Guía de seguridad de Oracle Dual Port QDR InfiniBand Adapter M4

Referencia: E76155-01
Junio de 2016

Referencia: E76155-01

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

Seguridad de Oracle Dual Port QDR InfiniBand Adapter M4

En este documento, se proporcionan directrices generales de seguridad para Oracle Dual Port QDR InfiniBand Adapter M4. Esta guía está destinada a administradores de red con experiencia y proporciona directrices generales e instrucciones específicas para mejorar la seguridad.

En este documento, se tratan los siguientes temas:

Principios de seguridad

Hay cuatro principios de seguridad básicos: 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 autorización (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 para el que se hayan capacitado y estén 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.

- Control

  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. Las tarjetas, los módulos y las placas base tienen números de referencia de Oracle registrados de manera electrónica.

Planificación de un entorno seguro

Utilice las siguientes notas para la instalación y la configuración de un servidor y de los equipos relacionados.

Seguridad del hardware

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

- Restricción del acceso
  - Instale los servidores y los equipos relacionados en una habitación cerrada con llave y de acceso restringido.
  - Si el equipo se instala en un bastidor con una puerta con llave, mantenga la puerta cerrada, a menos que sea necesario reparar algún componente del rack.
  - Restrinja el acceso a las consolas USB, que pueden proporcionar mayor acceso que las conexiones SSH. Los dispositivos como los controladores del sistema, las unidades de distribución de energía (PDU) y los switches de red pueden tener conexiones USB.

- Restrinja el acceso especialmente a los dispositivos de conexión en caliente o intercambio en caliente, porque se pueden eliminar fácilmente.
- Almacene las unidades sustituibles en campo (FRU) y las unidades sustituibles por el cliente (CRU) de repuesto en un armario cerrado. Restrinja el acceso al armario cerrado al personal autorizado.

- Registro de los números de serie
  - Realice una marca de seguridad en todos los elementos importantes del hardware de la computadora, como las unidades sustituibles en campo. Utilice plumas ultravioleta o etiquetas en relieve especiales.
  - Mantenga un registro de los números de serie de todo el hardware.
  - Mantenga las licencias y las claves de activación de hardware en una ubicación segura y de fácil acceso para el administrador del sistema en caso de una emergencia del sistema. Los documentos impresos podrían ser su única prueba para demostrar la propiedad.

Seguridad del software

La mayor parte de la seguridad del hardware y el software se implementa mediante medidas de software.

- Consulte la documentación incluida con el software para activar las funciones de seguridad disponibles para el software.
- Implemente la seguridad de los puertos para limitar el acceso sobre la base de las direcciones MAC. Desactive la función de enlace troncal automático en todos los puertos.
- Utilice una red dedicada de procesadores de servicio para separarlos de la red general.
- Puede iniciar un sistema de manera segura mediante una red de área extensa (WAN) o una red de área de almacenamiento (SAN). Para obtener información sobre cómo usar un inicio WAN o un inicio iSCSI para realizar un inicio seguro, consulte el manual Guía de instalación de Oracle Solaris: instalaciones basadas en red, correspondiente a su versión de sistema operativo Oracle Solaris.
- Cambie todas las contraseñas por defecto cuando instale un sistema nuevo. La mayoría de los tipos de equipos utilizan contraseñas por defecto, como changeme, que son muy conocidas y, por lo tanto, permiten el acceso no autorizado al equipo.
- Cambie cada una de las contraseñas de los switches de la red que, por defecto, pueden tener varias cuentas de usuario y contraseñas.

Directrices del sistema operativo Oracle Solaris

Consulte los documentos de directrices de seguridad de Oracle Solaris para obtener información sobre lo siguiente:

- Cómo proteger Oracle Solaris
- Cómo utilizar las funciones de seguridad de Oracle Solaris al configurar los sistemas
- Cómo trabajar de forma segura cuando se agregan aplicaciones y usuarios a un sistema
- Cómo proteger las aplicaciones basadas en red

  Los documentos de directrices de seguridad de Oracle Solaris se pueden encontrar en http://www.oracle.com/technetwork/indexes/documentation/index.html#sys_sw.

Directrices del sistema operativo Oracle Linux

Use los comandos del sistema operativo Oracle Linux para restringir el acceso al software, reforzar el sistema operativo, usar las funciones de seguridad y proteger las aplicaciones. Consulte la Guía de seguridad de Oracle Linux para la versión 6 en http://docs.oracle.com/cd/E37670_01/E36387/html/index.html.

Switches de red

Diferentes switches ofrecen distintos niveles de funciones de seguridad para puertos. Consulte la documentación del switch para aprender a realizar lo siguiente:

- Utilizar las funciones de autenticación, autorización y cuentas para el acceso local y remoto al switch.
- Gestionar switches fuera de banda (separados del tráfico de datos). Si la gestión fuera de banda no es factible, dedique un número VLAN independiente de gestión en banda.
- Utilizar la capacidad de creación de reflejo de puertos del switch de red para el acceso del sistema de detección de intrusos (IDS).
- Mantener un archivo de configuración del switch fuera de línea y limitar el acceso solamente a administradores autorizados. El archivo de configuración debe contener comentarios descriptivos para cada opción.
- Utilizar estas funciones de seguridad para puertos si están disponibles en el switch:
  - MAC Locking (Bloqueo MAC) consiste en asociar una dirección MAC (Media Access Control) de uno o más dispositivos conectados a un puerto físico en un switch. Si bloquea un puerto del switch a una dirección MAC en particular, los superusuarios no podrán crear las puertas traseras en su red con puntos de acceso peligrosos.
  - El bloqueo de MAC desactiva la conexión de una dirección MAC especificada a un switch.
  - MAC Learning (Aprendizaje MAC) utiliza los conocimientos sobre las conexiones directas de cada puerto del switch para que el switch de red pueda definir la seguridad en función de las conexiones actuales.

Seguridad del firmware de Oracle

Use una cuenta de superusuario para configurar y actualizar OpenBoot PROM (OBP) u otro firmware de Oracle. 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.

Para obtener información sobre la configuración de las variables de seguridad de OBP, consulte el Manual de referencia de comandos de OpenBoot 4.x disponible en http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069.

Firmware de Oracle ILOM

Puede proteger, gestionar y supervisar los componentes del sistema de manera activa mediante el firmware de gestión Oracle Integrated Lights Out Manager (Oracle ILOM), que está preinstalado en los servidores SPARC.

Para comprender mejor la configuración de contraseñas, la gestión de usuarios y la aplicación de funciones relacionadas con la seguridad, incluidas la autenticación de RADIUS, la capa de conexión segura (SSL) y el shell seguro (SSH), consulte la documentación de Oracle ILOM: http://docs.oracle.com/cd/E37444_01/index.html.

Seguridad de una VLAN

Si configura una red de área local virtual (VLAN), recuerde que las VLAN comparten el ancho de banda de la red y requieren medidas de seguridad adicionales.

- Defina las VLAN para separar clusters sensibles de 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 sobre un enlace troncal a las que sean estrictamente necesarias.
- Desactive el protocolo de enlace troncal de VLAN (VTP), si es posible. De lo contrario, configure lo siguiente para el VTP: dominio de gestión, contraseña y depuración. A continuación, defina VTP en modo transparente.

Seguridad de Infiniband

La seguridad de Infiniband (IB) es una función del tejido IB y del gestor de subred (SM) que se ejecuta en el tejido IB. Mantenga todos los hosts de IB conectados al tejido IB de manera

segura. Un tejido IB es tan seguro como el host IB menos seguro conectado al tejido. Los atacantes con acceso de usuario raíz a un host pueden desactivar un tejido IB completo. (El acceso físico también es importante en relación a esto: es posible que un atacante que puede conectar su propio host a un switch IB pueda comprometer la seguridad del tejido IB).

Si usa un adaptador Oracle Dual Port EDR InfiniBand Adapter u Oracle Dual Port QDR InfiniBand Adapter M4 en un entorno virtualizado, preste especial atención a la seguridad del dominio físico, porque un dominio físico comprometido podría causar la exposición y la vulnerabilidad de todas las máquinas virtuales.

Para obtener más información sobre cómo proteger InfiniBand y los switches admitidos, que también ejecutan el SM, consulte la Guía de seguridad del switch InfiniBand para el switch correspondiente:

- Para Sun Datacenter InfiniBand Switch 36, consulte la Guía de seguridad del hardware Sun Datacenter InfiniBand Switch 36, disponible en: http://docs.oracle.com/cd/E36265_01/.
- Para Sun Network QDR InfiniBand Gateway Switch, consulte la Guía de seguridad de hardware de Sun Network QDR InfiniBand Gateway Switch, disponible en: http://docs.oracle.com/cd/E36256_01/.
- Para el tejido IB y el SM en un switch Oracle Virtual Network InfiniBand, consulte: http://docs.oracle.com/cd/E38500_01/.

Cuentas de usuario

- Si es posible, configure los protocolos de acceso RADIUS y TACACS+: RADIUS (servicio de autenticación remota telefónica de usuario) es un protocolo cliente/servidor que protege las redes contra el acceso no autorizado.

  TACACS+ (sistema de control de acceso mediante controlador de acceso desde terminales) es un protocolo que permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si un usuario tiene acceso a la red.
- Limite el uso de la cuenta de superusuario (root). Tiene privilegios especiales, que si se usan de manera incorrecta, pueden afectar la seguridad de manera negativa. En su lugar, siempre que sea posible, use otras cuentas de usuario con menos privilegios. Esto se aplica al sistema operativo del host (Solaris, Linux) y a Oracle ILOM.
- 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 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, 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 del hardware

Puede usar software para encender y apagar algunos sistemas de Oracle. Las unidades de distribución de energía (PDU) de algunos armarios de sistemas se pueden activar y desactivar 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 del sistema o del armario para obtener más información.

Seguimiento de activos

Utilice los números de serie para hacer 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. Las notas del producto de Oracle, Cómo realizar un seguimiento de sus 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 las versiones del firmware y el software del host relacionado (controlador, herramientas de espacio de usuario) actualizadas en el equipo del servidor.

- Busque actualizaciones con regularidad.

- Instale siempre la versión publicada más reciente del software o el firmware.
- Instale los parches de seguridad necesarios para el software.
- Recuerde que los dispositivos como los switches de red también incluyen firmware, y pueden requerir parches y actualizaciones de firmware.

Compruebe la disponibilidad de las actualizaciones y los parches en https://support.oracle.com.

Acceso de red

Siga estas directrices para garantizar 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.
- Utilice la versión 3 de SNMP para proporcionar transmisiones seguras. Las primeras versiones 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 por una cadena de comunidad segura. Algunos productos tienen el valor PUBLIC establecido como cadena de comunidad SNMP por defecto. Los atacantes pueden enviar una consulta a una comunidad para obtener un mapa de red muy completo y, posiblemente, modificar los valores de la base de información de gestión (MIB).
- Siempre cierre la sesión después de usar el controlador del sistema si este utiliza una interfaz de explorador.
- Desactive los servicios de red innecesarios, como servidores pequeños TCP o HTTP. Active los servicios de red necesarios y configure estos servicios de manera segura.

Protección de datos

Siga estas directrices para optimizar la seguridad de los datos:

- Realice una copia de seguridad de datos importantes mediante dispositivos, como discos duros externos, pen drives o memorias extraíbles. Almacene los datos copiados en una segunda ubicación segura fuera del sitio.
- Utilice software de cifrado de datos para guardar de manera segura la información confidencial en unidades de disco duro.
- Al desechar una unidad de disco duro antigua, destruya físicamente la unidad o borre por completo todos los datos almacenados en ella. Después suprimir los archivos o de cambiar el formato de una unidad, aún se puede recuperar la información de la unidad. La supresión

de los archivos o el cambio de formato de la unidad eliminan únicamente las tablas de direcciones de la unidad. Utilice software de borrado del disco para borrar por completo todos los datos de una unidad.

Seguridad de los logs

Inspeccione y mantenga los archivos log 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.