Oracle® Hierarchical Storage Manager and StorageTek QFS Software

Guía de seguridad

Versión 6.0

E62073-01

Marzo de 2015

ORACLE®

Oracle® Hierarchical Storage Manager and StorageTek QFS Software
Guía de seguridad

E62073-01

Tabla de contenidos

Prólogo

La Guía de seguridad del software de Oracle Hierarchical Storage Manager and StorageTek QFS incluye información sobre el producto Oracle Hierarchical Storage Manager and QFS y explica los principios generales de seguridad de la aplicación.

Destinatarios

Esta guía está destinada a cualquier persona que se encargue de la utilización de funciones de seguridad y de la instalación y la configuración seguras de Oracle Hierarchical Storage Manager and StorageTek QFS Software.

Accesibilidad a la documentación

Para obtener información sobre el compromiso de Oracle con la accesibilidad, visite el sitio web del Programa de Accesibilidad de Oracle en `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Acceso a Oracle Support
Los clientes de Oracle que hayan contratado servicios de soporte electrónico pueden acceder a ellos mediante My Oracle Support. Para obtener información, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` o, si tiene alguna discapacidad auditiva, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`.

Convenciones tipográficas

La siguiente tabla describe las convenciones tipográficas utilizadas en este manual.

Tipos de letra	Significado	Ejemplo
AaBbCc123	Nombres de los comandos y la salida del equipo en pantalla	Utilice *Is -a* para mostrar todos los archivos.
AaBbCc123	Entrada de usuario que usted escribe cuando va junto con la salida del equipo en pantalla	*machine_name%* **su** *Password:*
aabbcc123	Marcador de posición: sustituir por un valor o nombre real	El comando necesario para eliminar un archivo es *rm filename*.
AaBbCc123	Títulos de los manuales, términos nuevos y palabras destacables	Consulte el Capítulo 6 de la *Guía del usuario*. Una copia en *caché* es aquella que se almacena localmente. No guarde el archivo. Nota: Algunos elementos destacados aparecen en negrita en línea.

Indicadores de los shells en los ejemplos de comandos

La tabla siguiente muestra los indicadores del sistema UNIX predeterminados y el indicador de superusuario para los shells que se incluyen en el SO Oracle Solaris. Tenga en cuenta que el indicador predeterminado del sistema que se muestra en los ejemplos de comandos varía según la versión de Oracle Solaris.

Shell	Indicador
Bashshell, Kornshell y Bourneshell	$
Bashshell, Kornshell y Bourneshell para superusuario	#
Cshell	machine_name%
Cshell para superusuario	machine_name#

1

Descripción general

En este capítulo, se proporciona una descripción general del producto Oracle Hierarchical Storage Manager and StorageTek QFS Software y se explican los principios generales de seguridad de la aplicación.

1.1. Descripción general del producto

Oracle Hierarchical Storage Manager and StorageTek QFS Software es un sistema de archivos compartido con un administrador de almacenamiento jerárquico. El producto consta de los siguientes componentes principales:

Paquete de StorageTek QFS
Incluye el sistema de archivos QFS de alto rendimiento que se pueden configurar como independientes o compartidos. Cuando se configura como independiente, QFS se configura en un solo sistema y no con clientes compartidos. QFS usa operaciones de vnode VFS estándar para conectarse con los sistemas operativos Oracle Solaris y Linux.

Los paquetes de instalación de QFS son SUNWqfsr y SUNWqfsu. Estos paquetes no incluyen el componente Oracle Hierarchical Storage Manager (HSM).

Si configura QFS de manera independiente sin clientes compartidos, se tienen menos riesgos de seguridad. Esta configuración no ejecuta daemons y no tiene conexiones remotas que no sean de canal de fibra con el disco. Si se configura QFS de manera compartida, se incluyen conexiones de canal de fibra con el disco y una conexión TCP/IP entre los clientes y el servidor de metadatos (MDS).

Paquete de Oracle HSM
Incluye el sistema de archivos QFS y el código necesario para ejecutar Oracle HSM. Los paquetes de instalación de Oracle HSM son SUNWsamfsr y SUNWsamfsu. Si no necesita gestión de almacenamiento jerárquico, instale *solo* el paquete de StorageTek QFS.

SAM-Remote
Permite el acceso a bibliotecas de cintas y unidades remotas por medio de conexiones de red de área extensa (WAN) TCP/IP. StorageTek SAM-Remote proporciona una manera de recuperación ante desastres mediante la ubicación remota de instalaciones de cinta. Puede instalar SAM-Remote con los paquetes de QFS o SAM-QFS, pero debe activar y configurar SAM-Remote de manera separada. Para obtener más información sobre SAM-Remote, consulte la *biblioteca de documentación del cliente de Oracle Hierarchical Storage Manager and StorageTek QFS Software versión 6.0* en: `http://`

www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs

Interfaz gráfica de usuario de Manager
La interfaz gráfica de usuario (GUI) de Manager, fsmgr, se ejecuta en el MDS y se accede a ella de manera remota desde un explorador web. El acceso se obtiene mediante el puerto 6789 (https://hostname:6789).

Para utilizar fsmgr, debe iniciar la sesión como un usuario válido en el MDS y agregar ciertos roles a la cuenta del usuario. Para obtener información sobre la instalación y la configuración de la GUI de Manager, consulte la *biblioteca de documentación del cliente de Oracle Hierarchical Storage Manager and StorageTek QFS Software versión 6.0* en: http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs

1.2. Principios generales de seguridad

En las siguientes secciones se describen los principios fundamentales necesarios para utilizar cualquier aplicación de manera segura.

1.2.1. Mantenga el software actualizado

Manténgase actualizado con la versión de Oracle HSM que ejecute. Puede encontrar las versiones actuales del software para descargarlas en Oracle Software Delivery Cloud (https://edelivery.oracle.com/).

1.2.2. Restrinja el acceso de red a los servicios críticos

Oracle HSM usa los siguientes puertos TCP/IP:

- tcp/7105 se utiliza para el tráfico de metadatos entre el cliente y el MDS
- tcp/1000 se utiliza para SAM-Remote
- tcp/6789 es el puerto HTTP que se usa para que un explorador contacte a fsmgr
- tcp/5012 se utiliza para sam-rpcd

Nota:

Para el tráfico bidireccional de cliente del MDS, considere la posibilidad de configurar una red separada que no esté interconectada con la WAN externa. Esta configuración previene la exposición ante amenazas externas y, además, garantiza que el tráfico externo no limite el rendimiento del MDS.

1.2.3. Siga el principio de privilegios mínimos

Otorgue al usuario o administrador el menor privilegio necesario para completar la tarea que se va a realizar. La GUI de Manager tiene varios roles que pueden otorgarse a los usuarios. Estos roles otorgan diferentes tipos y cantidades de privilegios. Si se realizan tareas administrativas desde la línea de comandos, se requiere permiso root.

Para obtener más información sobre la GUI de Manager, consulte la *biblioteca de documentación del cliente de Oracle Hierarchical Storage Manager and StorageTek QFS Software versión 6.0* en: http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs

1.2.4. Supervisión de la actividad del sistema

Supervise la actividad del sistema para determinar el funcionamiento de Oracle HSM y para determinar si está registrando una actividad inusual. Consulte los siguientes archivos de registro:

- /var/adm/messages
- /var/opt/SUNWsamfs/sam-log
- /var/opt/SUNWsamfs/archiver.log, consulte /etc/opt/SUNWsamfs/archiver.cmd
- /var/opt/SUNWsamfs/recycler.log, consulte /etc/opt/SUNWsamfs/recycler.cmd
- /var/opt/SUNWsamfs/releaser.log, consulte /etc/opt/SUNWsamfs/releaser.cmd
- /var/opt/SUNWsamfs/stager.log, consulte /etc/opt/SUNWsamfs/stager.cmd
- /var/opt/SUNWsamfs/trace/*

1.2.5. Manténgase actualizado acerca de la última información de seguridad

Puede acceder a distintas fuentes de información de seguridad. Para obtener información de seguridad y alertas para una gran variedad de productos de software, consulte http://www.us-cert.gov. Para obtener información específica para SAM-QFS , consulte https://communities.oracle.com/portal/server.pt/community/sam_qfs_storage_archive_manager_and_sun_qfs/401. La mejor forma de mantenerse actualizado con los asuntos de seguridad es ejecutar la versión más actualizada del software de Oracle HSM.

2

Instalación segura

En este capítulo, se describe el proceso de planificación para una instalación segura y se describen viarias topologías de implementación recomendadas para los sistemas.

2.1. Comprensión del entorno

Para comprender mejor las necesidades de seguridad, deben hacerse las siguientes preguntas:

2.1.1. ¿Qué recursos necesitan protección?

Puede proteger muchos de los recursos en el entorno de producción. Tenga en cuenta el tipo de recursos que desea proteger cuando determine el nivel de seguridad que se va a proporcionar.

Cuando utilice Oracle HSM, proteja los siguientes recursos:

Disco de datos principales y metadatos
Estos recursos de disco se utilizan para crear sistemas de archivos de Oracle HSM. Por lo general, están conectados mediante canal de fibra (FC). El acceso independiente a estos discos (no por medio de Oracle HSM) presenta un riesgo de seguridad porque se omiten los permisos de directorio y archivo normales de Oracle HSM. Este tipo de acceso externo podría ser desde un sistema no fiable que lee o escribe los discos de FC o desde un sistema interno que accidentalmente proporciona acceso no root a los archivos del dispositivo básico.

Cintas de Oracle HSM
El acceso independiente a cintas, por lo general en una biblioteca de cintas, donde se escriben los datos de archivos fuera de un sistema de archivos de Oracle HSM, es un riesgo para la seguridad.

Cintas de volcado de Oracle HSM
Los volcados de sistemas de archivos que se crean desde samfsdump contienen datos y metadatos. Estos datos y metadatos deben estar protegidos a fin de evitar el acceso que no sea del administrador del sistema durante un volcado de rutina o una actividad de restauración.

Servidor de metadatos (MDS) de Oracle HSM
Los clientes de Oracle HSM requieren acceso TCP/IP al MDS. Sin embargo, asegúrese de que los clientes estén protegidos del acceso WAN externo.

Archivos y valores de configuración
Los valores de configuración de Oracle HSM se deben proteger del acceso de usuarios que no sean administradores. En general, estos ajustes están protegidos automáticamente por Oracle HSM cuando usa la GUI de Manager. Tenga en cuenta que si habilita la opción de escritura de los archivos de configuración para usuarios que no sean el administrador, se genera un riesgo para la seguridad.

2.1.2. ¿De quién se protegen los recursos?

En general, los recursos descritos en la sección anterior deben estar protegidos contra el acceso de todos los usuarios que no sean root y que no sean administradores en un sistema configurado, o contra un sistema externo no fiable que pueda acceder a estos recursos por medio de WAN o tejido de canal de fibra.

2.1.3. ¿Qué sucede si falla la protección de los recursos estratégicos?

Los fallos de protección de recursos estratégicos pueden incluir desde el acceso inadecuado (acceso a datos más allá de los permisos de los archivos POSIX de Oracle HSM) hasta daños en los datos (escritura en el disco o cinta más allá de los permisos normales).

2.2. Topologías de implementación recomendadas

En esta sección se describe cómo instalar y configurar un componente de infraestructura de manera segura. Para obtener información sobre la instalación de Oracle HSM, consulte la *biblioteca de documentación del cliente de Oracle Hierarchical Storage Manager versión 6.0* en: `http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs`

Tenga en cuenta los siguientes puntos cuando instale y configure Oracle HSM:

Red de metadatos separada
Para conectar los clientes de Oracle HSM a los servidores de MDS, proporcione una red TCP/IP separada y conmute el hardware que no esté conectado a ninguna WAN. Como el tráfico de metadatos se implementa mediante TCP/IP, un ataque externo a este tráfico es posible en teoría. Si se configura una red de metadatos separada, se mitiga este riesgo y se proporciona un rendimiento mejorado. La mejora de rendimiento se obtiene mediante un ruta de datos garantizada para los metadatos. Si no es factible proporcionar una red de metadatos separada, por lo menos deniegue el tráfico a los puertos de Oracle HSM desde la WAN externa y desde cualquier host no confiable en la red. Consulte Sección 1.2.2, “Restrinja el acceso de red a los servicios críticos” [8].

Zonas de canal de fibra
Use zonas de canal de fibra para denegar el acceso a los discos de Oracle HSM desde cualquier servidor que no requiera acceso a los discos. Preferiblemente, utilice un conmutador de FC separado para conectar físicamente sólo los servidores que necesitan acceso al disco.

Protección del acceso de configuración de los discos SAN
Por lo general, puede accederse a los discos SAN RAID por motivos administrativos mediante TCP/IP o, lo que ocurre más habitualmente, mediante HTTP. Debe proteger los discos de acceso externo; para esto, limite el acceso administrativo a los discos SAN RAID sólo a sistemas dentro de un dominio de confianza. Además, cambie la contraseña predeterminada en las matrices de disco.

Instalación del paquete de Oracle HSM
Primero, instale solo los paquetes que necesite. Por ejemplo, si no utilizará la gestión de almacenamiento jerárquico, instale sólo los paquetes de QFS. Los permisos de directorio y archivo y los responsables de Oracle HSM predeterminados no deberían cambiarse después de la instalación sin tener en cuenta las consecuencias de tales cambios sobre la seguridad.

Acceso de cliente
Si tiene planificado configurar clientes compartidos, determine qué clientes deben tener acceso al sistema de archivos en el archivo hosts. Consulte la página del comando man hosts.fs(4). Configure sólo los hosts que requieren que se configure el acceso a un sistema de archivos particular.

Refuerzo del servidor de metadatos de Oracle Solaris
Para obtener información sobre cómo reforzar el sistema operativo Oracle Solaris, consulte las Directrices de seguridad de Oracle Solaris 10 y las Directrices de seguridad de Oracle Solaris 11. Como mínimo, escoja una buena contraseña root, instale una versión actualizada del sistema operativo Oracle Solaris, y manténgase actualizado con los parches, en especial, con los parches de seguridad.

Refuerzo de clientes Linux
Lea la documentación de Linux sobre cómo reforzar los clientes Linux. Como mínimo, escoja una buena contraseña root, instale una versión actualizada de Linux, y manténgase actualizado con los parches, en especial, con los parches de seguridad.

Seguridad de cinta de Oracle HSM
Impida el acceso externo a las cintas de Oracle HSM desde afuera de Oracle HSM o limite dicho acceso solo a los administradores. Utilice zonas de canal de fibra para limitar el acceso a unidades de cinta sólo al MDS (o los posibles MDS si se configura un MDS de respaldo). Los clientes Solaris que se configuren para usar E/S distribuida necesitarán acceso a unidades de cinta. Además, limite el acceso a los archivos del dispositivo de cinta otorgando permisos sólo a usuarios root. El acceso sin autorización a cintas de Oracle HSM puede poner en peligro o destruir datos del usuario.

Copias de seguridad
Defina y realice copias de seguridad de los datos de Oracle HSM mediante el comando samfsdump o el comando qfsdump. Limite el acceso a las cintas de volcado según lo recomendado para las cintas de Oracle HSM.

2.2.1. Instalación de SAM-Remote

Para obtener información sobre la instalación del software de StorageTek SAM-Remote, consulte la *biblioteca de documentación del cliente de Oracle Hierarchical Storage Manager*

and StorageTek QFS Software versión 6.0 en: http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs

2.2.2. Instalación de la GUI de Manager

Para obtener información sobre la instalación segura de la GUI de Manager, consulte la *biblioteca de documentación del cliente de Oracle Hierarchical Storage Manager and StorageTek QFS Software versión 6.0* en: http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs

2.2.3. Configuración posterior a la instalación

Después de instalar cualquiera de los paquetes de Oracle HSM, revise la lista de comprobación de seguridad en Apéndice A, *Lista de comprobación de implementación segura* [19]

3

Funciones de seguridad

Para evitar posibles amenazas para la seguridad, los clientes que usan un sistema de archivos compartido deben tener en cuenta lo siguiente:

- Revelación de datos del sistema de archivos con incumplimiento de políticas
- Pérdida de datos
- Modificación de datos no detectada

Estas amenazas de seguridad se pueden minimizar mediante la configuración correcta y siguiendo la lista de comprobación posterior a la instalación que figura en Apéndice A, *Lista de comprobación de implementación segura* [19]

3.1. El modelo de seguridad

Las funciones de seguridad críticas que proporcionan protección frente a las amenazas de seguridad son:

- Autenticación: garantiza que sólo personas autorizadas tengan acceso al sistema y los datos.
- Autorización: control de acceso para privilegios de sistema. Esta característica se basa en la autenticación para garantizar que las personas sólo obtengan el nivel de acceso adecuado.
- Auditoría: permite que los administradores detecten los intentos de incumplimiento del mecanismo de autenticación y los incumplimientos del control de acceso que se intentaron y que se llevados a cabo.

3.1.1. Autenticación

Oracle HSM usa autenticación de usuarios basada en host para controlar quién puede realizar tareas administrativas. La administración mediante la GUI de Manager se controla principalmente mediante roles asignados a varios usuarios. La administración mediante línea de comandos está limitada al usuario root.

3.1.2. Control de acceso

En Oracle HSM, el control de acceso se divide en dos partes:

- Control de acceso administrativo: controla quién puede realizar tareas administrativas para Oracle HSM. Los controles están basados en roles que se asignan a los usuarios mediante

la GUI de Manager. Para operaciones de línea de comando, los controles se basan en los permisos root. Para obtener más información sobre la GUI de Manager, consulte la *biblioteca de documentación del cliente de Oracle Hierarchical Storage Manager and StorageTek QFS Software versión 6.0* en: http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs

- Control de acceso de archivo/directorio: Oracle HSM implementa un sistema de archivos que cumple con POSIX y que cuenta con un amplio conjunto de controles de acceso. Consulte la documentación de Oracle HSM para obtener más información.

4

Consideraciones de seguridad para desarrolladores

Los desarrolladores, por lo general, no interaccionan directamente con Oracle HSM. Las dos excepciones son la API *`libsam`* y la API *`libsamrpc`*. Estas dos API proporcionan la misma funcionalidad. *`libsam`* es solo para el equipo local, mientras que *`libsamrpc`* se comunica con el MDS mediante *`rpc(3)`* para implementar las acciones solicitadas. La autenticación de las solicitudes realizadas con cualquiera de los dos métodos se basa en el UID y el GID del proceso de llamada. Tienen los mismos permisos que la solicitudes realizadas mediante la línea de comandos. Asegúrese de que tengan un espacio de UID y GID común para el MDS y los sistemas de clientes.

Para obtener más información, consulte las páginas del comando man *`intro_libsam(3)`* y *`intro_libsamrpc(3)`*.

Apéndice A

Lista de comprobación de implementación segura

Esta lista de comprobación de seguridad incluye instrucciones que ayudan a proteger su base de datos.

1. Defina contraseñas seguras para las cuentas root y para otras cuentas que tengan roles de Oracle HSM asignados a ellas. Esta instrucción incluye:
   - Las cuentas a las que la GUI de Manager les asignan roles administrativos.
   - Los ID de usuario *`acsss`*, *`acsdb`* y *`acssa`* (si se utilizan).
   - Cualquier cuenta administrativa de matriz de disco.
2. Si utiliza el usuario predeterminado *`samadmin`* con la GUI de Manager, cambie inmediatamente la contraseña instalada predeterminada por una contraseña segura. No utilice el rol root con la GUI de Manager, en cambio, asigne roles a otras cuentas de usuarios según sea necesario. Proteja las otras cuentas también con contraseñas seguras.
3. Instale filtrado de puertos en enrutadores edge WAN para impedir que el tráfico de los puertos detallados en Sección 1.2, “Principios generales de seguridad” [8] ingrese en el MDS o los clientes, excepto según sea necesario para SAM-Remote.
4. Separe las cintas y los discos de canal de fibra, ya sea físicamente o mediante zonas de canal de fibra de manera que sólo se pueda acceder a los discos desde el MDS y los clientes, y a las cintas desde el MDS y los posibles MDS. Esta práctica de seguridad ayuda a evitar los accidentes de pérdida de datos debido a la sobreescritura accidental de la cinta o el disco.
5. Compruebe */dev* para asegurarse de que ningún usuario que no sea root pueda acceder a los archivos del dispositivo de disco y cinta. Esta práctica impide que se acceda inadecuadamente a los datos de Oracle HSM o que éstos se destruyan.
6. Oracle HSM es un sistema de archivos POSIX, y proporciona un amplio conjunto de permisos de archivo/directorio, incluidas las listas de control de acceso (ACL). Utilícelos según sea necesario para proteger los datos del usuario en el sistema de archivos. Para obtener más información, consulte la documentación de Oracle HSM.
7. Configure un conjunto adecuado de volcados de copia de seguridad en función de la política local. Las copias de seguridad forman parte de la seguridad y proporcionan una manera de restaurar los datos perdidos, ya sea accidentalmente o por cualquier infracción de seguridad. Su copia de seguridad debe incluir alguna política cuando se la transporta a una ubicación externa. Las copias de seguridad tienen que estar protegidas en la misma medida que las cintas y discos de Oracle HSM.