Configuración segura

vRealize Operations Manager 6.5

Este documento admite la versión de todos los productos enumerados y admite todas las versiones posteriores hasta que el documento se reemplace por una edición nueva. Para buscar ediciones más recientes de este documento, consulte http://www.vmware.com/es/support/pubs.

ES-002407-01

vmware®

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

http://www.vmware.com/es/support/

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

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

Contenido

Configuración segura

La finalidad de la documentación de *Configuración segura* es servir de base segura para la implementación de vRealize Operations Manager. Consulte este documento cuando utilice las herramientas de supervisión del sistema para asegurarse de que la configuración de base segura se supervisa y mantiene de forma continua ante los cambios inesperados.

Las actividades de protección que no están aún definidas de forma predeterminada se pueden ejecutar de forma manual.

Destinatarios

Esta información está dirigida a los administradores de vRealize Operations Manager.

Glosario de las publicaciones técnicas de VMware

Las publicaciones técnicas de VMware presentan un glosario de términos con los que es posible que no esté familiarizado. Para consultar las definiciones de términos tal cual se utilizan en la documentación técnica de VMware, diríjase a http://www.vmware.com/support/pubs.

Plan de seguridad de vRealize Operations Manager 1

El plan de seguridad de vRealize Operations Manager asume la existencia de un entorno seguro completo basado en la configuración del sistema y de la red, las políticas de seguridad de la organización y las recomendaciones. Es importante que lleve a cabo las actividades de protección según las políticas y las recomendaciones de seguridad de su organización.

Este documento se divide en las secciones siguientes:

- Implementación segura
- Configuración segura
- Seguridad de red
- Comunicación

En la guía se detalla la instalación de la aplicación virtual. No obstante, también se explica el siguiente tipo de implementación:

- "Implementación instalada en Linux," página 34

Para garantizar que el sistema está protegido de forma segura, consulte las recomendaciones y evalúelas según las políticas de seguridad y la exposición a riesgos de su organización.

Implementación segura de vRealize Operations Manager 2

Debe comprobar la integridad de los medios de instalación antes de instalar el producto para garantizar la autenticidad de los archivos descargados.

Este capítulo cubre los siguientes temas:

Comprobación de la integridad de los medios de instalación

Después de descargar los medios, utilice el valor de la suma MD5/SHA1 para comprobar la integridad de la descarga. Compruebe siempre el hash SHA1 después de descargar una imagen ISO, un paquete sin conexión o una revisión para asegurarse de la integridad y la autenticidad de los archivos descargados. Si VMware le proporciona medios físicos y el sello de seguridad está roto, devuelva el software a VMware para que lo cambien.

Procedimiento

- Compare la salida del hash MD5/SHA1 con el valor publicado en el sitio web de VMware.

  El hash SHA1 o MD5 debe coincidir.

  NOTA: Los archivos vRealize Operations Manager `6.x-x.pak` están firmados mediante el certificado de publicación de software de VMware. vRealize Operations Manager valida la firma del archivo PAK antes de la instalación.

Protección de la infraestructura de software implementada

Como parte del proceso de protección, debe proteger la infraestructura de software implementada donde se aloje su sistema VMware.

Antes de proteger su sistema VMware, examine y solucione cualquier deficiencia de seguridad que exista en la infraestructura de software de apoyo para crear un entorno seguro y completamente protegido. Entre los elementos de infraestructura de software que debe examinar se incluyen los componentes del sistema operativo, el software de apoyo y el 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.

Fortalecimiento del entorno de VMware vSphere

vRealize Operations Manager se basa en un entorno de VMware vSphere seguro para sacar el máximo partido y lograr una infraestructura segura.

Evalúe el entorno de VMware vSphere y compruebe si se respeta y mantiene el nivel de fortalecimiento adecuado según las directrices de fortalecimiento de vSphere.

Para obtener más información sobre el fortalecimiento, consulte http://www.vmware.com/security/hardening-guides.html.

Fortalecimiento para instalación en Linux

Revise las recomendaciones especificadas en las directrices de procedimientos recomendados de seguridad y protección de Linux correspondientes, y asegúrese de que sus hosts Linux disponen del fortalecimiento adecuado. Si no sigue las recomendaciones de fortalecimiento, es posible que el sistema quede expuesto a vulnerabilidades de seguridad conocidas procedentes de componentes inseguros de versiones de Linux.

Se admite la instalación de vRealize Operations Manager en Red Hat Enterprise Linux (RHEL) 6 a partir de la versión 6.5.

Revisión del software instalado y no compatible

Las vulnerabilidades en el software que no se utiliza pueden incrementar el riesgo de accesos no autorizados al sistema y de interrupción de la disponibilidad. Revise el software instalado en las máquinas host de VMware y evalúe su uso.

No instale ningún software que no sea necesario para el funcionamiento seguro del sistema en ninguno de los hosts de nodo de vRealize Operations Manager. Desinstale el software que no se utilice o que no sea esencial.

La instalación de software no compatible, sin probar o no aprobado en los productos de infraestructura, como vRealize Operations Manager, constituye una amenaza para la infraestructura.

Para minimizar la amenaza a la infraestructura, no instale ni use software de terceros no admitido por VMware en los hosts proporcionados por VMware.

Evalúe la implementación de vRealize Operations Manager y el inventario de los productos instalados para comprobar que no haya ningún software no compatible instalado.

Para obtener más información sobre las políticas de compatibilidad para productos de terceros, consulte la compatibilidad de VMware en http://www.vmware.com/security/hardening-guides.html.

Comprobación del software de terceros

No utilice software de terceros que no sea admitido por VMware. Compruebe que todo el software de terceros está configurado y revisado correctamente según las indicaciones del proveedor externo.

Las vulnerabilidades no auténticas, inseguras o sin revisar del software de terceros instalado en las máquinas host VMware exponen el sistema a riesgos de accesos no autorizados y puede provocar la interrupción de la disponibilidad. Se debe proteger y revisar de forma adecuada todo el software que no haya sido proporcionado por VMware.

Si debe usar software de terceros que no admitido por VMware, consulte al proveedor externo los requisitos de configuración y revisión seguras.

Avisos y revisiones de seguridad de VMware

En ocasiones VMware publica avisos y revisiones de seguridad de los productos. Conocer estos avisos puede garantizar que disponga del producto subyacente más seguro y que no sea vulnerable ante amenazas conocidas.

Evalúe la instalación, las revisiones y el historial de actualizaciones de vRealize Operations Manager, y compruebe que se han seguido y aplicado los avisos de seguridad publicados por VMware.

Se recomienda disponer siempre de la versión más reciente de vRealize Operations Manager, ya que también incluirá las correcciones de seguridad más recientes.

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

Configuración segura de vRealize Operations Manager 3

Como recomendación de seguridad, debe proteger la consola de vRealize Operations Manager y gestionar las cuentas administrativas de Secure Shell (SSH) y el acceso a la consola. Asegúrese de que el sistema se implementa con canales de transmisión segura.

También debe seguir determinadas recomendaciones de seguridad para ejecutar los agentes de Endpoint Operations Management.

Este capítulo cubre los siguientes temas:

Seguridad de la consola de vRealize Operations Manager

Después de instalar vRealize Operations Manager, deberá iniciar sesión por primera vez y proteger la consola de cada nodo del clúster.

Prerequisitos

Instale vRealize Operations Manager.

Procedimiento

1 Localice la consola del nodo en vCenter o mediante acceso directo.

En vCenter, pulse Alt+F1 para acceder a la solicitud de inicio de sesión. Por motivos de seguridad, las sesiones de terminales remotos de vRealize Operations Manager están deshabilitadas de manera predeterminada.

2 Inicie sesión como root.

vRealize Operations Manager no permite acceder al símbolo del sistema hasta que cree una contraseña raíz.

3 En la solicitud de contraseña, pulse **Intro**.

4 En la solicitud de contraseña anterior, pulse **Intro**.

5 En la solicitud de contraseña nueva, introduzca la contraseña raíz que desee y anótela para consultarla en el futuro.

6 Vuelva a introducir la contraseña raíz.

7 Cierre sesión en la consola.

Cambio de la contraseña raíz

Puede cambiar la contraseña raíz de cualquier nodo maestro o de datos de vRealize Operations Manager en cualquier momento mediante la consola.

El usuario root omite la comprobación de complejidad de contraseña de módulo `pam_cracklib`, que se encuentra en `etc/pam.d/common-password`. Todos los dispositivos protegidos habilitan `enforce_for_root` para el módulo `pw_history`, que se encuentra en el archivo `etc/pam.d/common-password`. De manera predeterminada, el sistema recuerda las cinco últimas contraseñas. Las contraseñas antiguas de cada usuario se almacenan en el archivo `/etc/security/opasswd`.

Prerequisitos

Compruebe que la contraseña raíz del dispositivo cumple los requisitos de complejidad de contraseña corporativa de su organización. Si la contraseña de la cuenta empieza por `$6$`, significa que usa un hash sha512. Se trata del hash estándar para todos los dispositivos protegidos.

Procedimiento

1 Ejecute el comando `# passwd` en el shell raíz del dispositivo.

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

Aparecerá la información del hash.

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

Gestión de la expiración de las contraseñas

Configure la expiración de todas las contraseñas de cuenta según las políticas de seguridad de su organización.

De forma predeterminada, todos los dispositivos VMware protegidos utilizan una expiración de contraseña de 60 días. En la mayoría de los dispositivos protegidos, la cuenta root tiene una expiración de contraseña de 365 días. Como recomendación, compruebe que la expiración de todas las cuentas cumple los estándares de requisitos de seguridad y funcionamiento.

Si la contraseña del usuario root expira, no podrá reactivarla. Deberá implementar políticas específicas del sitio para evitar que expiren las contraseñas administrativas y del usuario root.

Procedimiento

1 Inicie sesión en las máquinas de dispositivos virtuales como usuario root y ejecute el comando `# more /etc/shadow` para comprobar la expiración de la contraseña en todas las cuentas.

2 Para modificar la expiración de la cuenta root, ejecute el comando `# passwd –x 365 root`.

   En este comando, 365 especifica el número de días hasta la expiración de la contraseña. Utilice el mismo comando para modificar cualquier usuario, sustituyendo la cuenta específica de `root` y reemplazando el número de días para cumplir las normas de expiración de la organización.

   De manera predeterminada, la contraseña del usuario root está establecida en 365 días.

Gestión de Secure Shell, cuentas administrativas y acceso a la consola

Para las conexiones remotas, todos los dispositivos protegidos incluyen el protocolo Secure Shell (SSH). SSH está deshabilitado de forma predeterminada en el dispositivo protegido.

SSH es un entorno interactivo de línea de comandos que admite conexiones remotas a un nodo de vRealize Operations Manager. SSH necesita credenciales de cuenta de usuario con privilegios elevados. En general, las actividades de SSH omiten el control de acceso basado en funciones (RBAC) y los controles de auditoría del nodo de vRealize Operations Manager.

Como recomendación, deshabilite SSH en un entorno de producción y habilítelo solo para diagnosticar o solucionar problemas que no se puedan resolver por otros medios. Déjelo habilitado solo mientras sea necesario para una finalidad específica y según las políticas de seguridad de su organización. Si habilita SSH, asegúrese de que está protegido contra los ataques y que lo habilita solamente mientras sea necesario. Según la configuración de vSphere, puede habilitar o deshabilitar SSH cuando se implementa la plantilla OVF (Open Virtualization Format, formato de virtualización abierto).

Una prueba sencilla para determinar si SSH está habilitado en una máquina es intentar abrir una conexión mediante SSH. Si la conexión se abre y solicita credenciales, significa que SSH está habilitado y disponible para establecer conexiones.

Usuario root de Secure Shell

Como los dispositivos de VMware no incluyen cuentas de usuario predeterminadas ya configuradas, la cuenta root puede usar SSH directamente para iniciar sesión de manera predeterminada. Deshabilite SSH como usuario root lo antes posible.

Para cumplir los estándares para evitar el rechazo, el servidor SSH está preconfigurado en todos los dispositivos protegidos con la entrada wheel para restringir el acceso de SSH al grupo wheel secundario. Para separar las obligaciones, puede modificar la entrada wheel de 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 el acceso de superusuario, por lo que los miembros del grupo wheel pueden usar el comando su-root, en el cual se precisa la contraseña raíz. La separación de grupos permite a los usuarios usar SSH en el dispositivo, pero no el comando "su" para iniciar sesión como usuario raíz. No elimine ni modifique otras entradas del campo AllowGroups, lo que garantiza el funcionamiento correcto del dispositivo. Después de realizar un cambio, ejecute el comando `# service sshd restart` para reiniciar el daemon SSH.

Activación o desactivación de Secure Shell en un nodo de vRealize Operations Manager

Puede activar Secure Shell (SSH) en un nodo de vRealize Operations Manager para solucionar problemas. Por ejemplo, para solucionar un problema en un servidor, es posible que la consola necesite acceder al servidor. Esta acción se lleva a cabo mediante SSH. Desactive SSH en un nodo de vRealize Operations Manager para el funcionamiento habitual.

Procedimiento

1 Acceda a la consola del nodo de vRealize Operations Manager desde vCenter.

2 Pulse Alt + F1 para acceder a la solicitud de inicio de sesión y, a continuación, inicie sesión.

3 Ejecute el comando `#chkconfig`.

4 Si el servicio sshd está desactivado, ejecute el comando `#chkconfig sshd on`.

5 Ejecute el comando `#service sshd start` para iniciar el servicio sshd.

6 Ejecute el comando `#service sshd stop` para detener el servicio sshd.

Creación de una cuenta administrativa local para Secure Shell

Debe crear cuentas administrativas locales que se puedan utilizar como Secure Shell (SSH) y que sean miembros del grupo "wheel" secundario antes de eliminar el acceso SSH raíz.

Antes de desactivar el acceso raíz directo, pruebe si los administradores autorizados pueden acceder a SSH `AllowGroups`, y si pueden utilizar el grupo "wheel" y el comando `su` para iniciar sesión como raíz.

Procedimiento

1 Inicie sesión como raíz y ejecute los siguientes comandos.

```
# useradd –d /home/vropsuser –g users –G wheel –m
# passwd username
```

El grupo "wheel" es el que se especifica en el campo `AllowGroups` para el acceso SSH. Para añadir varios grupos secundarios, utilice `–G wheel,sshd`.

2 Cambie de usuario y proporcione una nueva contraseña para garantizar la comprobación de la complejidad de la contraseña.

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

Si se cumplen los criterios de complejidad de la contraseña, la contraseña se actualizará. En caso contrario, la contraseña volverá a la contraseña anterior y deberá ejecutar de nuevo el comando "password".

Después de crear las cuentas de inicio de sesión para permitir el acceso remoto SSH y utilizar el comando `su` para iniciar sesión como raíz mediante el acceso al grupo "wheel", podrá eliminar la cuenta raíz desde el inicio de sesión directo a SSH.

3 Para eliminar el inicio de sesión directo a SSH, modifique el archivo `/etc/ssh/sshd_config`. Para ello, sustituya `(#)PermitRootLogin yes` por `PermitRootLogin no`.

Qué hacer a continuación

Desactive los inicios de sesión directos como raíz. De forma predeterminada, los dispositivos protegidos permiten el inicio de sesión directo a raíz a través de la consola. Después de crear las cuentas administrativas para evitar el rechazo y probar si permiten el acceso al grupo "wheel" (`su–root`), desactive los inicios de sesión directos como raíz. Para ello, edite el archivo `/etc/securetty` como usuario raíz y sustituya la entrada `tty1` por `console`.

Restricción del acceso a Secure Shell

Como parte del proceso de protección del sistema, restrinja el acceso de Secure Shell (SSH) mediante la configuración del paquete tcp_wrappers de forma adecuada en todas las máquinas host de dispositivo virtual de VMware. Mantenga también los permisos del archivo de claves de SSH necesarios en los dispositivos.

Todos los dispositivos virtuales de VMware incluyen el paquete tcp_wrappers para permitir que los daemons compatibles con tcp controlen las subredes a las que pueden acceder los daemons incluidos en bibliotecas. De forma predeterminada, el archivo `/etc/hosts.allow` contiene una entrada genérica, `sshd: ALL : ALLOW`, que permite todo el acceso a Secure Shell. Restrinja este acceso según corresponda para su organización.

Procedimiento

1 Abra el archivo `/etc/hosts.allow` en la máquina host del dispositivo virtual en un editor de texto.

2 Cambie la entrada genérica del entorno de producción para incluir únicamente las entradas de host local y la subred de gestión para las 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 establezcan en la subred 10.0.0.0.

3 Añada la identificación de máquina adecuada, por ejemplo, nombre de host, dirección IP, nombre de dominio completo (FQDN) y loopback.

4 Guarde el archivo y ciérrelo.

Mantenimiento de los permisos de archivos de claves de Secure Shell

Para mantener un nivel de seguridad adecuado, configure los permisos de archivo de claves de Secure Shell (SSH).

Procedimiento

1 Los archivos de claves públicas de host se encuentran en `/etc/ssh/*key.pub`.

2 Compruebe que estos archivos son propiedad del usuario root, que el grupo sea propiedad del usuario root y que los archivos tengan los permisos establecidos en 0644.

Los permisos son (-rw-r--r--).

3 Cierre todos los archivos.

4 Los archivos de claves privadas del host se encuentran en `/etc/ssh/*key`.

5 Compruebe que el usuario root es el propietario de los archivos y del grupo, y que los archivos tengan los permisos establecidos en 0600.

Los permisos son (-rw-------).

6 Cierre todos los archivos.

Protección de la configuración del servidor de Secure Shell

Siempre que es posible, la instalación de la aplicación virtual (Virtual Application Installation, OVF) ofrece una configuración de protección predeterminada. Los usuarios pueden examinar el servidor y el servicio cliente en la sección de opciones globales del archivo de configuración para comprobar si sus configuraciones disponen de la protección adecuada.

Siempre que sea posible, limite el uso del servidor de SSH a una subred de gestión en el archivo `/etc/hosts.allow`.

Procedimiento

1 Abra el archivo de configuración de servidor `/etc/ssh/sshd_config` y compruebe si los ajustes son correctos.

Configuración	Estado
Protocolo de daemon de servidor	Protocolo 2
Claves de cifrado	Claves de cifrado aes256-ctr,aes128-ctr
Reenvío TCP	Permitir reenvío TCP no
Puertos de puerta de enlace de servidor	Puertos de puerta de enlace no
Reenvío X11	Reenvío X11 no
Servicio SSH	Utilice el campo Permitir grupos y especifique un grupo con permiso para acceder y añadir miembros al grupo secundario para los usuarios con permiso para utilizar el servicio.
Autenticación GSSAPI	Autenticación GSSAPI no, si no está en uso
Autenticación Kerberos	Autenticación Kerberos no, si no está en uso
Variables locales (opción global AcceptEnv)	Fije este ajuste en `desactivado por comentario` o `activado solo para variables LC_* o LANG`
Configuración de túnel	Permitir túnel no
Sesiones de red	Sesiones máx. 1
Comprobación en modo strict	Modos strict sí
Separación de privilegios	Utilizar separación de privilegios sí
Autenticación rhosts RSA	Autenticación rhosts RSA no
Compresión	Compresión retrasada o Compresión no
Código de autenticación de mensajes	MACs hmac-sha1
Restricción de acceso de usuarios	Permitir entorno de usuarios no

2 Guarde los cambios y cierre el archivo.

Protección de la configuración del cliente de Secure Shell

Como parte del proceso de supervisión de la protección de su sistema, compruebe la protección del cliente de SSH. Para ello, examine el archivo de configuración del cliente de SSH en las máquinas host de dispositivo virtual para asegurarse de que están configuradas de acuerdo con las directrices de VMware.

Procedimiento

1 Abra el archivo de configuración del cliente de SSH, `/etc/ssh/ssh_config`, y compruebe si los ajustes de la sección de opciones globales son correctos.

Configuración	Estado
Protocolo de cliente	Protocolo 2
Puertos de puerta de enlace de cliente	Puertos de puerta de enlace no
Autenticación GSSAPI	Autenticación GSSAPI no
Variables locales (opción global SendEnv)	Proporcionar únicamente variables LC_* o LANG
Claves de cifrado CBC	Claves de cifrado aes256-ctr,aes128-ctr
Códigos de autenticación de mensajes	Solo se utiliza en la entrada `MACs hmac-sha1`

2 Guarde los cambios y cierre el archivo.

Desactivación de inicios de sesión directos como raíz

De forma predeterminada, los dispositivos protegidos permiten utilizar la consola para iniciar sesión directamente como raíz. Como procedimiento de seguridad recomendado, puede desactivar los inicios de sesión directos después de crear una cuenta administrativa para evitar el rechazo y probar si permite acceso al grupo "wheel" mediante el comando `su-root`.

Prerequisitos

- Realice los pasos que se indican en el tema llamado "Creación de una cuenta administrativa local para Secure Shell," página 16.
- Compruebe que se ha probado el acceso al sistema como administrador antes de desactivar los inicios de sesión raíz directos.

Procedimiento

1 Inicie sesión como raíz y desplácese hasta el archivo `/etc/securetty`.

Puede acceder a este archivo desde la línea de comandos.

2 Sustituya la entrada `tty1` por `console`.

Desactivación del acceso SSH a la cuenta de usuario admin

Como recomendación de seguridad, puede deshabilitar el acceso SSH a la cuenta de usuario admin. La cuenta admin de vRealize Operations Manager y la cuenta admin de Linux comparten la misma contraseña. La desactivación del acceso SSH al usuario admin impone una protección en profundidad asegurando que todos los usuarios de SSH inicien primero sesión en una cuenta de servicio con menos privilegios con una contraseña que difiere de la de la cuenta admin de vRealize Operations Manager y, a continuación, cambiando el usuario a un privilegio mayor como admin o raíz.

Procedimiento

1 Edite el archivo `/etc/ssh/sshd_config`.

  Puede acceder a este archivo desde la línea de comandos.

2 Añada la entrada `DenyUsers admin` a cualquier parte del archivo y guarde el archivo.

3 Para reiniciar el servidor sshd, ejecute el comando `service sshd restart`.

Configuración de la autenticación del cargador de arranque

Para ofrecer un nivel de seguridad apropiado, 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 de consola al sistema podrían modificar la configuración de arranque del sistema o arrancar el sistema en modo de un solo usuario o de mantenimiento, lo que puede provocar la denegación de servicio o un acceso no autorizado al sistema.

Como la autenticación del cargador de arranque no está configurada de forma predeterminada en los dispositivos virtuales de VMware, deberá crear una contraseña GRUB para configurarla.

Procedimiento

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

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

  Se generará una contraseña MD5 y el comando proporcionará la salida del hash md5.

3 Añada la contraseña al archivo `menu.lst` mediante la ejecución del comando `# password --md5 <hash from grub-md5-crypt>`.

Autenticación del modo de usuario individual o de mantenimiento

Si el sistema no necesita una autenticación de usuario raíz válida antes de iniciar el modo de usuario individual o de mantenimiento, a cualquier usuario que invoque el modo de usuario individual o de mantenimiento se le concederá acceso a todos los archivos del sistema.

Procedimiento

- Consulte el archivo `/etc/inittab` y compruebe que aparecen las dos líneas siguientes: `ls:S:wait:/etc/init.d/rc S` y `~~:S:respawn:/sbin/sulogin`.

Supervisión de la cantidad mínima de cuentas de usuario necesarias

Debe supervisar las cuentas de usuario existentes y asegurarse de eliminar las innecesarias.

Procedimiento

- Ejecute el comando *host*`:~ # cat /etc/passwd` y compruebe la cantidad mínima de cuentas de usuario necesarias:

```
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
haldaemon:x:101:102:User for haldaemon:/var/run/hald:/bin/false
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
messagebus:x:100:101:User for D-Bus:/var/run/dbus:/bin/false
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
ntp:x:74:106:NTP daemon:/var/lib/ntp:/bin/false
polkituser:x:103:104:PolicyKit:/var/run/PolicyKit:/bin/false
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
root:x:0:0:root:/root:/bin/bash
sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false
suse-ncc:x:104:107:Novell Customer Center User:/var/lib/YaST2/suse-ncc-fakehome:/bin/bash
uuidd:x:102:103:User for uuidd:/var/run/uuidd:/bin/false
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
nginx:x:105:108:user for nginx:/var/lib/nginx:/bin/false
admin:x:1000:1003::/home/admin:/bin/bash
tcserver:x:1001:1004:tc Server User:/home/tcserver:/bin/bash
postgres:x:1002:100::/var/vmware/vpostgres/9.3:/bin/bash
```

Supervisión de la cantidad mínima de grupos necesarios

Debe supervisar los grupos y los miembros existentes para asegurarse de que se eliminan los grupos o los accesos a grupo innecesarios.

Procedimiento

- Ejecute el comando `<host>:~ # cat /etc/group` para comprobar la cantidad mínima de grupos y pertenencia a grupo necesarios.

```
audio:x:17:
bin:x:1:daemon
cdrom:x:20:
console:x:21:
daemon:x:2:
dialout:x:16:u1,tcserver,postgres
disk:x:6:
floppy:x:19:
haldaemon:!:102:
kmem:x:9:
mail:x:12:
man:x:62:
messagebus:!:101:
modem:x:43:
nobody:x:65533:
nogroup:x:65534:nobody
ntp:!:106:
polkituser:!:105:
```

```
public:x:32:
root:x:0:admin
shadow:x:15:
sshd:!:65:
suse-ncc:!:107:
sys:x:3:
tape:!:103:
trusted:x:42:
tty:x:5:
utmp:x:22:
uuidd:!:104:
video:x:33:u1,tcserver,postgres
wheel:x:10:root,admin
www:x:8:
xok:x:41:
maildrop:!:1001:
postfix:!:51:
users:x:100:
vami:!:1002:root
nginx:!:108:
admin:!:1003:
vfabric:!:1004:admin,wwwrun
```

Restablecimiento de la contraseña de administrador de vRealize Operations Manager (Linux)

Como recomendación de seguridad, puede restablecer la contraseña de vRealize Operations Manager en los clústeres Linux para instalaciones de vApp o Linux.

Procedimiento

1 Inicie sesión en la consola remota del nodo principal como usuario raíz.

2 Introduzca el comando `$VMWARE_PYTHON_BIN $VCOPS_BASE/../vmware-vcopssuite/utilities/sliceConfiguration/bin/vcopsSetAdminPassword.py --reset` y siga las indicaciones.

Configuración NTP en dispositivos de VMware

Para un abastecimiento de tiempo importante, desactive la sincronización de tiempo del host y utilice Network Time Protocol (Protocolo de tiempo de redes, NTP) en los dispositivos de VMware. Debe configurar un servidor NTP remoto de confianza para el proceso de sincronización de hora. El servidor NTP debe ser un servidor de hora autoritativo o, al menos, estar sincronizado con uno.

El daemon NTP de los dispositivos virtuales de VMware proporciona servicios de tiempo sincronizados. NTP se encuentra desactivado de forma predeterminada, por lo que deberá configurarlo manualmente. Si es posible, utilice NTP en entornos de producción para realizar el seguimiento de las acciones de los usuarios y detectar posibles intrusiones y ataques malintencionados mediante una exhausta auditoría y el mantenimiento de registros. 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 el archivo `/etc/ntp.conf` de cada dispositivo.

Procedimiento

1 Desplácese hasta el archivo de configuración `/etc/ntp.conf` de su máquina host de dispositivo virtual.

2 Defina la propiedad del archivo en **`root:root`**

3 Defina los permisos en **0640**.

4 Para reducir el riesgo de un ataque de amplificación de denegación de servicio en el servicio NTP, abra el archivo `/etc/ntp.conf` y asegúrese de que las líneas de restricción aparecen 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.

Para obtener información sobre los avisos de seguridad de NTP, consulte http://support.ntp.org/bin/view/Main/SecurityNotice.

Desactivación de la respuesta de marca de hora TCP en Linux

Utilice la respuesta de marca de hora TCP para aproximarse al tiempo activo del host remoto y como ayuda en futuros ataques. Además, algunos sistemas operativos pueden dejar huellas en la memoria en función del comportamiento de sus marcas de hora TCP.

Procedimiento

- Desactive la respuesta de marca de hora TCP en Linux.
  a Para fijar el valor de `net.ipv4.tcp_timestamps` en `0`, ejecute el comando `sysctl –w net.ipv4.tcp_timestamps=0`.
  b Añada el valor `ipv4.tcp_timestamps=0` en el archivo `sysctl.conf` predeterminado.

Activación del modo FIPS 140-2

La versión de OpenSSL que se proporciona con vRealize Operations Manager 6.3 y versiones posteriores dispone de certificado FIPS 140-2. Sin embargo, el modo FIPS no está activado de forma predeterminada.

Puede activar el modo FIPS si existe un requisito de cumplimiento de normas de seguridad para utilizar algoritmos criptográficos con certificación FIPS con el modo FIPS habilitado.

Procedimiento

1 Para reemplazar el archivo `mod_ssl.so`, ejecute el siguiente comando:

```
cd /usr/lib64/apache2–prefork/
cp mod_ssl.so mod_ssl.so.old
cp mod_ssl.so.FIPSON.openssl1.0.2 mod_ssl.so
```

2 Modifique su configuración de Apache2. Para ello, edite el archivo `/etc/apache2/ssl–global.conf`.

3 Busque la línea `<IfModule mod_ssl.c>` y añada la directiva `SSLFIPS on` a continuación de esta.

4 Para restablecer la configuración de Apache, ejecute el comando `service apache2 restart`.

TLS para datos en transferencia

Como recomendación de seguridad, asegúrese de que el sistema se ha implementado con canales de transmisión segura.

Configuración de protocolos estrictos para vRealize Operations Manager

Los protocolos SSLv2 y SSLv3 han dejado de considerarse seguros. Se recomienda que deshabilite TLS 1.0, y habilite únicamente TLS 1.1 y TLS 1.2.

Comprobación del uso correcto de los protocolos en Apache HTTPD

vRealize Operations Manager desactiva SSLv2 y SSLv3 de forma predeterminada. Debe deshabilitar los protocolos débiles en todos los equilibradores de carga antes de poner el sistema en producción.

Procedimiento

1 Ejecute el comando `grep SSLProtocol /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf | grep -v '#'` del símbolo del sistema para comprobar que SSLv2 y SSLv3 están deshabilitados.

Si los protocolos están deshabilitados, el comando devolverá el siguiente resultado: `SSLProtocol All -SSLv2 -SSLv3`

2 Para deshabilitar también el protocolo TLS 1.0, ejecute el comando `sed -i "/^[^#]*SSLProtocol/c\SSLProtocol All -SSLv2 -SSLv3 -TLSv1" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` del símbolo del sistema.

3 Para reiniciar el servidor Apache2, ejecute el comando `/etc/init.d/apache2 restart` del símbolo del sistema.

Comprobación del uso correcto de los protocolos en el Handler GemFire TLS

vRealize Operations Manager deshabilita SSLv3 de forma predeterminada. Debe deshabilitar los protocolos débiles en todos los equilibradores de carga antes de poner el sistema en producción.

Procedimiento

1 Compruebe que los protocolos están habilitados. Para comprobarlo, ejecute los siguientes comandos en cada uno de los nodos:

```
grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.properties | grep -v '#'
```

Debería aparecer el siguiente resultado:

```
cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1
grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.native.properties | grep -v '#'
```

Debería aparecer el siguiente resultado:

```
cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1
grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties | grep -v '#'
```

Debería aparecer el siguiente resultado:

```
cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1
```

2 Deshabilite TLS 1.0.

a Vaya a la interfaz de usuario del administrador en `url/admin`.

b Haga clic en **Desconectar**.

c Para deshabilitar SSLv3 y TLS 1.0, ejecute los siguientes comandos:

```
sed –i "/^[^#]*cluster–ssl–protocol/ c\cluster–ssl–protocols=TLSv1.2
TLSv1.1" /usr/lib/vmware–vcops/user/conf/gemfire.properties
sed –i "/^[^#]*cluster–ssl–protocol/ c\cluster–ssl–protocols=TLSv1.2
TLSv1.1" /usr/lib/vmware–vcops/user/conf/gemfire.native.properties
sed –i "/^[^#]*cluster–ssl–protocol/ c\cluster–ssl–protocols=TLSv1.2
TLSv1.1" /usr/lib/vmware–vcops/user/conf/gemfire.locator.properties
```

Repita este paso para cada nodo

d Vaya a la interfaz de usuario del administrador.

e Haga clic en **Conectar**.

3 Vuelva a habilitar TLS 1.0.

a Vaya a la interfaz de usuario del administrador para desconectar el clúster: `url/admin`.

b Haga clic en **Desconectar**.

c Para garantizar que SSLv3 y TLS 1.0 están deshabilitados, ejecute los siguientes comandos:

```
sed –i "/^[^#]*cluster–ssl–protocol/ c\cluster–ssl–protocols=TLSv1.2 TLSv1.1
TLSv1" /usr/lib/vmware–vcops/user/conf/gemfire.properties
sed –i "/^[^#]*cluster–ssl–protocol/ c\cluster–ssl–protocols=TLSv1.2 TLSv1.1
TLSv1" /usr/lib/vmware–vcops/user/conf/gemfire.native.properties
sed –i "/^[^#]*cluster–ssl–protocol/ c\cluster–ssl–protocols=TLSv1.2 TLSv1.1
TLSv1" /usr/lib/vmware–vcops/user/conf/gemfire.locator.properties
```

Repita este paso en cada uno de los nodos.

d Vaya a la interfaz de usuario del administrador para conectar el clúster.

e Haga clic en **Conectar**.

Configuración de vRealize Operations Manager para que utilice claves de cifrado seguras

Para la máxima seguridad, debe configurar los componentes de vRealize Operations Manager para que utilicen claves de cifrado seguras. Para garantizar que solo se seleccionan claves de cifrado seguras, debe desactivar el uso de claves de cifrado no seguras. Configure el servidor para que solo admita claves de cifrado seguras; debe utilizar claves con una longitud suficiente. Además, configure las claves de cifrado en un orden adecuado.

De forma predeterminada, vRealize Operations Manager deshabilita el uso de conjuntos de claves de cifrado mediante el intercambio de claves DHE. Asegúrese de deshabilitar los conjuntos de claves de cifrado en todos los equilibradores de carga antes de poner el sistema en producción.

Uso de claves de cifrado seguras

Las claves de cifrado negociadas entre el servidor y el navegador determinan el método de intercambio de claves y la seguridad del cifrado que se utiliza durante una sesión TLS.

Comprobación del uso correcto de los conjuntos de claves de cifrado en Apache HTTPD

Para disfrutar de la máxima seguridad, compruebe que se están utilizando correctamente los conjuntos de claves de cifrado en Apache HTTPD.

Procedimiento

1 Para comprobar el correcto uso de los conjuntos de claves de cifrado en Apache HTTPD, ejecute el comando `grep SSLCipherSuite /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf | grep -v '#'` del símbolo del sistema.

En caso de que Apache HTTPD emplee los conjuntos de claves de cifrado correctos, el comando devolverá el siguiente resultado: `SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH +AES:ECDH+AES:RSA+AES:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH`

2 Para configurar el uso correcto de los conjuntos de claves de cifrado, ejecute el comando `sed -i "/^[^#]*SSLCipherSuite/ c\SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH +AES:RSA+AES:\!aNULL\!ADH:\!EXP:\!MD5:\!3DES:\!CAMELLIA:\!PSK:\!SRP:\!DH" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` del símbolo del sistema.

Ejecute este comando si el resultado del Paso 1 no es el esperado.

Este comando deshabilita todos los conjuntos de claves de cifrado que utilizan métodos de intercambio de claves DH y DHE.

3 Ejecute el comando `/etc/init.d/apache2 restart` del símbolo del sistema para reiniciar el servidor Apache2.

4 Para volver a habilitar DH, elimine `!DH` de los conjuntos de claves de cifrado ejecutando el comando `sed -i "/^[^#]*SSLCipherSuite/ c\SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH +AES:ECDH+AES:RSA+AES:\!aNULL\!ADH:\!EXP:\!MD5:\!3DES:\!CAMELLIA:\!PSK:\! SRP" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` del símbolo del sistema.

5 Ejecute el comando `/etc/init.d/apache2 restart` del símbolo del sistema para reiniciar el servidor Apache2.

Comprobación del uso correcto de los conjuntos de claves de cifrado en el Handler GemFire TLS

Para disfrutar de la máxima seguridad, compruebe que se están utilizando correctamente los conjuntos de claves de cifrado en el Handler GemFire TLS.

Procedimiento

1 Para comprobar que los conjuntos de claves de cifrado están habilitados, ejecute los siguientes comandos en los nodos para verificar que los protocolos están activados:

```
grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/gemfire.properties | grep -v '#'

grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/gemfire.native.properties | grep -v '#'

grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties | grep -v '#'
```

2 Configure los conjuntos de claves de cifrado correspondientes.

a Vaya a la interfaz de usuario del administrador en *URL*`/admin`.

b Haga clic en **Desconectar** para desconectar el clúster.

c Para configurar los conjuntos de claves de cifrado correspondientes, ejecute los siguientes comandos:

```
sed –i "/^[^#]*cluster–ssl–ciphers/ c\cluster–ssl–
ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware–
vcops/user/conf/gemfire.properties

sed –i "/^[^#]*cluster–ssl–ciphers/ c\cluster–ssl–
ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware–
vcops/user/conf/gemfire.native.properties

sed –i "/^[^#]*cluster–ssl–ciphers/ c\cluster–ssl–
ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware–
vcops/user/conf/gemfire.locator.properties
```

Repita este paso en cada uno de los nodos.

d Vaya a la interfaz de usuario del administrador en *URL*`/admin`.

e Haga clic en **Conectar**.

Recursos de aplicación que se deben proteger

Como recomendación de seguridad, asegúrese de que los recursos de aplicación estén protegidos.

Siga los pasos para asegurarse de que los recursos de aplicación están protegidos.

Procedimiento

1 Ejecute el comando `Find / –path /proc –prune –o –type f –perm +6000 –ls` para verificar que los archivos tienen un conjunto de bits SUID y GUID bien definido.

Aparecerá la siguiente lista:

```
354131   24 –rwsr–xr–x   1 polkituser root 23176 /usr/lib/PolicyKit/polkit–set–default–helper
354126   20 –rwxr–sr–x   1 root     polkituser    19208 /usr/lib/PolicyKit/polkit–grant–
helper
354125   20 –rwxr–sr–x   1 root     polkituser    19008 /usr/lib/PolicyKit/polkit–explicit–
grant–helper
354130   24 –rwxr–sr–x   1 root     polkituser    23160 /usr/lib/PolicyKit/polkit–revoke–
helper
354127   12 –rwsr–x–––   1 root     polkituser    10744 /usr/lib/PolicyKit/polkit–grant–
helper–pam
354128   16 –rwxr–sr–x   1 root     polkituser    14856 /usr/lib/PolicyKit/polkit–read–auth–
helper
 73886   84 –rwsr–xr–x   1 root     shadow      77848 /usr/bin/chsh
 73888   88 –rwsr–xr–x   1 root     shadow      85952 /usr/bin/gpasswd
 73887   20 –rwsr–xr–x   1 root     shadow      19320 /usr/bin/expiry
 73890   84 –rwsr–xr–x   1 root     root        81856 /usr/bin/passwd
 73799  240 –rwsr–xr–x   1 root     root       238488 /usr/bin/sudo
 73889   20 –rwsr–xr–x   1 root     root        19416 /usr/bin/newgrp
 73884   92 –rwsr–xr–x   1 root     shadow      86200 /usr/bin/chage
 73885   88 –rwsr–xr–x   1 root     shadow      82472 /usr/bin/chfn
 73916   40 –rwsr–x–––   1 root     trusted     40432 /usr/bin/crontab
296275   28 –rwsr–xr–x   1 root     root        26945 /usr/lib64/pt_chown
353804  816 –r–xr–sr–x   1 root     mail       829672 /usr/sbin/sendmail
278545   36 –rwsr–xr–x   1 root     root        35792 /bin/ping6
278585   40 –rwsr–xr–x   1 root     root        40016 /bin/su
278544   40 –rwsr–xr–x   1 root     root        40048 /bin/ping
278638   72 –rwsr–xr–x   1 root     root        69240 /bin/umount
```

```
278637  100 -rwsr-xr-x   1 root     root        94808 /bin/mount
475333   48 -rwsr-x---   1 root     messagebus    47912 /lib64/dbus-1/dbus-daemon-launch-
helper
 41001   36 -rwsr-xr-x   1 root     shadow      35688 /sbin/unix_chkpwd
 41118   12 -rwsr-xr-x   1 root     shadow      10736 /sbin/unix2_chkpwd
```

2 Ejecute el comando `find / -path */proc -prune -o -nouser -o -nogroup` para comprobar que todos los archivos de vApp tienen un propietario.

Si no se obtiene ningún resultado, todos los archivos tienen un propietario.

3 Ejecute el comando `find / -name "*.*" -type f -perm -a+w | xargs ls -ldb` para verificar que el entorno no tiene acceso de escritura a ninguno de los archivos; para ello, revise los permisos de todos los archivos de vApp.

Ninguno de los archivos debe incluir el permiso `xx2`.

4 Ejecute el comando `find / -path */proc -prune -o ! -user root -o -user admin -print` para verificar que los archivos son propiedad del usuario correcto.

Si no se obtiene ningún resultado, todos los archivos pertenecen a `root` o `admin`.

5 Ejecute el comando `find /usr/lib/vmware-casa/ -type f -perm -o=w` para asegurarse de que el entorno no tiene acceso de escritura a los archivos del directorio `/usr/lib/vmware-casa/`.

No se deben obtener resultados.

6 Ejecute el comando `find /usr/lib/vmware-vcops/ -type f -perm -o=w` para asegurarse de que el entorno no tiene acceso de escritura a los archivos del directorio `/usr/lib/vmware-vcops/`.

No se deben obtener resultados.

7 Ejecute el comando `find /usr/lib/vmware-vcopssuite/ -type f -perm -o=w` para asegurarse de que el entorno no tiene acceso de escritura en los archivos del directorio `/usr/lib/vmware-vcopssuite/`.

No se deben obtener resultados.

Configuración de la autenticación del cliente de PostgreSQL

Puede configurar el sistema para la autenticación de cliente. Puede configurar el sistema para la autenticación de confianza local. Esto permite que cualquier usuario local, incluido el superusario de la base de datos, se conecte como un usuario de PostgreSQL sin una contraseña. Si desea proporcionar una defensa sólida y no tiene un nivel de confianza significativo en todas las cuentas de usuario locales, utilice otro método de autenticación. El método md5 está configurado de forma predeterminada. Compruebe que md5 está configurado para todas las conexiones locales y de host.

Encontrará las opciones de configuración de autenticación de cliente de la instancia del servicio de postgres en `/storage/db/vcops/vpostgres/data/pg_hba.conf`. Compruebe que md5 está configurado para todas las conexiones locales y de host.

Las opciones de configuración de autenticación de cliente de la instancia del servicio postgres-repl se pueden encontrar en `/storage/db/vcops/vpostgres/repl/pg_hba.conf`. Compruebe que md5 está configurado para todas las conexiones locales y de host.

NOTA: No modifique las opciones de configuración del cliente para la cuenta de usuario de postgres.

Configuración de Apache

Deshabilitar la exploración del directorio web

Como recomendación de seguridad, asegúrese de que un usuario no puede explorar un directorio, ya que puede aumentar el riesgo de exposición a los ataques transversales de directorio.

Procedimiento

- Compruebe que la exploración de directorios está deshabilitada en todos los directorios.
  a. Abra los archivos `/etc/apache2/default-server.conf` y `/usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` en un editor de textos.
  b. Compruebe que por cada lista `<Directorio>`, la opción llamada `Indexes` para la etiqueta correspondiente se omite de la línea `Options`.

Eliminación del código de muestra para el servidor Apache2

Apache incluye dos scripts para la interfaz de entrada común (Common Gateway Interface, CGI) de muestra, `printenv` y `test-cgi`. Un servidor web de producción solo debería contener componentes que resulten indispensables para un correcto funcionamiento. Estos componentes pueden revelar a un atacante información crítica sobre el sistema.

Como recomendación de seguridad, es recomendable que elimine los scripts para la CGI del directorio `cgi-bin`.

Procedimiento

- Para eliminar los scripts `test-cgi` y `prinenv`, ejecute los comandos `rm /usr/share/doc/packages/apache2/test-cgi` y `rm /usr/share/doc/packages/apache2/printenv`.

Comprobación de los tokens de servidor para el servidor Apache2

Como parte del proceso de protección del sistema, le recomendamos que compruebe los tokens de servidor para el servidor Apache2. El encabezado de respuesta web de una respuesta HTTP puede contener varios campos. Esta información incluye la página HTML solicitada, el tipo y la versión del servidor web, el sistema operativo y su versión, además de los puertos asociados a dicho servidor web. Esta información proporciona a los usuarios malintencionados datos importantes sin necesidad de utilizar herramientas adicionales.

La directiva `ServerTokens` debe estar definida en `Prod`. Por ejemplo, `ServerTokens Prod`. Los controles de directiva del campo de encabezado de respuesta del servidor que se reenvía a los clientes incluye una descripción del sistema operativo e información sobre los módulos integrados.

Procedimiento

1. Para verificar los tokens de servidor, ejecute el comando `cat /etc/apache2/sysconfig.d/global.conf | grep ServerTokens`.
2. Para cambiar `ServerTokens OS` a `ServerTokens Prod`, ejecute el comando `sed -i 's/\(ServerTokens\s\+\)OS/\1Prod/g' /etc/apache2/sysconfig.d/global.conf`.

Deshabilitación del modo de seguimiento en el servidor Apache2

En las operaciones de producción estándar, el uso de herramientas de diagnóstico puede identificar vulnerabilidades no detectadas que pueden poner en peligro los datos. Para evitar un uso incorrecto de los datos, deshabilite el modo de `Trace` HTTP.

Procedimiento

1 Para comprobar el modo de `Trace` en el servidor Apache2, ejecute el siguiente comando: `grep TraceEnable /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf`.

2 Para deshabilitar el modo de `Trace` en el servidor Apache2, ejecute el siguiente comando: `sed -i "/^[^#]*TraceEnable/ c\TraceEnable off" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf`.

Desactivación de los modos de configuración

Como procedimiento recomendado, al realizar tareas de instalación, configuración o mantenimiento en vRealize Operations Manager, es posible modificar la configuración o los ajustes para solucionar problemas y depurar la instalación.

Catalogue y audite cada uno de los cambios que realice para asegurarse de que disponen del nivel de seguridad adecuado. No ponga en marcha los cambios si no está seguro de que los cambios de configuración que ha realizado disponen del nivel de seguridad adecuado.

Gestión de componentes de software no esenciales

Para reducir los riesgos de seguridad, elimine o configure el software no esencial desde las máquinas host de vRealize Operations Manager.

Configure todo el software que no elimine según las recomendaciones del fabricante y las recomendaciones de seguridad para minimizar el potencial de generar infracciones de seguridad.

Seguridad del controlador de almacenamiento masivo USB

Proteja el controlador de almacenamiento masivo USB para evitar que se cargue de forma predeterminada en los dispositivos de vRealize y para evitar que se use como el controlador de dispositivo USB con los dispositivos de vRealize. Los posibles atacantes pueden aprovechar este controlador para instalar un software malintencionado.

Procedimiento

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

2 Compruebe que aparezca la línea `install usb-storage /bin/true` en el archivo.

3 Guarde el archivo y ciérrelo.

Seguridad del controlador del protocolo Bluetooth

Proteja el controlador del protocolo Bluetooth en los dispositivos vRealize para evitar que los posibles atacantes lo aprovechen.

Vincular el protocolo Bluetooth a la pila de red es innecesario y puede aumentar la exposición de ataque del host. Evite que el módulo del controlador del protocolo Bluetooth se cargue de forma predeterminada en los dispositivos vRealize.

Procedimiento

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

2 Compruebe que aparezca la línea `install bluetooth /bin/true` en este archivo.

3 Guarde el archivo y ciérrelo.

Seguridad del protocolo SCTP (transmisión de control de secuencias)

Evite que el módulo SCTP (protocolo de transmisión de control de secuencias) se cargue en los dispositivos vRealize 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 SCTP a menos que sea absolutamente necesario. SCTP es un protocolo de capa de transporte estandarizado por IETF que no se usa. Vincular este protocolo a la pila de red aumenta la exposición de ataque del host. Los procesos locales sin privilegios podrían provocar que el kernel cargue dinámicamente un controlador de protocolo mediante el protocolo para abrir un socket.

Procedimiento

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

2 Compruebe que la línea siguiente aparece en este archivo.

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

3 Guarde el archivo y ciérrelo.

Seguridad del protocolo DCCP (control de congestión de datagramas)

Como parte de las actividades de protección del sistema, evite que el protocolo DCCP (control de congestión de datagramas) se cargue en los dispositivos vRealize de forma predeterminada. Los posibles atacantes pueden aprovechar este protocolo para poner en peligro el sistema.

Evite cargar el módulo DCCP a menos que sea absolutamente necesario. DCCP es un protocolo de capa de transporte propuesto que no se utiliza. Vincular este protocolo a la pila de red aumenta la exposición de ataque del host. Los procesos locales sin privilegios pueden provocar que el kernel cargue dinámicamente un controlador de protocolo mediante el protocolo para abrir un socket.

Procedimiento

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

2 Compruebe 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.

Seguridad del protocolo RDS (sockets de datagramas fiables)

Como parte de las actividades de protección del sistema, evite que el protocolo RDS (sockets de datagramas fiables) se cargue en los dispositivos vRealize de forma predeterminada. Los posibles atacantes pueden aprovechar este protocolo para poner en peligro el sistema.

Vincular el protocolo RDS a la pila de red aumenta la exposición de ataque del host. Los procesos locales sin privilegios podrían provocar que el kernel cargue dinámicamente un controlador de protocolo mediante el protocolo para abrir un socket.

Procedimiento

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

2 Compruebe que aparezca la línea `install rds /bin/true` en este archivo.

3 Guarde el archivo y ciérrelo.

Seguridad del protocolo TIPC (comunicación transparente entre procesos)

Como parte de las actividades de protección del sistema, evite que el protocolo TIPC (comunicación transparente entre procesos) 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 protocolo TIPC a la pila de red aumenta la exposición de ataque del host. Los procesos locales sin privilegios pueden provocar que el kernel cargue dinámicamente un controlador de protocolo mediante el protocolo para abrir un socket.

Procedimiento

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

2 Compruebe que aparezca la línea `install tipc /bin/true` en este archivo.

3 Guarde el archivo y ciérrelo.

Seguridad del protocolo de intercambio de paquetes de Internet

Evite que el protocolo IPX (intercambio de paquetes de Internet) se cargue en los dispositivos vRealize de forma predeterminada. Los posibles atacantes podrían aprovechar este protocolo para poner en peligro el sistema.

Evite cargar el protocolo IPX a menos que sea absolutamente necesario. El protocolo IPX es un protocolo de nivel de red obsoleto. Vincular este protocolo a la pila de red aumenta la exposición de ataque del host. Los procesos locales sin privilegios podrían provocar que el sistema cargue dinámicamente un controlador de protocolo mediante el protocolo para abrir un socket.

Procedimiento

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

2 Compruebe que aparezca la línea `install ipx /bin/true` en este archivo.

3 Guarde el archivo y ciérrelo.

Seguridad del protocolo Appletalk

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

Evite cargar el protocolo Appletalk a menos que sea absolutamente necesario. Vincular este protocolo a la pila de red aumenta la exposición de ataque del host. Los procesos locales sin privilegios podrían provocar que el sistema cargue dinámicamente un controlador de protocolo mediante el protocolo para abrir un socket.

Procedimiento

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

2 Compruebe que aparezca la línea `install appletalk /bin/true` en este archivo.

3 Guarde el archivo y ciérrelo.

Seguridad del 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 protocolo DECnet a menos que sea absolutamente necesario. Vincular este protocolo a la pila de red aumenta la exposición de ataque del host. Los procesos locales sin privilegios podrían provocar que el sistema cargue dinámicamente un controlador de protocolo 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 Compruebe que aparezca la línea `install decnet /bin/true` en este archivo.

3 Guarde el archivo y ciérrelo.

Seguridad del módulo Firewire

Evite que el módulo Firewire se cargue en los dispositivos vRealize 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 Compruebe que aparezca la línea `install ieee1394 /bin/true` en este archivo.

3 Guarde el archivo y ciérrelo.

Auditoría y registro del kernel

La especificación `kernel.printk` del archivo `/etc/sysctl.conf` indica las especificaciones del registro de impresión del kernel.

Se especifican cuatro valores:

- `console loglevel`. La prioridad más baja de los mensajes impresos en la consola.
- `default loglevel`. El nivel más bajo de los mensajes sin un nivel de registro específico.
- El nivel más bajo posible del nivel de registro de la consola.
- El nivel predeterminado del nivel de registro de la consola.

Hay ocho entradas posibles por valor.

- `define KERN_EMERG "<0>" /* system is unusable */`
- `define KERN_ALERT "<1>" /* action must be taken immediately */`
- `define KERN_CRIT "<2>" /* critical conditions */`
- `define KERN_ERR "<3>" /* error conditions */`
- `define KERN_WARNING "<4>" /* warning conditions */`
- `define KERN_NOTICE "<5>" /* normal but significant condition */`
- `define KERN_INFO "<6>" /* informational */`
- `define KERN_DEBUG "<7>" /* debug-level messages */`

Establezca los valores de `kernel.printk` en **`3 4 1 7`** y compruebe que la línea `kernel.printk=3 4 1 7` existe en el archivo `/etc/sysctl.conf`.

Implementación instalada en Linux

Puede activar el servicio de protocolo de tiempo de redes (Network Time Protocol, NTP) y asegurarse de que el sistema está implementado con canales de transmisión segura.

Habilitación del servicio NTP

Para un abastecimiento de tiempo importante, puede deshabilitar la sincronización de tiempo del host y utilizar el protocolo de tiempo de redes (NTP). NTP en producción es un medio de realizar un seguimiento de las acciones del usuario de forma precia y de detectar los posibles ataques malintencionados y las intrusiones a través de una auditoría y un registro precisos.

El daemon ntp está incluido en el dispositivo y se utiliza para proporcionar servicios de tiempo sincronizados. El archivo de configuración de NTP se encuentra en `/etc/ntp.conf`.

TLS para datos en transferencia

Como recomendación de seguridad, asegúrese de que el sistema se ha implementado con canales de transmisión segura.

Configuración de protocolos estrictos para vRealize Operations Manager

Los protocolos SSLv2 y SSLv3 han dejado de considerarse seguros, incluidos el SSLv2 y el SSLv3. Como procedimiento de seguridad recomendado para la protección de la capa de transporte, proporcione compatibilidad únicamente para protocolos TLS.

Antes de la puesta en producción, debe comprobar que los protocolos SSLv2 y SSLv3 están deshabilitados.

Configuración de vRealize Operations Manager para utilizar claves de cifrado seguras

La seguridad de cifrado que se utiliza durante una sesión TLS viene determinada por la clave de cifrado negociada entre el servidor y el navegador. Para garantizar que solo se seleccionan claves de cifrado seguras, debe modificar el servidor para desactivar el uso de claves de cifrado no seguras. Además, debe configurar las claves de cifrado en un orden adecuado. Debe configurar el servidor para que admita solo claves de cifrado seguras, y debe utilizar claves con una longitud suficiente.

Desactivación de las claves de cifrado no seguras

Desactive los conjuntos de claves de cifrado que no ofrezcan autenticación, tales como los conjuntos de claves de cifrado NULL: NULL o eNULL. La falta de autenticación hace que sean vulnerables a ataques tipo "Man in the middle".

También debe desactivar el intercambio de claves Diffie-Hellman anónimo (ADH), las claves de cifrado de nivel de exportación (EXP, claves de cifrado que contienen DES), las claves con tamaños inferiores a 128 bits para el cifrado de tráfico de carga útil, el uso de MD5 como mecanismo de dispersión (hashing) para el tráfico de carga útil, los conjuntos de claves de cifrado IDEA y los conjuntos de claves de cifrado RC4, ya que son vulnerables a ataques en su totalidad.

Desactivación de claves de cifrado no seguras en el controlador HTTPD Apache

Desactive las claves de cifrado no seguras y active las claves de cifrado seguras que se utilizan en el controlador HTTPD Apache. Para evitar ataques de tipo "Man in the middle", revise las claves de cifrado del controlador HTTPD Apache en vRealize Operations Manager con respecto a la lista de claves de cifrado aceptables y desactive todas aquellas consideradas no seguras.

Procedimiento

1 Abra el archivo `/usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` en un editor de texto.

2 Compruebe que el archivo contiene la línea `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH`.

3 Guarde y cierre el archivo.

Activación del intercambio de claves Diffie-Hellman

El intercambio de claves Diffie-Hellman tiene puntos débiles. Debe desactivar todos los conjuntos de claves de cifrado que contengan DH, DHE y EDH. Estos conjuntos de claves de cifrado están disponibles de forma predeterminada. Se pueden activar si necesita utilizarlos.

Procedimiento

1 Abra el archivo `/usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf`.

2 Busque la línea `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH`.

3 Elimine `!DH:` para que la línea quede así: `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:@STRENGTH`.

4 Guarde y cierre el archivo.

Desactivación de los modos de configuración

Como procedimiento recomendado, al realizar tareas de instalación, configuración o mantenimiento en vRealize Operations Manager, es posible modificar la configuración o los ajustes para solucionar problemas y depurar la instalación.

Catalogue y audite cada uno de los cambios que realice para asegurarse de que disponen del nivel de seguridad adecuado. No ponga en marcha los cambios si no está seguro de que los cambios de configuración que ha realizado disponen del nivel de seguridad adecuado.

Comprobación de la configuración segura del servidor host

Para que vRealize Operations Manager funcione de forma segura, debe proteger y verificar las actividades de protección.

Para obtener más información, consulte la guía de protección de Red Hat Enterprise Linux 6 según las políticas de seguridad de su organización.

Agente de Endpoint Operations Management

El agente de Endpoint Operations Management añade recursos de supervisión y descubrimiento basado en agente a vRealize Operations Manager.

El agente de Endpoint Operations Management se instala directamente en los hosts, y puede estar o no en el mismo nivel de confianza que el servidor de Endpoint Operations Management. Por tanto, debe comprobar si los agentes se han instalado de una forma segura.

Recomendaciones de seguridad para ejecutar agentes de Endpoint Operations Management

Debe seguir determinadas recomendaciones de seguridad al utilizar cuentas de usuario.

- Para realizar una instalación silenciosa, elimine las credenciales y las huellas digitales del certificado del servidor almacenadas en el archivo `AGENT_HOME/conf/agent.properties`.
- Utilice una cuenta de usuario de vRealize Operations Manager reservada específicamente para el registro del agente de Endpoint Operations Management. Para obtener más información, consulte el tema "Funciones y privilegios" en vRealize Operations Manager en la ayuda de vRealize Operations Manager.
- Deshabilite la cuenta de usuario de vRealize Operations Manager que ha utilizado para el registro de agente una vez finalizada la instalación. Debe habilitar el acceso del usuario para las actividades de administración de agente. Para obtener más información, consulte el tema Configuración de usuarios y grupos en vRealize Operations Manager en la ayuda de vRealize Operations Manager.
- Si un sistema que ejecuta un agente está en riesgo, puede revocar el certificado de agente a través de la interfaz de usuario de vRealize Operations Manager mediante la eliminación del recurso de agente. Consulte la sección Revocación de un agente para obtener más información.

Cantidad mínima de permisos necesarios para la funcionalidad de agente

Son necesarios permisos para instalar y modificar un servicio. Si quiere detectar un proceso en ejecución, la cuenta de usuario que se utilice para ejecutar el agente también debe tener privilegios para acceder a los procesos y programas. En el caso de las instalaciones de sistemas operativos Windows, necesita permisos para instalar y modificar un servicio. En las instalaciones de sistemas operativos Linux, necesita permisos para instalar el agente como un servicio, si lo instala mediante un instalador RPM.

La cantidad mínima de credenciales que se necesitan para que el agente se registre con el servidor de vRealize Operations Manager es lo que se concede a un usuario con la función de gestor de agentes, sin asignaciones a objetos en el sistema.

Archivos y permisos de las plataformas basadas en Linux

Después de instalar el agente de Endpoint Operations Management, el propietario es el usuario que lo instala.

Los permisos de directorios y archivos de instalación, como 600 y 700, están configurados para el propietario cuando el usuario que instala el agente de Endpoint Operations Management extrae el archivo TAR o instala el RPM.

NOTA: Cuando se extrae el archivo ZIP, es posible que los permisos no se apliquen correctamente. Compruebe y asegúrese de que los permisos son correctos.

A todos los archivos que crea y escribe el agente se les asignan permisos 700 y el propietario es el usuario que ejecuta el agente.

Tabla 3-1. Archivos y permisos de Linux

Directorio o archivo	Permisos	Grupos o usuarios	Leer	Escribir	Ejecutar
directorio de agente/bin	700	Propietario	Sí	Sí	Sí
		Grupo	No	No	No
		Todo	No	No	No
directorio de agente/conf	700	Propietario	Sí	Sí	Sí

Tabla 3-1. Archivos y permisos de Linux (Continua)

Directorio o archivo	Permisos	Grupos o usuarios	Leer	Escribir	Ejecutar
		Grupo	No	No	No
		Todo	No	No	No
directorio de agente/log	700	Propietario	Sí	Sí	No
		Grupo	No	No	No
		Todo	No	No	No
directorio de agente/data	700	Propietario	Sí	Sí	Sí
		Grupo	No	No	No
		Todo	No	No	No
directorio de agente/bin/ep-agent.bat	600	Propietario	Sí	Sí	No
		Grupo	No	No	No
		Todo	No	No	No
directorio de agente/bin/ep-agent.sh	700	Propietario	Sí	Sí	Sí
		Grupo	No	No	No
		Todo	No	No	No
directorio de agente/conf/* (todos los archivos del directorio `conf`)	600	Propietario	Sí	Sí	Sí
		Grupo	No	No	No
		Todo	No	No	No
directorio de agente/log/* (todos los archivos del directorio `log`)	600	Propietario	Sí	Sí	No
		Grupo	No	No	No
		Todo	No	No	No
directorio de agente/data/* (todos los archivos del directorio `data`)	600	Propietario	Sí	Sí	No
		Grupo	No	No	No
		Todo	No	No	No

Archivos y permisos de las plataformas basadas en Windows

En el caso de una instalación basada en Windows del agente de Endpoint Operations Management, el usuario que instala el agente debe tener permisos para instalar y modificar el servicio.

Después de instalar el agente de Endpoint Operations Management, la carpeta de instalación, incluidos todos los subdirectorios y archivos, solo deben ser accesibles para SISTEMA, el grupo de administradores y el usuario de la instalación. Cuando instale el agente de Endpoint Operations Management mediante `ep-agent.bat`, asegúrese de que el proceso de protección se lleva a cabo correctamente. Como usuario que instala el agente, se recomienda que anote los mensajes de error. Si el proceso de protección no se realiza, el usuario puede aplicar estos permisos manualmente.

Tabla 3-2. Archivos y permisos de Windows

Directorio o archivo	Grupos o usuarios	Control total	Modificar	Leer y ejecutar	Leer	Escribir
<directorio de agente>/bin	SISTEMA	Sí	-	-	-	-
	Administrador	Sí	-	-	-	-

Tabla 3-2. Archivos y permisos de Windows (Continua)

Directorio o archivo	Grupos o usuarios	Control total	Modificar	Leer y ejecutar	Leer	Escribir
	Usuario de instalación	Sí	-	-	-	-
	Usuarios		-	-	-	-
<directorio de agente>/conf	SISTEMA	Sí	-	-	-	-
	Administrador	Sí	-	-	-	-
	Usuario de instalación	Sí	-	-	-	-
	Usuarios		-	-	-	-
<directorio de agente>/log	SISTEMA	Sí	-	-	-	-
	Administrador	Sí	-	-	-	-
	Usuario de instalación	Sí	-	-	-	-
	Usuarios		-	-	-	-
<directorio de agente>/data	SISTEMA	Sí	-	-	-	-
	Administrador	Sí	-	-	-	-
	Usuario de instalación	Sí	-	-	-	-
	Usuarios		-	-	-	-
<directorio de agente>/bin/hq-agent.bat	SISTEMA	Sí	-	-	-	-
	Administrador	Sí	-	-	-	-
	Usuario de instalación	Sí	-	-	-	-
	Usuarios		-	-	-	-
<directorio de agente>/bin/hq-agent.sh	SISTEMA	Sí	-	-	-	-
	Administrador	Sí	-	-	-	-
	Usuario de instalación	Sí	-	-	-	-
	Usuarios		-	-	-	-
<directorio de agente>/conf/* (todos los archivos del directorio `conf`)	SISTEMA	Sí	-	-	-	-
	Administrador	Sí	-	-	-	-
	Usuario de instalación	Sí	-	-	-	-
	Usuarios		-	-	-	-
<directorio de agente>/log/* (todos los archivos del directorio `log`)	SISTEMA	Sí	-	-	-	-
	Administrador	Sí	-	-	-	-

Tabla 3-2. Archivos y permisos de Windows (Continua)

Directorio o archivo	Grupos o usuarios	Control total	Modificar	Leer y ejecutar	Leer	Escribir
	Usuario de instalación	Sí	-	-	-	-
	Usuarios		-	-	-	-
<directorio de agente>/data/* (todos los archivos del directorio `data`)	SISTEMA	Sí	-	-	-	-
	Administrador	Sí	-	-	-	-
	Usuario de instalación	Sí	-	-	-	-
	Usuarios		-	-	-	-

Apertura de puertos en el host del agente

El proceso del agente escucha los comandos en dos puertos, 127.0.0.1:2144 y 127.0.0.1:32000; dichos puertos se pueden configurar. Estos puertos se pueden asignar de forma arbitraria y, por tanto, el número de puerto exacto puede variar. El agente no abre puertos en interfaces externas.

Tabla 3-3. Cantidad mínima de puertos obligatorios

Puerto	Protocolo	Dirección	Comentarios
443	TCP	Saliente	Lo utiliza el agente para las conexiones salientes a través de HTTP, TCP o ICMP.
2144	TCP	Escucha	Solo interno. Configurable. Se utiliza para la comunicación entre procesos entre el agente y la línea de comandos que lo carga y lo configura. El proceso de agente escucha en este puerto. **NOTA:** El número de puerto se asigna de forma arbitraria y puede ser diferente.
32000	TCP	Escucha	Solo interno. Configurable. Se utiliza para la comunicación entre procesos entre el agente y la línea de comandos que lo carga y lo configura. El proceso de agente escucha en este puerto. **NOTA:** El número de puerto se asigna de forma arbitraria y puede ser diferente.

Revocación de un agente

Si por algún motivo necesita revocar un agente, por ejemplo, si un sistema con agente en ejecución está en riesgo, puede eliminar el recurso de agente del sistema. Cualquier solicitud posterior no superará la verificación.

Utilice la interfaz de usuario de vRealize Operations Manager para revocar el certificado de agente mediante la eliminación del recurso de agente. Para obtener más información, consulte "Eliminación de un recurso de agente," página 40.

Cuando el sistema vuelva a estar protegido, podrá volver a activar el agente. Para obtener más información, consulte "Reactivación de un recurso de agente," página 40.

Eliminación de un recurso de agente

También puede usar vRealize Operations Manager para revocar el certificado de agente mediante la eliminación del recurso de agente.

Prerequisitos

Para mantener la continuidad del recurso con los datos de métrica registrados previamente, efectúe un registro del token de agente de Endpoint Operations Management que se muestra en los detalles del recurso.

Procedimiento

1 Vaya a Explorador de inventario en la interfaz de usuario de vRealize Operations Manager.

2 Abra el árbol Tipos de adaptador.

3 Abra la lista Adaptador de EP Ops.

4 Seleccione **Agente de EP Ops - *NOMBRE_HOST_DNS***.

5 Haga clic en **Editar objeto**.

6 Registre el ID de agente, que es la cadena de token de agente.

7 Cierre el cuadro de diálogo Editar objeto.

8 Seleccione **Agente de EP Ops - *NOMBRE_HOST_DNS*** y haga clic en **Eliminar objeto**.

Reactivación de un recurso de agente

Una vez recuperado el estado de seguridad de un sistema, se puede reactivar un agente revocado. De este modo se asegura de que el agente continúa informando de los mismos recursos sin perder el historial de datos. Para ello, debe crear un nuevo archivo token de Endpoint Operations Management mediante el mismo token registrado antes de eliminar el recurso de agente. Consulte la sección Eliminación del recurso de agente.

Prerequisitos

- Compruebe que dispone de la cadena de token de Endpoint Operations Management registrada.
- Utilice el token de recurso registrado antes de eliminar el recurso de agente del servidor de vRealize Operations Manager.
- Compruebe que dispone del privilegio Gestionar agentes.

Procedimiento

1 Cree el archivo token de agente con el usuario que ejecuta el agente.

Por ejemplo, ejecute el comando para crear un archivo token que contenga el token 123-456-789.

- En Linux:

```
echo 123-456-789 > /etc/epops/epops-token
```

- En Windows:

```
echo 123-456-789 > %PROGRAMDATA%\VMware\Ep Ops Agent\epops-token
```

En el ejemplo, el archivo token se escribe en la ubicación de token predeterminada para dicha plataforma

2 Instale un nuevo agente y regístrelo con el servidor de vRealize Operations Manager. Compruebe que el agente carga el token que ha insertado en el archivo token.

Debe disponer del privilegio Gestionar agentes para realizar esta acción.

Revocación de certificados de agente y actualización de certificados

El flujo de nueva emisión se inicia desde el agente mediante el argumento de la línea de comandos `setup`. Cuando un agente que ya está registrado usa el argumento `ep-agent.sh setup` de la línea de comandos `setup` y rellena las credenciales obligatorias, se envía un nuevo comando `registerAgent` al servidor.

El servidor detecta que el agente ya está registrado y le envía un nuevo certificado de cliente sin crear otro recurso de agente. En el agente, el nuevo certificado de cliente reemplaza al anterior. En los casos en que el certificado de servidor está modificado y ejecuta el comando `ep-agent.sh setup`, aparecerá un mensaje en el que se le pide que confíe en el nuevo certificado. También puede proporcionar la huella digital del nuevo certificado de servidor en el archivo `agent.properties` antes de ejecutar el comando `ep-agent.sh setup` para que el proceso sea silencioso.

Prerequisitos

Gestione el privilegio de agente para revocar y actualizar certificados.

Procedimiento

- En los sistemas operativos basados en Linux, ejecute el comando `ep-agent.sh setup` en el host del agente. En los sistemas operativos basados en Windows, ejecute el comando `ep-agent.bat setup`.

  Si el agente detecta que se ha modificado el certificado del servidor, se muestra un mensaje. Acepte el nuevo certificado si confía en él y es válido.

Revisión y actualización del agente de Endpoint Operations Management

Por si fueran necesarios, hay nuevos paquetes del agente de Endpoint Operations Management disponibles, independientes de las versiones de vRealize Operations Manager.

No se proporcionan revisiones ni actualizaciones para el agente de Endpoint Operations Management. Debe instalar la versión más reciente del agente que incluya las correcciones de seguridad más recientes. Las correcciones de seguridad importantes se comunicarán de acuerdo con las directrices de avisos de seguridad de VMware. Consulte el tema sobre avisos de seguridad.

Actividades adicionales de configuración segura

Verifique las cuentas de usuario del servidor y elimine las aplicaciones innecesarias en los servidores host. Bloquee los puertos innecesarios y deshabilite los servicios en ejecución en su servidor host que no sean necesarios.

Comprobación de la configuración de la cuenta de usuario de servidor

Se recomienda comprobar que no hay cuentas de usuario innecesarias en la configuración y en las cuentas de usuario locales y de dominio.

Restrinja las cuentas de usuario que no estén relacionadas con el funcionamiento de la aplicación a las cuentas necesarias para la administración, el mantenimiento y la solución de problemas. Restrinja el acceso remoto de las cuentas de usuario de dominio al mínimo necesario para mantener el servidor. Controle y audite de forma estricta estas cuentas.

Eliminación y desactivación de aplicaciones innecesarias

Borre las aplicaciones innecesarias de los servidores host. Cada aplicación innecesaria adicional aumenta el riesgo de exposición debido a sus vulnerabilidades desconocidas o no revisadas.

Desactivación de servicios y puertos innecesarios

Compruebe la lista de puertos abiertos al tráfico del cortafuegos del servidor host.

Bloquee todos los puertos que no aparezcan en la lista como requisito mínimo para vRealize Operations Manager en la sección "Configuración de puertos y protocolos," página 52 de este documento, o que no sean necesarios. Además, audite los servicios en ejecución en el servidor host y desactive aquellos que no sean necesarios.

Seguridad de red y comunicación segura 4

Como recomendación de seguridad, revise y edite la configuración de las comunicaciones de red de los dispositivos virtuales y las máquinas host de VMware. También debe configurar la cantidad mínima de puertos entrantes y salientes para vRealize Operations Manager.

Este capítulo cubre los siguientes temas:

Configuración de los ajustes de red para la instalación de la aplicación virtual

Para garantizar que los equipos host y el dispositivo virtual de VMware permiten solo comunicaciones esenciales y seguras, revise y edite los ajustes de comunicación de red.

Evitar el control de usuario de las interfaces de red

Como recomendación de seguridad, restrinja la capacidad de modificar la configuración de la interfaz de red a los usuarios con privilegios. Si la manipulación de las interfaces de red por parte de los usuarios, podría dar como resultado la omisión de mecanismos de seguridad de red o denegaciones de servicio. Asegúrese de que las interfaces de red no están configuradas para el control de usuario.

Procedimiento

1 Para comprobar la configuración de control de usuario, ejecute el comando `#grep –i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*`.

2 Asegúrese de que cada interfaz está establecida en `NO`.

Configuración del tamaño de la cola de las conexiones pendientes de TCP

Como recomendación de seguridad, configure un tamaño predeterminado de la cola de conexiones pendientes de TCP en las máquinas host de dispositivos VMware. Para mitigar los ataques de denegación de TCP o de servicio, configure un tamaño adecuado para la cola de conexiones pendientes de TCP. La configuración predeterminada recomendada es 1280.

Procedimiento

1 Ejecute el comando `# cat /proc/sys/net/ipv4/tcp_max_syn_backlog` en cada máquina host de dispositivo de VMware.

2 Configure el tamaño de cola para las conexiones pendientes de TCP.

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

b Añada la siguiente entrada al archivo para configurar el tamaño de cola de conexiones pendientes de TCP.

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

c Guarde los cambios y cierre el archivo.

Denegación de ecos de ICMPv4 de direcciones de difusión

Las respuestas a ecos del protocolo de mensajes de control de Internet (ICMP) de difusión proporcionan un vector de ataque para los ataques de amplificación y pueden facilitar la asignación de redes por parte de agentes malintencionados. La configuración del sistema para que ignore los ecos de ICMPv4 proporciona protección frente a este tipo de ataques.

Procedimiento

1 Ejecute el comando `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` para comprobar que el sistema no está enviando respuestas a solicitudes de eco de direcciones de difusión de ICMP.

2 Configure el sistema host para denegar solicitudes de eco de direcciones de difusión de ICMPv4.

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

b Si el valor para esta entrada no se encuentra fijado en `1`, añada la entrada `net.ipv4.icmp_echo_ignore_broadcasts=1`.

c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que desactive el proxy ARP IPv4

El proxy ARP IPv4 permite a un sistema enviar respuestas a solicitudes ARP en una interfaz en nombre de hosts conectados a otra interfaz. Debe desactivar el proxy ARP IPv4 para evitar el uso compartido de información no autorizada. Desactive este parámetro para evitar la pérdida de información relacionada con direcciones entre los segmentos de red conectados.

Procedimiento

1 Ejecute el comando `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp|egrep "default|all"` para comprobar si el proxy ARP está desactivado.

2 Configure el sistema host para desactivar el proxy ARP IPv4.

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

b Si los valores no se encuentran fijados en `0`, añada las entradas o actualice las entradas existentes según corresponda. Fije el valor en `0`.

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

c Guarde los cambios realizados y cierre el archivo.

Configuración del sistema host para que ignore mensajes de redirección de ICMP IPv4

Como procedimiento de seguridad recomendado, compruebe que el sistema host ignora los mensajes de redirección del protocolo de mensajes de control de Internet (ICMP) IPv4. Un mensaje de redirección de ICMP malintencionado puede permitir que se produzca un ataque de tipo "Man in the middle". Los enrutadores utilizan mensajes de redirección de ICMP para indicar a los hosts que existe una ruta más directa para alcanzar un destino. Estos mensajes modifican la tabla de rutas del host y no están autenticados.

Procedimiento

1 Ejecute el comando `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects|egrep "default|all"` en el sistema host para comprobar si el sistema host ignora los mensajes de redirección IPv4.

2 Configure el sistema host para que ignore los mensajes de redirección de ICMP IPv4.

   a Abra el archivo `/etc/sysctl.conf`.

   b Si los valores no se encuentran fijados en `0`, añada las siguientes entradas al archivo o actualice las entradas existentes según corresponda. Fije el valor en `0`.

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

   c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que ignore mensajes de redirección de ICMP IPv6

Como procedimiento de seguridad recomendado, compruebe que el sistema host ignora los mensajes de redirección del protocolo de mensajes de control de Internet (ICMP) IPv6. Un mensaje de redirección de ICMP malintencionado puede permitir que se produzca un ataque de tipo "Man in the middle" (intermediarios). Los enrutadores utilizan mensajes de redirección de ICMP para indicar a los hosts que existe una ruta más directa para alcanzar un destino. Estos mensajes modifican la tabla de rutas del host y no están autenticados.

Procedimiento

1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects|egrep "default|all"` en el sistema host y compruebe si ignora los mensajes de redirección IPv6.

2 Configure el sistema host para que ignore los mensajes de redirección de ICMP IPv6.

   a Abra el archivo `/etc/sysctl.conf` para configurar el sistema host para que ignore los mensajes de redirección IPv6.

   b Si los valores no se encuentran fijados en `0`, añada las siguientes entradas al archivo o actualice las entradas existentes según corresponda. Fije el valor en `0`.

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

   c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que deniegue los mensajes de redirección del protocolo de mensajes de control de Internet (ICMP) IPv4

Como procedimiento de seguridad recomendado, compruebe que el sistema host deniega los mensajes de redirección del protocolo de mensajes de control de Internet (ICMP) IPv4. Los enrutadores utilizan mensajes de redirección de ICMP para informar a los servidores de que existe una ruta directa para alcanzar un destino concreto. Estos mensajes contienen información procedente de la tabla de rutas del sistema que puede poner de manifiesto partes de la topología de la red.

Procedimiento

1 Ejecute el comando `# grep [01] /proc/sys/net/ipv4/conf/*/send_redirects|egrep "default|all"` en el sistema host para comprobar si deniega los mensajes de redirección del protocolo de mensajes de control de Internet (ICMP) IPv4.

2 Configure el sistema host para que deniegue los mensajes de redirección del protocolo de mensajes de control de Internet (ICMP) IPv4.

   a Abra el archivo `/etc/sysctl.conf` para configurar el sistema host.

   b Si los valores no se encuentran fijados en `0`, añada las siguientes entradas al archivo o actualice las entradas existentes según corresponda. Fije el valor en `0`.

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

   c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que registre los paquetes Martian IPv4

Como recomendación de seguridad, compruebe que el sistema host registra los paquetes Martian IPv4. Los paquetes Martian contienen direcciones que el sistema sabe que no son válidas. Configure el sistema host para que registre los mensajes de modo que pueda identificar las configuraciones incorrectas o los ataques en curso.

Procedimiento

1 Ejecute el comando `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians|egrep "default|all"` para comprobar si el host registra los paquetes Martian IPv4.

2 Configure el sistema host para que registre los paquetes Martian IPv4.

   a Abra el archivo `/etc/sysctl.conf` para configurar el sistema host.

   b Si los valores no se encuentran fijados en `1`, añada las siguientes entradas al archivo o actualice las entradas existentes según corresponda. Fije el valor en `1`.

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

   c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que utilice el método de filtrado de rutas inverso IPv4

Como procedimiento de seguridad recomendado, configure las máquinas host para que utilicen el método de filtrado de rutas inverso IPv4. El filtrado de rutas inverso ofrece protección frente a direcciones de origen falsificadas haciendo que el sistema descarte paquetes con direcciones de origen sin ruta o cuya ruta no identifica la interfaz que los origina.

Configure el sistema para que utilice el filtrado de rutas inverso siempre que sea posible. Según la función del sistema, el filtrado de rutas inverso podría provocar el descarte de tráfico legítimo. En tal caso, es posible que necesite utilizar un modo más permisivo o desactivar completamente el filtrado de rutas inverso.

Procedimiento

1 Ejecute el comando `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|egrep "default|all"` en el sistema host para comprobar si el sistema utiliza el método de filtrado de rutas inverso IPv4.

2 Configure el sistema host para que utilice el método de filtrado de rutas inverso IPv4.

   a Abra el archivo `/etc/sysctl.conf` para configurar el sistema host.

   b Si los valores no se encuentran fijados en `1`, añada las siguientes entradas al archivo o actualice las entradas existentes según corresponda. Fije el valor en `1`.

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

   c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que deniegue el reenvío IPv4

Como procedimiento de seguridad recomendado, compruebe que el sistema host deniega el reenvío IPv4. Si el sistema está configurado para el reenvío de direcciones IP y no es un enrutador designado, se podría utilizar para omitir la seguridad de red proporcionando una ruta de comunicación que no es filtrada por los dispositivos de red.

Procedimiento

1 Ejecute el comando `# cat /proc/sys/net/ipv4/ip_forward` para comprobar si el host deniega el reenvío IPv4.

2 Configure el sistema host para que deniegue el reenvío IPv4.

   a Abra el archivo `/etc/sysctl.conf` para configurar el sistema host.

   b Si el valor no se encuentra fijado en `0`, añada la siguiente entrada al archivo o actualice la entrada existente según corresponda. Fije el valor en `0`.

   ```
   net.ipv4.ip_forward=0
   ```

   c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que deniegue el reenvío de paquetes enrutados en origen IPv4

Los paquetes enrutados en origen permiten al origen del paquete sugerir que los enrutadores reenvíen el paquete por una ruta diferente a la configurada en el enrutador. Esto se puede utilizar para omitir medidas de seguridad de red.

Este requisito se aplica solo al reenvío de tráfico enrutado en origen como, por ejemplo, cuando se activa el reenvío IPv4 y el sistema funciona como enrutador.

Procedimiento

1 Ejecute el comando `# grep [01] /proc/sys/net/ipv4/conf/*/accept_source_route|egrep "default|all"` para comprobar que el sistema no utiliza paquetes enrutados en origen IPv4.

2 Configure el sistema host para que deniegue el reenvío de paquetes enrutados en origen IPv4.

   a Abra el archivo `/etc/sysctl.conf` con un editor de texto.

   b Si los valores no se encuentran fijados en `0`, asegúrese de que `net.ipv4.conf.all.accept_source_route=0` y `et.ipv4.conf.default.accept_source_route=0` están fijados en `0`.

   c Guarde y cierre el archivo.

Configuración del sistema host para que deniegue el reenvío IPv6

Como procedimiento de seguridad recomendado, compruebe que el sistema host deniega el reenvío IPv6. Si el sistema está configurado para el reenvío de direcciones IP y no es un enrutador designado, se puede utilizar para omitir la seguridad de red proporcionando una ruta de comunicación que no es filtrada por los dispositivos de red.

Procedimiento

1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding|egrep "default|all"` para comprobar si el host deniega el reenvío IPv6.

2 Configure el sistema host para que deniegue el reenvío IPv6.

   a Abra el archivo `/etc/sysctl.conf` para configurar el sistema host.

   b Si los valores no se encuentran fijados en `0`, añada las siguientes entradas al archivo o actualice las entradas existentes según corresponda. Fije el valor en `0`.

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

   c Guarde los cambios y cierre el archivo.

Configuración del sistema host para utilizar cookies SYN de TCP IPv4

Como recomendación de seguridad, compruebe que el sistema host usa cookies SYN de TCP (protocolo de control de transmisión) IPv4. Un ataque de inundación SYN de TCP podría provocar una denegación de servicio al rellenar la tabla de conexiones TCP de un sistema con conexiones en estado SYN_RCVD. Las cookies SYN se utilizan para no realizar el seguimiento de una conexión hasta que se reciba la indicación ACK posterior, con lo que se verifica que el iniciador está intentando realizar una conexión válida y no es una fuente de inundación.

Esta técnica no cumple totalmente los estándares, pero solo se activa cuando se detecta una condición de inundación y permite la defensa del sistema mientras se sirven solicitudes válidas.

Procedimiento

1 Ejecute el comando `# cat /proc/sys/net/ipv4/tcp_syncookies` para comprobar si el sistema host usa las cookies SYN de TCP IPv4.

2 Configure el sistema host para que use las cookies SYN IPv4.

a Abra el archivo `/etc/sysctl.conf` para configurar el sistema host.

b Si el valor no se encuentra fijado en `1`, añada la siguiente entrada al archivo o actualice la entrada existente según corresponda. Fije el valor en `1`.

```
net.ipv4.tcp_syncookies=1
```

c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que deniegue anuncios de enrutador IPv6

Como procedimiento de seguridad recomendado, compruebe que el sistema host deniega la aceptación de anuncios de enrutador y mensajes de redirección del protocolo de mensajes de control de Internet (ICMP), salvo que sean necesarios. Una función actual de IPv6 es que los sistemas pueden configurar sus dispositivos en red mediante el uso automático de información procedente de la red. Desde el punto de vista de la seguridad, es preferible ajustar manualmente la información de configuración importante en lugar de aceptarla de 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 el sistema host para comprobar si el sistema deniega la aceptación de anuncios de enrutador y mensajes de redirección del protocolo de mensajes de control de Internet (ICMP), salvo que sean necesarios.

2 Configure el sistema host para que deniegue los anuncios de enrutador IPv6.

a Abra el archivo `/etc/sysctl.conf`.

b Si los valores no se encuentran fijados en `0`, añada las siguientes entradas al archivo o actualice las entradas existentes según corresponda. Fije el valor en `0`.

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

c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que deniegue solicitudes de enrutador IPv6

Como procedimiento de seguridad recomendado, compruebe que el sistema host deniega las solicitudes de enrutador IPv6, salvo que sean necesarias. El ajuste de las 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"` para comprobar si el sistema host deniega las solicitudes de enrutador IPv6, salvo que sean necesarias.

2 Configure el sistema host para que deniegue solicitudes de enrutador IPv6.

a Abra el archivo `/etc/sysctl.conf`.

b Si los valores no se encuentran fijados en `0`, añada las siguientes entradas al archivo o actualice las entradas existentes según corresponda. Fije el valor en `0`.

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

c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que deniegue la preferencia de enrutador IPv6 en solicitudes de enrutador

Como procedimiento de seguridad recomendado, compruebe que el sistema host deniega las solicitudes de enrutador IPv6, salvo que sean necesarias. La preferencia de enrutador en la configuración de 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 el sistema host para comprobar si el sistema host deniega las solicitudes de enrutador IPv6.

2 Configure el sistema host para que deniegue la preferencia de enrutador IPv6 en solicitudes de enrutador.

   a Abra el archivo `/etc/sysctl.conf`.

   b Si los valores no se encuentran fijados en `0`, añada las siguientes entradas al archivo o actualice las entradas existentes según corresponda. Fije el valor en `0`.

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

   c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que deniegue prefijos de enrutador IPv6

Como procedimiento de seguridad recomendado, compruebe que el sistema host deniega los prefijos de enrutador IPv6, salvo que sean necesarios. El parámetro `accept ra pinfo` controla si el sistema acepta información de prefijos procedente del enrutador. Si las direcciones se asignan de forma estática, el sistema no recibe ninguna información de prefijos de enrutador.

Procedimiento

1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo|egrep "default|all"` para comprobar si el sistema deniega la información de prefijos de enrutador IPv6.

2 Configure el sistema host para que deniegue prefijos de enrutador IPv6.

   a Abra el archivo `/etc/sysctl.conf`.

   b Si los valores no se encuentran fijados en `0`, añada las siguientes entradas al archivo o actualice las entradas existentes según corresponda. Fije el valor en `0`.

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

   c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que deniegue las opciones de límite de saltos de anuncios del enrutador IPv6

Como recomendación de seguridad, compruebe que el sistema host deniega las opciones de límite de saltos de anuncios del enrutador IPv6, salvo que sean necesarias. El parámetro `accept_ra_defrtr` controla si el sistema aceptará las opciones de límite de saltos procedentes de un anuncio de enrutador. Si se configura en `0`, se impedirá que el enrutador cambie el límite de saltos del IPv6 predeterminado para los paquetes salientes.

Procedimiento

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

2 Si los valores no se definen en `0`, configure el sistema host para que deniegue las opciones de límite de saltos de anuncios del enrutador IPv6.

   a Abra el archivo `/etc/sysctl.conf`.

   b Si los valores no se encuentran fijados en `0`, añada las siguientes entradas al archivo o actualice las entradas existentes según corresponda. Fije el valor en `0`.

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

   c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que deniegue el ajuste de configuración automática de anuncios de enrutador IPv6

Como procedimiento de seguridad recomendado, compruebe que el sistema host deniega el ajuste `autoconf` de anuncios de enrutador IPv6. El ajuste `autoconf` controla 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"` para comprobar si el sistema deniega el ajuste `autoconf` de anuncios de enrutador IPv6.

2 Si los valores no se encuentran fijados en `0`, configure el sistema host para que deniegue el ajuste configuración automática de anuncios de enrutador IPv6.

   a Abra el archivo `/etc/sysctl.conf`.

   b Si los valores no se encuentran fijados en `0`, añada las siguientes entradas al archivo o actualice las entradas existentes según corresponda. Fije el valor en `0`.

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

   c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que deniegue solicitudes de vecino IPv6

Como procedimiento de seguridad recomendado, compruebe que el sistema host deniega las solicitudes de vecino IPv6, salvo que sean necesarias. El parámetro `dad_transmits` determina cuántas solicitudes de vecino se enviarán por dirección, incluidas las direcciones globales y locales de vínculo, al acceder a una interfaz para asegurarse de que la dirección deseada es única en la red.

Procedimiento

1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits|egrep "default|all"` para comprobar si el sistema deniega las solicitudes de vecino IPv6.

2 Si los valores no se encuentran fijados en `0`, configure el sistema host para que deniegue las solicitudes de vecino IPv6.

   a Abra el archivo `/etc/sysctl.conf`.

   b Si los valores no se encuentran fijados en `0`, añada las siguientes entradas al archivo o actualice las entradas existentes según corresponda. Fije el valor en `0`.

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

   c Guarde los cambios y cierre el archivo.

Configuración del sistema host para que restrinja el número máximo de direcciones IPv6

Como recomendación de seguridad, compruebe que el host restringe el número máximo de direcciones IPv6 que se pueden asignar. La configuración del número máximo de direcciones determina cuántas direcciones IPv6 de unidifusión se pueden asignar a cada interfaz. El valor predeterminado es 16, pero debe configurar el número según las direcciones globales necesarias que se han configurado estadísticamente.

Procedimiento

1 Ejecute el comando `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses|egrep "default|all"` para comprobar que el sistema host restringe el número máximo de direcciones IPv6 que se pueden asignar.

2 Si los valores no se configuran como `1`, configure el sistema host para que restrinja el número máximo de direcciones IPv6 que se pueden asignar.

   a Abra el archivo `/etc/sysctl.conf`.

   b Añada las siguientes entradas al archivo o actualice las entradas existentes según corresponda. Fije el valor en `1`.

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

   c Guarde los cambios y cierre el archivo.

Configuración de puertos y protocolos

Como procedimiento de seguridad recomendado, desactive todos los puertos y protocolos que no sean esenciales.

Configure los puertos de entrada y salida mínimos de los componentes de vRealize Operations Manager, ya que es necesario para que los componentes importantes del sistema funcionen a máximo rendimiento.

Cantidad mínima de puertos entrantes predeterminados

Como recomendación de seguridad, configure los puertos entrantes necesarios para que vRealize Operations Manager funcionen a máximo rendimiento.

Tabla 4-1. cantidad mínima obligatoria de puertos entrantes

Puerto	Protocolo	Comentarios
443	TCP	Se utiliza para acceder a la interfaz de usuario de vRealize Operations Manager y a la interfaz de administrador de vRealize Operations Manager.
123	UDP	vRealize Operations Manager lo utiliza para la sincronización de protocolo de tiempo de redes (Network Time Protocol, NTP) con el nodo primario.
5433	TCP	Lo utilizan los nodos maestros y de réplica para replicar la base de datos global (vPostgreSQL) cuando High Availability está habilitada.
7001	TCP	Cassandra lo utiliza para la comunicación segura de clúster internodo. No conecte este puerto a Internet. Añada este puerto a un cortafuegos.
9042	TCP	Cassandra lo utiliza para la comunicación segura relacionada con los clientes entre nodos. No conecte este puerto a Internet. Añada este puerto a un cortafuegos.
6061	TCP	Los clientes lo utilizan para conectar GemFire Locator y obtener información de conexión a los servidores en el sistema distribuido. También supervisa la carga de servidor para enviar clientes a los servidores menos cargados.
10000-10010	TCP y UDP	Rango de puertos efímeros de GemFire Server que se utilizan para mensajería UDP de unidifusión y para detección de fallos TCP en un sistema distribuido punto a punto.
20000-20010	TCP y UDP	Rango de puertos efímeros de GemFire Locator que se utilizan para mensajería UDP de unidifusión y para detección de fallos TCP en un sistema distribuido punto a punto.

Tabla 4-2. Puertos entrantes opcionales

Puerto	Protocolo	Comentarios
22	TCP	Opcional. Secure Shell (SSH). La escucha del servicio SSH en el puerto 22, o en cualquier otro puerto, debe estar deshabilitada en un entorno de producción y el puerto 22 debe estar cerrado.
80	TCP	Opcional. Redirige a 443.
3091-3101	TCP	Si Horizon View está instalado, se utilizan para acceder a los datos de vRealize Operations Manager desde Horizon View.

Auditoría y registro en su sistema de vRealize Operations Manager 5

Como práctica de seguridad recomendada, lleve a cabo un procedimiento de auditoría y registro en su sistema de vRealize Operations Manager.

La implementación detallada del procedimiento de auditoría y registro queda fuera del alcance de este documento.

El registro remoto en un host de registro central proporciona un almacén seguro para los registros. La recopilación de los archivos de registro en un host central permite supervisar fácilmente el entorno con una única herramienta. También puede realizar análisis conjuntos y búsquedas de ataques coordinados en varias entidades dentro de la infraestructura. Un servidor de registros centralizado y seguro puede ayudarle a evitar la manipulación de registros, además de proporcionarle un registro de auditoría a largo plazo.

Este capítulo cubre los siguientes temas:

Seguridad del servidor de registro remoto

Como procedimiento de seguridad recomendado, asegúrese de que solo un usuario autorizado puede configurar el servidor de registro remoto y de que es seguro.

Es posible que los atacantes que quebrantan la seguridad de las máquinas host busquen e intenten manipular los archivos de registro para encubrir sus ataques y mantener el control sin ser descubiertos.

Uso de un servidor NTP autorizado

Compruebe que todos los sistemas host utilizan la misma fuente de tiempo relativo, incluido el desplazamiento de localización correspondiente. Puede correlacionar la fuente de tiempo relativo con un estándar de tiempo acordado, como UTC (hora universal coordinada).

Puede realizar el seguimiento de las acciones de un intruso, y correlacionarlas, al revisar los archivos de registro pertinentes. La configuración de tiempo incorrecta puede dificultar la inspección y la correlación de los archivos de registro para detectar ataques y generar una auditoría imprecisa. Puede utilizar al menos tres servidores NTP de fuentes de tiempo externas o configurar servidores NTP locales en una red de confianza que obtenga el tiempo de al menos tres fuentes de tiempo externas.

Consideraciones del navegador cliente

Como recomendación de seguridad, no utilice vRealize Operations Manager desde clientes que no sean de confianza o que no se hayan revisado, ni desde clientes que utilicen extensiones de navegador.

Índice

T

U