Guía de seguridad de Oracle® Storage 12 Gb/s SAS PCIe RAID HBA, Internal

Para los modelos de HBA 7110116 y 7110117

Referencia: E59792
Diciembre de 2014

Contenido

Seguridad de Oracle Storage 12 Gb/s SAS PCIe RAID HBA, Internal 5
Descripción general del HBA 5
Principios de seguridad 6
Planificación de un entorno seguro 7
Seguridad del hardware 7
Seguridad de software 8
Seguridad de firmware 8
Firmware de Oracle ILOM 8
Registros del sistema 9
Mantenimiento de un entorno seguro 9
Seguimiento de activos 9
Actualizaciones de firmware 9
Actualizaciones de software 10
Seguridad del registro 10
Seguridad del módulo 10

Seguridad de Oracle Storage 12 Gb/s SAS PCIe RAID HBA, Internal

En este documento, se establecen directrices y principios de seguridad generales que se deben tener en cuenta cuando se usa Oracle Storage 12 Gb/s SAS PCIe RAID HBA, Internal.

Esta documentación *no* abarca la siguiente información de seguridad:

- Seguridad específica de firmware de plataforma que se relaciona con el BIOS, Open Boot Prom (OBP) y el hipervisor
- Problemas de seguridad del sistema operativo
- Seguridad física del sistema de hardware
- Seguridad de red de infraestructura de red externa
- Información del Módulo de plataforma segura

Para obtener información sobre la seguridad de cualquiera de estas áreas, consulte la documentación de seguridad que se proporciona con el producto específico.

En este documento, se incluyen los siguientes temas:

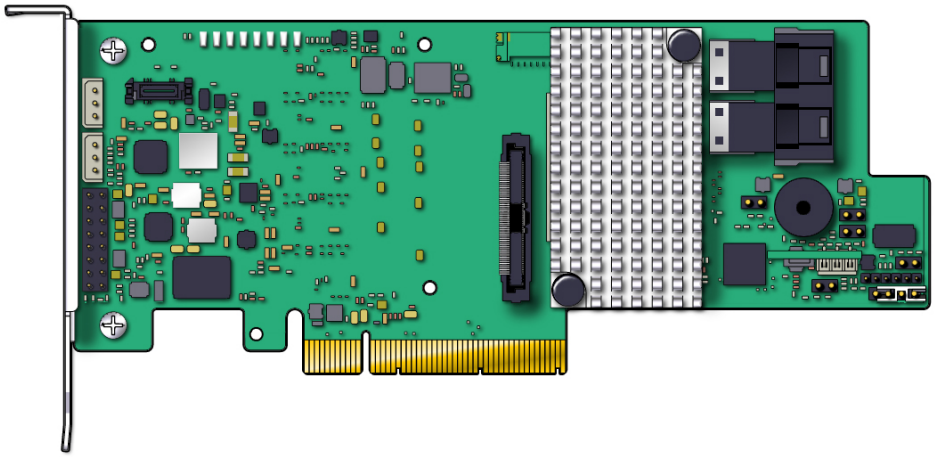
- "Descripción general del HBA" [5]
- "Principios de seguridad" [6]
- "Planificación de un entorno seguro" [7]
- "Mantenimiento de un entorno seguro" [9]

Descripción general del HBA

Oracle Storage 12 Gb/s SAS PCIe RAID HBA, Internal (con los números de referencia de marketing 7110116 y 7110117) es un controlador RAID PCIe 3.0 de bajo perfil, que admite ocho puertos internos SAS/SATA de 12 Gb/s mediante dos conectores Mini SAS HD internos de 4 vías SFF-8643.

Nota - El único tipo de SATA admitido por este HBA es SATA II.

En la siguiente imagen, se muestra Oracle Storage 12 Gb/s SAS PCIe RAID HBA, Internal:



Principios de seguridad

Hay cuatro principios básicos de seguridad: acceso, autenticación, autorización y contabilidad.

- **Acceso**

  Los controles físicos y de software protegen el hardware y sus datos frente a posibles intrusiones.

  - En el caso del hardware, los límites de acceso por lo general son límites de acceso *físicos*.
  - En el caso del software, el acceso está limitado por medios físicos y virtuales.
  - El firmware no se puede cambiar, excepto por medio del proceso de actualización de Oracle.
- **Autenticación**

  Configure las funciones de autenticación, por ejemplo, un sistema de contraseñas, en los sistemas operativos de la plataforma para asegurarse de que los usuarios sean quienes dicen ser.

  Asegúrese de que el personal utilice correctamente las identificaciones de empleado para ingresar a la sala de cómputo.
- **Autorización**

Permita al personal trabajar únicamente con hardware y software que estén capacitados y cualificados para utilizar. Establezca un sistema de permisos de lectura, escritura y ejecución para controlar el acceso del usuario a los comandos, el espacio en el disco, los dispositivos y las aplicaciones.

- **Contabilidad**

  Utilice las funciones de software y de hardware de Oracle para supervisar la actividad de conexión y mantener los inventarios de hardware.

  - Use los logs del sistema para supervisar el inicio de sesión de los usuarios. Supervise las cuentas de servicio y administrador del sistema en particular, ya que esas cuentas tienen acceso a comandos potentes.
  - Utilice los números de serie de los componentes para realizar un seguimiento de los activos del sistema. Los números de pieza de Oracle se registran electrónicamente en todas las tarjetas, módulos y placas base.

Planificación de un entorno seguro

Revise la información de esta sección antes y durante la instalación y configuración de un servidor y de Oracle Storage 12 Gb/s SAS PCIe RAID HBA, Internal.

En esta sección, se incluyen los siguientes temas:

- “Seguridad del hardware ” [7]
- “Seguridad de software ” [8]
- “Seguridad de firmware” [8]
- “Firmware de Oracle ILOM” [8]
- “Registros del sistema” [9]

Seguridad del hardware

El hardware físico se puede proteger con relativa facilidad limitando el acceso al hardware y registrando los números de serie.

- **Restricción del acceso**
  - Si el equipo se instala en un rack con una puerta con llave, mantenga la puerta cerrada, a menos que sea necesario reparar algún componente del rack.
  - Almacene las unidades sustituibles en campo (FRU) o las unidades sustituibles por el cliente (CRU) de repuesto en un armario cerrado. Restrinja el acceso al armario cerrado a personal autorizado.
- **Registro de los números de serie**

  Mantenga un registro de los números de serie de todas las tarjetas de HBA.

Seguridad de software

Las siguientes son las consideraciones de seguridad para los componentes de software:

- Consulte la documentación incluida con el software para activar las funciones de seguridad disponibles para el software.
- Use la cuenta de superusuario para configurar y actualizar los controladores de HBA.
- La mayoría de las medidas de seguridad del hardware se implementan por medio de medidas de software.
- Los componentes de software que admiten el HBA dependen de las funciones de seguridad del sistema para proporcionar acceso seguro.

Seguridad de firmware

El HBA se envía con todo el firmware instalado. No es necesario realizar la instalación del firmware en el campo, salvo las actualizaciones.

- Si alguna vez se necesitan las actualizaciones del firmware, estas se deben obtener en el área de soporte de Oracle del sitio web de LSI: http://www.lsi.com/sep/Pages/oracle/index.aspx

  También puede contactarse con Oracle para solicitar soporte o buscar en My Oracle Support las últimas actualizaciones y procedimientos del producto:

  https://support.oracle.com
- Use la cuenta de superusuario para configurar y actualizar la utilidad de gestión de firmware del HBA. Las cuentas de usuarios comunes solo le permiten al usuario ver el firmware, no editarlo. El proceso de actualización del firmware del sistema operativo Oracle Solaris evita que se realicen modificaciones de firmware sin autorización.
- Consulte la guía de instalación del HBA, que se encuentra en el sitio web de Oracle, para obtener las noticias más recientes, información sobre los requisitos de actualización de firmware y otros datos sobre seguridad.
- Para obtener más información sobre la configuración de las variables de seguridad de OpenBootPROM (OBP), consulte el *Manual de referencia del comando OpenBoot 4.x*.

Firmware de Oracle ILOM

Puede proteger, gestionar y supervisar de manera activa los componentes del sistema mediante el firmware Oracle Integrated Lights Out Manager (Oracle ILOM), que está preinstalado en algunos servidores x86. Para obtener más información sobre el uso de este firmware al configurar contraseñas, administrar usuarios y aplicar funciones relacionadas con la seguridad, así como los Secure Shell (SSH), los Secure Socket Layer (SSL) y la autenticación RADIUS, consulte la documentación de Oracle ILOM:

http://www.oracle.com/pls/topic/lookup?ctx=ilom31

Registros del sistema

- Active el registro y envíe los logs a un host de registro dedicado seguro.
- Configure el registro para incluir información de tiempo precisa mediante NTP y registros de hora.

Mantenimiento de un entorno seguro

Después de la instalación y la configuración iniciales del HBA, use las funciones de seguridad del hardware y el software de Oracle para continuar controlando el hardware y realizando un seguimiento de los activos del sistema.

Se incluyen las siguientes secciones:

- "Seguimiento de activos" [9]
- "Actualizaciones de firmware" [9]
- "Actualizaciones de software " [10]
- "Seguridad del registro" [10]
- "Seguridad del módulo" [10]

Seguimiento de activos

Utilice los números de serie para realizar un seguimiento del inventario. Oracle incorpora los números de serie del firmware en tarjetas opcionales y placas base del sistema. Puede leer estos números de serie mediante conexiones de red de área local.

También puede utilizar lectores inalámbricos de identificación por radiofrecuencia (RFID) para simplificar aún más el seguimiento de los activos. Consulte las notas del producto de Oracle, *Cómo realizar un seguimiento de sus activos del sistema Oracle Sun mediante RFID*.

Actualizaciones de firmware

Mantenga actualizadas las versiones de firmware en sus equipos.

- Busque actualizaciones con regularidad.
- Todos los sistemas operativos en general, y Oracle Solaris en particular, requieren que se inicie sesión con las credenciales root para administrar las tarjetas y actualizar los controladores o el firmware.
- Instale siempre la versión publicada más reciente del firmware.

Actualizaciones de software

Mantenga actualizadas sus versiones de software en sus equipos.

- Las actualizaciones de software de los controladores de Oracle Solaris están disponibles mediante parches y actualizaciones de Oracle Solaris.
- Puede que las actualizaciones de software para controladores para otros sistemas operativos estén disponibles en http://www.lsi.com/sep/Pages/oracle/index.aspx.
- Consulte la documentación del HBA, que se encuentra en el sitio web de Oracle, para obtener las noticias más recientes, información sobre los requisitos de actualización de software y otros datos sobre seguridad.
- Instale siempre la versión más reciente del software.
- Instale los parches de seguridad necesarios para el software.
- Los dispositivos también contienen firmware y pueden requerir actualizaciones de firmware.

Seguridad del registro

Inspeccione y mantenga los archivos de registro de manera periódica.

- Revise los logs para detectar posibles incidentes y archívelos de acuerdo con una política de seguridad.
- Retire con regularidad los archivos log cuando excedan un tamaño razonable. Mantenga copias de los archivos retirados para utilizarlos en el futuro para referencia o análisis estadístico.

Seguridad del módulo

El HBA se gestiona mediante la interfaz de línea de comandos (CLI) LSI StorCLI o mediante el software de interfaz gráfica de usuario (GUI) MegaRAID SAS. Este software le permite realizar lo siguiente:

- Supervisar el funcionamiento del HBA.
- Actualizar el firmware del HBA.

El software de la GUI MegaRAID SAS y StorCLI proporcionan acceso solo a los usuarios con credenciales `root`. Por lo tanto, los usuarios sin privilegios no pueden hacer cambios en el entorno SAN mediante estas utilidades.

Para obtener información sobre la CLI StorCLI y la GUI MegaRAID SAS, consulte la documentación de LSI en el siguiente sitio web: http://www.lsi.com/sep/Pages/oracle/index.aspx.