Guía de seguridad de hardware de Oracle® EDR Infiniband Switch y sistemas de E/S virtualizada

Referencia: E75987-01
Septiembre de 2016

Referencia: E75987-01

Accesibilidad a la documentación

Para obtener información acerca del 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 adquirido servicios de soporte disponen de acceso a soporte electrónico a través de My Oracle Support. Para obtener información, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` o `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si tiene problemas de audición.

Contenido

Uso de esta documentación 7
Biblioteca de documentación del producto 7
Comentarios 7

Guía de seguridad de Oracle InfiniBand Switch IS2-46 9
Descripción de los principios de seguridad 9
Planificación de un entorno seguro 10
Seguridad de hardware 10
Seguridad de software 11
Firmware de Oracle ILOM 11
Seguridad de VLAN 12
Cuentas de usuario 12
Logs del sistema 12
Mantenimiento de un entorno seguro 13
Control de energía de hardware 13
Seguimiento de activos 13
Actualizaciones para software y firmware 13
Acceso a la red 14
Protección de datos 14
Seguridad de los logs 15

Uso de esta documentación

- **Visión general**: describe cómo implementar las políticas de seguridad en el switch de Oracle.
- **Destinatarios**: técnicos, administradores de sistemas y proveedores de servicios autorizados.
- **Conocimiento requerido**: experiencia avanzada en la administración del hardware de red.

Biblioteca de documentación del producto

La documentación y los recursos para este producto y los productos relacionados están disponibles en http://www.oracle.com/goto/is2-46/docs.

Comentarios

Puede escribir sus comentarios sobre esta documentación en http://www.oracle.com/goto/docfeedback.

Guía de seguridad de Oracle InfiniBand Switch IS2-46

En este documento, se proporcionan directrices de seguridad generales para ayudarlo a proteger el chasis de switch Oracle IS2-46.

Los temas incluidos son los siguientes:

- "Descripción de los principios de seguridad" [9]
- "Planificación de un entorno seguro" [10]
- "Mantenimiento de un entorno seguro" [13]

Descripción de los principios de seguridad

Los cuatro principios de seguridad básicos son: acceso, autenticación, autorización y control.

- **Acceso**

  Los controles físicos y de software protegen el hardware y los 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 el switch para asegurarse de que los usuarios sean quienes dicen ser.

  Asegúrese de que el personal utilice correctamente las identificaciones de empleado para ingresar al centro de datos.
- **Autorización**

  Permita al personal trabajar únicamente con hardware y software para el que cuente con la capacitación y cualificación necesaria.

  Establezca un sistema de permisos de lectura, escritura y ejecución, para controlar el acceso del usuario a los comandos, al espacio en el disco, a los dispositivos y a las aplicaciones.

- **Contabilidad**

  Utilice las funciones de software y hardware de Oracle para supervisar las actividades de inicio de sesión y mantener los inventarios de hardware.

  - Use los logs del sistema y de Oracle ILOM para supervisar el inicio de sesión de los usuarios. Supervise la cuenta `root`y la cuenta con privilegios de root en particular, ya que estas cuentas pueden acceder a comandos importantes.
  - Use los números de serie de los componentes para realizar un seguimiento de los activos del sistema. Los números de serie de Oracle se marcan físicamente en el chasis y se registran electrónicamente en todos los SP y SCP, y en todas las placas principales.

Planificación de un entorno seguro

Consulte estos temas antes de realizar la instalación y configuración del switch, y mientras lo esté haciendo.

- "Seguridad de hardware" [10]
- "Seguridad de software" [11]
- "Firmware de Oracle ILOM" [11]
- "Seguridad de VLAN" [12]
- "Cuentas de usuario" [12]
- "Logs del sistema" [12]

Seguridad de hardware

El hardware físico se puede proteger de manera simple mediante la limitación del acceso al hardware y el registro de los números de serie.

- **Restricción del acceso**
  - Instale el switch en un área cerrada con llave y de acceso restringido.
  - Si el equipo se instala en un rack con una puerta con llave, mantenga la puerta cerrada en todo momento.
  - Restrinja el acceso a las conexiones de red y al tejido del switch. Además de proteger al switch, esto también permite protege los nodos similares.
  - Restrinja el acceso a las consolas serie en el área del switch y no más allá del perímetro protegido. No use servidores de terminales ni concentradores de puertos. Las consolas serie otorgan mayores privilegios a la gestión de usuarios, y a la mensajería de depuración y de error. Esos mensajes proporcionan inadvertidamente pistas que permiten intrusiones maliciosas y que ponen en riesgo la seguridad. Las consolas serie no están cifradas por lo que son menos seguras que las conexiones SSH.
  - Restrinja el acceso a las fuentes de alimentación, a los módulos de ventilación y a los transceptores en particular, ya que se pueden eliminar fácilmente.

  - Almacene los componentes de repuesto en un armario cerrado. Permita el acceso al armario cerrado solo al personal autorizado.
- **Registro de los números de serie**
  - Realice una marca de seguridad en todos los elementos importantes incluidos los componentes sustituibles. Utilice plumas ultravioleta o etiquetas en relieve especiales.
  - Mantenga un registro de los números de serie de todo el hardware.
  - Guarde copias de las facturas, los registros de compra y las licencias en una ubicación segura a la que el administrador del sistema pueda acceder fácilmente en caso de emergencia del sistema. Estos documentos impresos podrían ser su única prueba para demostrar la propiedad.

Seguridad de software

La mayoría de las medidas de protección del hardware se implementan por medio de medidas de software.

- Consulte la documentación del switch para obtener las directrices adicionales para la implementación de las funciones de seguridad en el firmware.
- Consulte la documentación de OFOS y de OFM para activar las funciones de seguridad disponibles para el paquete de software.
- Gestione el switch fuera de banda por medio del puerto SER MGT. Este puerto está separado del tráfico de datos y de la red general.
- Si la gestión fuera de banda no es factible, dedique un número de VLAN único específicamente para la gestión en banda.
- Cambie todas las contraseñas por defecto lo antes posible cuando instale un switch nuevo. El switch tiene una cuenta de usuario por defecto, `root`. El usuario `root` tiene privilegios de superusuario. La contraseña por defecto es `changeme`. Cambie la contraseña con el comando de Oracle ILOM `set /SP/users/root password=`*password*, preferentemente antes de conectar el switch a la red.
- Programe el cambio regular de todas las contraseñas del switch, en especial cuando se configura con cuentas de usuario adicionales.

Firmware de Oracle ILOM

Puede proteger, gestionar y supervisar los componentes del sistema de manera activa por medio del firmware de Oracle ILOM, que ya viene preinstalado en el switch. Consulte la documentación de Oracle ILOM para comprender mejor la configuración de contraseñas, la gestión de usuarios y la aplicación de funciones relacionadas con la seguridad, incluidos los protocolos de autenticación Secure Shell (SSH), Secure Socket Layer (SSL), RADIUS, Active Directory y LDAP. Para obtener directrices de seguridad específicas de Oracle ILOM, consulte la *Guía de seguridad de Oracle ILOM, versiones de firmware 3.0, 3.1 y 3.2*, que forma parte

de la biblioteca de documentación de Oracle ILOM 3.2. Puede encontrar la documentación de Oracle ILOM 3.2 en:

http://docs.oracle.com/cd/E37444_01

Seguridad de VLAN

Si configura redes de área local virtual (VLAN), por ejemplo, para la gestión de red en banda, recuerde que las VLAN comparten el ancho de banda de la red y requieren medidas de seguridad adicionales.

- Defina las VLAN para separar los clusters sensibles de los sistemas del resto de la red. De esta manera, se reduce la probabilidad de que los usuarios tengan acceso a la información almacenada en esos clientes y servidores.
- Asigne un número único de VLAN nativa a los puertos de enlace troncal.
- Limite las VLAN que se pueden transportar por medio de un enlace troncal a las que sean estrictamente necesarias.
- Desactive el protocolo de enlace troncal de VLAN (VTP), si es posible. De no ser así, configure los siguientes parámetros para el VTP: dominio de gestión, contraseña y eliminación. A continuación, defina el VTP en modo transparente.

Cuentas de usuario

- Implemente protocolos de autenticación seguros como Active Directory, LDAP y RADIUS. Use la gestión centralizada de la autenticación y la autorización.
- Limite el uso de la cuenta de superusuario `root`. En su lugar, cree cuentas de Oracle ILOM con menos privilegios solo para administración. Como directriz general, cree y use cuentas de usuario con la menor cantidad de privilegios posible, pero que sean suficientes como para realizar determinadas tareas.
- Utilice listas de control de acceso cuando corresponda.
- Defina timeouts para las sesiones ampliadas.
- Defina niveles de privilegio.
- Cree un mensaje inicial del sistema para recordar al usuario que el acceso no autorizado está prohibido.

Logs del sistema

- Active la creación de logs y envíe los logs del sistema a un host de log dedicado seguro.
- Configure la creación de logs para que incluya información de tiempo precisa mediante NTP y registros de hora.

Mantenimiento de un entorno seguro

Después de la instalación y la configuración iniciales, 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.

- "Control de energía de hardware" [13]
- "Seguimiento de activos" [13]
- "Actualizaciones para software y firmware" [13]
- "Acceso a la red" [14]
- "Protección de datos" [14]
- "Seguridad de los logs" [15]

Control de energía de hardware

Puede encender y apagar algunos sistemas de Oracle mediante software. Las unidades de distribución de energía (PDU) de algunos armarios de sistemas pueden activarse y desactivarse de manera remota. La autorización para estos comandos se suele definir durante la configuración del sistema y normalmente está limitada a los administradores del sistema y al personal de mantenimiento. Consulte la documentación de su sistema o armario para obtener más información.

Seguimiento de activos

Utilice los números de serie para hacer un seguimiento del inventario. Oracle incrusta números de serie en el firmware en SP, SCP y placas principales. Consulte la documentación del switch para obtener instrucciones sobre cómo leer estos números de serie.

También puede utilizar lectores inalámbricos de identificación por radiofrecuencia (RFID) para simplificar aún más el seguimiento de los activos. Las notas del producto de Oracle *Cómo realizar un seguimiento de los activos del sistema Oracle Sun mediante RFID* están disponibles en:

`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf`

Actualizaciones para software y firmware

Mantenga actualizadas las versiones de software y firmware del switch.

- Consulte periódicamente si hay actualizaciones.
- Instale siempre la versión publicada más reciente del software o del firmware.
- Instale los parches de seguridad necesarios para el software.

Compruebe la disponibilidad de las actualizaciones y de los parches en:

http://support.oracle.com

Acceso a la red

Siga estas directrices para proteger el acceso local y remoto a los sistemas:

- Implemente la seguridad de los puertos para limitar el acceso en función de una dirección MAC. Desactive la función de enlace troncal automático en todos los puertos.
- Limite la configuración remota a direcciones IP específicas mediante SSH en lugar de Telnet. Telnet acepta nombres de usuario y contraseñas en texto no cifrado y, como consecuencia, permite potencialmente que todos los miembros del segmento LAN vean las credenciales de inicio de sesión. Defina una contraseña segura para SSH.
- Configure y use la versión 3 (v3) de SNMP para proporcionar transmisiones seguras. Las versiones v1 y v2c de SNMP no son seguras y transmiten datos de autenticación en texto no cifrado.
- Si SNMP es necesario, cambie la cadena de comunidad SNMP por defecto (pública) por una cadena de comunidad segura. Los atacantes pueden pedir a una comunidad que realice un mapa de red muy completo y, posiblemente, modificar los valores de la base de información de gestión (MIB).
- No active las solicitudes `set` de SNMP a menos que sea absolutamente necesario. Si se activan, cree usuarios SNMP v3 distintos con permisos de lectura y de escritura, y de solo lectura.
- Siempre cierre la sesión después de acceder a SP o a SCP por medio de la interfaz web.
- Desactive los servicios no utilizados o innecesarios, como los servidores pequeños TCP. Solo active los servicios que sean necesarios y configúrelos de manera segura.
- Desactive el servicio IPMI si no lo usa. El protocolo IPMI no es un medio seguro para acceder al SP.
- Desactive el servicio HTTP y, en su lugar, use HTTPS. En algunos casos, es posible que sea necesario activar temporalmente HTTP para la compatibilidad con Java. Hágalo según su criterio.
- Desactive los puertos del switch que no use.

Protección de datos

Siga estas directrices para optimizar la seguridad de los datos:

- Realice copias de seguridad de los archivos de configuración del switch, guárdelas en ubicaciones seguras y remotas, y limite el acceso solo a los administradores autorizados. Los archivos de configuración deben contener comentarios descriptivos para cada valor.
- Utilice software de cifrado de datos para guardar de manera segura la información confidencial en unidades de disco duro.
- El SP, el SCP y la SSD son componentes del switch que contienen datos que equivalen al disco duro del sistema. Cuando reemplace un switch, destruya físicamente estos componentes o borre por completo todos los datos en los sistemas de archivos correspondientes. Utilice software de borrado de disco para borrar por completo todos los datos en un sistema de archivos.

Seguridad de los logs

Inspeccione y mantenga los archivos log de manera periódica.

- Revise los logs del sistema y de Oracle ILOM para detectar posibles incidentes y archivarlos de acuerdo con una política de seguridad.
- Archive y borre con regularidad los archivos log cuando excedan un tamaño razonable. Guarde los archivos en una ubicación segura para consultas o análisis estadísticos futuros.