas que comiencen con `net.ipv6.conf`.

Si los valores de las siguientes entradas no son 0 o si las entradas no existen, agréguelas o actualice las entradas existentes según corresponda.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

## Usar cookies SYN de TCP IPv4

Compruebe que las máquinas host del dispositivo VMware utilizan cookies SYN de TCP IPv4.

Un ataque "flood" SYN de TCP podría provocar una denegación de servicio al rellenar la tabla de conexiones TCP de un sistema con conexiones con el estado SYN\_RCVD. Las cookies SYN impiden que se realice el seguimiento de una conexión hasta que se reciba un ACK posterior que comprueba que el iniciador está intentando una conexión válida y no es un origen "flood". Esta técnica no funciona de una manera totalmente conforme con los estándares, pero solo se activa durante una condición "flood" y permite defender el sistema mientras continúa dando servicio a las solicitudes de servicio válidas.

### Procedimiento

- 1 Ejecute el comando `# cat /proc/sys/net/ipv4/tcp_syncookies` en las máquinas host del dispositivo de VMware para comprobar que utilizan cookies SYN de TCP IPv4.

Si las máquinas host se configuran para denegar el reenvío de IPv4, este comando devolverá 1 para `/proc/sys/net/ipv4/tcp_syncookies`. Si las máquinas virtuales están configuradas correctamente, no se necesita ninguna otra acción.

- 2 Si necesita configurar un dispositivo virtual para utilizar cookies SYN de TCP IPv4, abra el archivo `/etc/sysctl.conf` en un editor de texto.

- 3 Busque la entrada que rece `net.ipv4.tcp_syncookies=1`.

Si el valor para esta entrada no está establecido actualmente en 1, o bien si no existe, agregue la entrada o actualice la entrada existente según corresponda.

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

## Denegar anuncios de enrutador IPv6

Compruebe que las máquinas host de VMware denieguen la aceptación de anuncios de enrutador y redirecciones de ICMP, a menos que sean necesarios para el funcionamiento del sistema.

IPv6 permite a los sistemas configurar sus dispositivos de red mediante el uso automático de información de la red. Desde una perspectiva de seguridad, es preferible definir manualmente la información de configuración importante a aceptarla desde la red de una forma no autenticada.

### Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que deniegan los anuncios de enrutador.

Si las máquinas host están configuradas para denegar anuncios de enrutador IPv6, este comando devolverá 0:

```
/proc/sys/net/ipv6/conf/all/accept_ra:0
/proc/sys/net/ipv6/conf/default/accept_ra:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar una máquina host para que deniegue anuncios de enrutador IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.

### 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

Si no existen estas entradas o sus valores no son 0, agregue las entradas o actualice las existentes según corresponda.

### 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

## Denegar solicitudes de enrutador IPv6

Como procedimiento de seguridad recomendado, compruebe que las máquinas host del dispositivo de VMware deniegan solicitudes de enrutador IPv6, a menos se requieran para el funcionamiento del sistema.

La configuración de solicitudes de enrutador determina cuántas solicitudes de enrutador se envían al acceder a la interfaz. Si las direcciones se asignan de forma estática, no es necesario enviar ninguna solicitud.

### Procedimiento

#### 1 Ejecute el comando # `grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations|egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que deniegan las solicitudes de enrutador IPv6.

Si las máquinas host están configuradas para denegar anuncios de enrutador IPv6, este comando devolverá lo siguiente:

```
/proc/sys/net/ipv6/conf/all/router_solicitations:0
/proc/sys/net/ipv6/conf/default/router_solicitations:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

#### 2 Si necesita configurar máquinas host para denegar solicitudes de enrutador IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.

### 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.router_solicitations=0
net.ipv6.conf.default.router_solicitations=0
```

Si las entradas no existen o si sus valores no son 0, agréuelas o actualice las entradas existentes según corresponda.

### 4 Guarde todos los cambios y cierre el archivo.

## Denegar la preferencia de enrutador IPv6 en solicitudes de enrutador

Compruebe que las máquinas host del dispositivo de VMware denieguen las solicitudes de enrutador IPv6, a menos que sean necesarias para el funcionamiento del sistema.

La opción de preferencia de enrutador en las solicitudes determina las preferencias de enrutador. Si las direcciones se asignan de forma estática, no es necesario recibir ninguna preferencia de enrutador para las solicitudes.

### Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que denieguen las solicitudes de enrutador IPv6.

Si las máquinas host están configuradas para denegar anuncios de enrutador IPv6, este comando devolverá lo siguiente:

```
/proc/sys/net/ipv6/conf/all/accept_ra_rtr_pref:0
/proc/sys/net/ipv6/conf/default/accept_ra_rtr_pref:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar las máquinas host para que denieguen solicitudes de enrutamiento de IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
```

Si las entradas no existen o si sus valores no son 0, agréguelas o actualice las entradas existentes según corresponda.

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

## Denegar prefijos de enrutador IPv6

Compruebe que las máquinas host del dispositivo de VMware denieguen la información de prefijos de enrutador IPv6, a menos que sea necesaria para el funcionamiento del sistema.

La opción `accept_ra_pinfo` determina si el sistema acepta información de prefijos procedente del enrutador. Si las direcciones se asignan de forma estática, no es necesario recibir ninguna información de prefijos de enrutador.

**Procedimiento**

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que deniegan la información de prefijos de enrutador IPv6.

Si las máquinas host están configuradas para denegar anuncios de enrutador IPv6, este comando devolverá lo siguiente.

```
/proc/sys/net/ipv6/conf/all/accept_ra_pinfo:0
/proc/sys/net/ipv6/conf/default/accept_ra_pinfo:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar las máquinas host para que denieguen la información de prefijos de enrutador IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_pinfo=0
```

Si las entradas no existen o si sus valores no son 0, agréguelas o actualice las entradas existentes según corresponda.

- 4 Guarde todos los cambios y cierre el archivo.

## Denegar opciones de límite de saltos de anuncio de enrutador IPv6

Compruebe que las máquinas host del dispositivo de VMware denieguen las opciones de límite de saltos de enrutador IPv6, a menos que sean necesarias.

La opción `accept_ra_defrtr` determina si el sistema aceptará las opciones de límite de saltos de un anuncio de enrutador. Si se establece como 0, evita que un enrutador cambie el límite de saltos de IPv6 predeterminado para los paquetes salientes.

**Procedimiento**

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que deniegan las opciones de límite de saltos de enrutador IPv6.

Si las máquinas host están configuradas para denegar las opciones de límite de saltos de enrutador IPv6, este comando devolverá 0.

```
/proc/sys/net/ipv6/conf/all/accept_ra_defrtr:0
/proc/sys/net/ipv6/conf/default/accept_ra_defrtr:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar una máquina host para que deniegue las opciones de límite de saltos de enrutador IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Si las entradas no existen o si sus valores no son 0, agréguelas o actualice las entradas existentes según corresponda.

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

## Denegar opciones de configuración automática de anuncios de enrutador IPv6

Compruebe que las máquinas host del dispositivo de VMware denieguen las opciones de configuración automática de enrutador IPv6, a menos que sean necesarias.

La opción `autoconf` determina si los anuncios de enrutador pueden hacer que el sistema asigne una dirección de unidifusión global a una interfaz.

### Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que deniegan las opciones de configuración automática de enrutador IPv6.

Si las máquinas host están configuradas para denegar las opciones de configuración automática de enrutador IPv6, este comando devolverá 0.

```
/proc/sys/net/ipv6/conf/all/autoconf:0
/proc/sys/net/ipv6/conf/default/autoconf:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar una máquina host para que deniegue las opciones de configuración automática de enrutador IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Si las entradas no existen o si sus valores no son 0, agréguelas o actualice las entradas existentes según corresponda.

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

## Denegar solicitudes de vecino de IPv6

Compruebe que las máquinas host del dispositivo de VMware estén configuradas para denegar solicitudes de vecino de IPv6, a menos que sean necesarias.

La configuración de `dad_transmits` determina cuántas solicitudes de vecino se deben enviar por dirección (globales y locales de vínculo) al acceder a una interfaz para garantizar que la dirección deseada sea única en la red.

### Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits | egrep "default|all"` en las máquinas host del dispositivo de VMware para confirmar que denieguen las solicitudes de vecino de IPv6.

Si las máquinas host están configuradas para denegar solicitudes de vecino de IPv6, este comando devolverá 0.

```
/proc/sys/net/ipv6/conf/all/dad_transmits:0
/proc/sys/net/ipv6/conf/default/dad_transmits:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar una máquina host para que deniegue solicitudes de vecino de IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.dad_transmits=0
net.ipv6.conf.default.dad_transmits=0
```

Si las entradas no existen o si sus valores no son 0, agréguelas o actualice las entradas existentes según corresponda.

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

## Restringir la cantidad máxima de direcciones IPv6

Compruebe las máquinas host del dispositivo de VMware para restringir la configuración de la cantidad máxima de direcciones IPv6 al valor mínimo necesario para el funcionamiento del sistema.

La configuración de la cantidad máxima de direcciones determina cuántas direcciones IPv6 de unidifusión globales están disponibles para cada interfaz. El valor predeterminado es 16, pero debe establecerlo como la cantidad exacta de direcciones globales configuradas de manera estática que sean necesarias para el sistema.

## Procedimiento

- 1 Ejecute el comando `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que la cantidad máxima de direcciones IPv6 se restrinja correctamente.

Si se configuran las máquinas host para restringir la cantidad máxima de direcciones IPv6, este comando devolverá valores iguales a 1.

```
/proc/sys/net/ipv6/conf/all/max_addresses:1
/proc/sys/net/ipv6/conf/default/max_addresses:1
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar la cantidad máxima de direcciones IPv6 en máquinas host, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```

Si las entradas no existen o si sus valores no se establecen como 1, añada entradas o actualice las entradas existentes según corresponda.

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

## Configurar ajustes de red para el host de infraestructura como servicio

Como procedimiento de seguridad recomendado, configure los ajustes de comunicación de red en la máquina host del componente de infraestructura como servicio (IaaS) de VMware según los requisitos y las directrices de VMware.

Configure la red de la máquina host de infraestructura como servicio (IaaS) para admitir todas las funciones de vRealize Automation con la seguridad apropiada.

Consulte [Proteger el componente de infraestructura como servicio](#).

## Configurar puertos y protocolos

Como procedimiento de seguridad recomendado, configure los puertos y los protocolos de todos los dispositivos y componentes de vRealize Automation siguiendo las directrices de VMware.

Configure los puertos entrantes y salientes de los componentes de vRealize Automation según lo que se requiere para que los componentes críticos del sistema funcionen en producción. Deshabilite todos los protocolos y los puertos innecesarios. Consulte *Arquitectura de referencia de vRealize Automation*.



## Puertos de usuario necesarios

Como procedimiento de seguridad recomendado, configure los puertos de usuario de vRealize Automation según las directrices de VMware.

Exponga los puertos necesarios solo en una red segura.

SERVIDOR	PUERTOS
Dispositivo de vRealize Automation	443, 8443

## Puertos de administrador necesarios

Como procedimiento de seguridad recomendado, configure los puertos de administrador de vRealize Automation según las directrices de VMware.

Exponga los puertos necesarios solo en una red segura.

SERVIDOR	PUERTOS
Servidor de vRealize Application Services	5480

## Puertos de dispositivo de vRealize Automation

Como procedimiento recomendado de seguridad, configure los puertos entrantes y salientes de Dispositivo de vRealize Automation según las recomendaciones de VMware.

### Puertos entrantes

Configure el número mínimo de puertos entrantes necesarios para Dispositivo de vRealize Automation. Configure puertos opcionales si son necesarios para la configuración de su sistema.

**Tabla 8-1. Cantidad mínima de puertos entrantes necesaria**

PUERTO	PROTOCOLO	COMENTARIOS
443	TCP	Acceso a la consola de vRealize Automation y a las llamadas de API.
8443	TCP	Proxy de la consola (VMRC).
5480	TCP	Acceso a la consola de administración web del dispositivo virtual.
5488, 5489	TCP	Interno. Utilizado por Dispositivo de vRealize Automation para las actualizaciones.
5672	TCP	Mensajes de RabbitMQ.
		<b>NOTA:</b> Cuando agrupa instancias de Dispositivo de vRealize Automation en clústeres, es posible que deba configurar los puertos abiertos 4369 y 25672.
40002	TCP	Necesario para el servicio de vIDM. Protegido por un firewall contra todo el tráfico externo a excepción del tráfico procedente de otros nodos de Dispositivo de vRealize Automation cuando se agrega en la configuración de HA.

Si es necesario, configure puertos entrantes opcionales.

**Tabla 8-2. Puertos entrantes opcionales**

PUERTO	PROTOCOLO	COMENTARIOS
22	TCP	(Opcional) SSH. En un entorno de producción, deshabilite el servicio SSH que escucha en el puerto 22 y cierre el puerto 22.
80	TCP	(Opcional) Redirige a 443.

### Puertos salientes

Configure los puertos salientes necesarios.

**Tabla 8-3. Cantidad mínima de puertos salientes**

PUERTO	PROTOCOLO	COMENTARIOS
25, 587	TCP, UDP	SMTP para enviar correos electrónicos de notificación salientes.
53	TCP, UDP	DNS.
67, 68, 546, 547	TCP, UDP	DHCP.
110, 995	TCP, UDP	POP para recibir correos electrónicos de notificación entrantes.
143, 993	TCP, UDP	IMAP para recibir correos electrónicos de notificación entrantes.
443	TCP	Manager Service de infraestructura como servicio en HTTPS.

Si es necesario, configure puertos salientes opcionales.

**Tabla 8-4. Puertos salientes opcionales**

PUERTO	PROTOCOLO	COMENTARIOS
80	TCP	(Opcional) Para obtener actualizaciones de software. Puede descargar y aplicar las actualizaciones por separado.
123	TCP, UDP	(Opcional) Para conectarse directamente a NTP en lugar de usar la hora del host.

### Puertos de infraestructura como servicio

Como procedimiento de seguridad recomendado, configure los puertos entrantes y salientes de los componentes de infraestructura como servicio (Infrastructure as a Service, IaaS) según las directrices de VMware.

### Puertos entrantes

Configure la cantidad mínima de puertos entrantes necesaria para los componentes de IaaS.

**Tabla 8-5. Cantidad mínima de puertos entrantes necesaria**

COMPONENTE	PUERTO	PROTOCOLO	COMENTARIOS
Manager Service	443	TCP	Comunicación con los componentes de IaaS y el dispositivo de vRealize Automation en HTTPS. Todos los hosts de virtualización que administren agentes de proxy también deben tener el puerto TCP 443 abierto para el tráfico entrante.

**Puertos salientes**

Configure la cantidad mínima de puertos salientes necesaria para los componentes de IaaS.

**Tabla 8-6. Cantidad mínima de puertos salientes**

COMPONENTE	PUERTO	PROTOCOL O	COMENTARIOS
Todo	53	TCP, UDP	DNS.
Todo		TCP, UDP	DHCP.
Manager Service	443	TCP	Comunicación con el dispositivo de vRealize Automation en HTTPS.
Sitio web	443	TCP	Comunicación con Manager Service sobre HTTPS.
Distributed Execution Managers	443	TCP	Comunicación con Manager Service sobre HTTPS.
Agentes de proxy	443	TCP	Comunicación con Manager Service y con los hosts de virtualización sobre HTTPS.
Agente invitado	443	TCP	Comunicación con Manager Service sobre HTTPS.
Manager Service, sitio web	1433	TCP	MSSQL.

Si es necesario, configure puertos salientes opcionales.

**Tabla 8-7. Puertos salientes opcionales**

COMPONENTE	PUERTO	PROTOCOLO	COMENTARIOS
Todo	123	TCP, UDP	NTP es opcional.

## Auditoría y registro

Como procedimiento de seguridad recomendado, configure la auditoría y el registro en el sistema de vRealize Automation de acuerdo con las recomendaciones de VMware.

El registro remoto en un host de log central proporciona un almacén seguro para los archivos de log. Mediante la recopilación de archivos de log en un host central, puede supervisar el entorno con una sola herramienta. Además, puede realizar análisis agregados y buscar evidencias de amenazas, como ataques coordinados a varias entidades en la infraestructura. El inicio de sesión en un servidor de log centralizado y seguro puede ayudar a prevenir la adulteración de logs, además de proporcionar un registro de auditoría a largo plazo.

### Garantizar la seguridad del servidor de registro remoto

A menudo, después de que los atacantes vulneran la seguridad de la máquina host, intentan buscar y manipular los archivos de log para borrar su rastro y mantener el control sin ser descubiertos. La protección correcta del servidor de registro remoto permite impedir que se adulteren los logs.

### Utilizar un servidor NTP autorizado

Asegúrese de que todas las máquinas host usen el mismo origen de hora relativo, incluido el desfase de localización correspondiente, y que puedan relacionar el origen de hora relativo con un tiempo acordado estándar, como la hora universal coordinada (UTC). Un enfoque disciplinado en los orígenes de hora le permite realizar un seguimiento de las acciones de un intruso y relacionarlas de forma rápida al revisar los archivos de log pertinentes. Una configuración incorrecta de la hora puede dificultar la inspección y la correlación de los archivos de log a fin de detectar ataques; también puede hacer imprecisas las auditorías.

Utilice al menos tres servidores NTP de orígenes de hora externos, o bien configure algunos servidores NTP locales en una red de confianza que, a su vez, obtenga la hora de al menos tres orígenes de hora externos.