

Guía de seguridad de Oracle® Server X5-4

Guía de seguridad



Referencia: E64502-01
Junio de 2015

Referencia: E64502-01

Copyright © 2015, Oracle y/o sus filiales. Todos los derechos reservados.

Este software y la documentación relacionada están sujetos a un contrato de licencia que incluye restricciones de uso y revelación, y se encuentran protegidos por la legislación sobre la propiedad intelectual. A menos que figure explícitamente en el contrato de licencia o esté permitido por la ley, no se podrá utilizar, copiar, reproducir, traducir, emitir, modificar, conceder licencias, transmitir, distribuir, exhibir, representar, publicar ni mostrar ninguna parte, de ninguna forma, por ningún medio. Queda prohibida la ingeniería inversa, desensamblaje o descompilación de este software, excepto en la medida en que sean necesarios para conseguir interoperabilidad según lo especificado por la legislación aplicable.

La información contenida en este documento puede someterse a modificaciones sin previo aviso y no se garantiza que se encuentre exenta de errores. Si detecta algún error, le agradeceremos que nos lo comuniqué por escrito.

Si este software o la documentación relacionada se entrega al Gobierno de EE.UU. o a cualquier entidad que adquiera las licencias en nombre del Gobierno de EE.UU. entonces aplicará la siguiente disposición:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Este software o hardware se ha desarrollado para uso general en diversas aplicaciones de gestión de la información. No se ha diseñado ni está destinado para utilizarse en aplicaciones de riesgo inherente, incluidas las aplicaciones que pueden causar daños personales. Si utiliza este software o hardware en aplicaciones de riesgo, usted será responsable de tomar todas las medidas apropiadas de prevención de fallos, copia de seguridad, redundancia o de cualquier otro tipo para garantizar la seguridad en el uso de este software o hardware. Oracle Corporation y sus subsidiarias declinan toda responsabilidad derivada de los daños causados por el uso de este software o hardware en aplicaciones de riesgo.

Oracle y Java son marcas comerciales registradas de Oracle y/o sus subsidiarias. Todos los demás nombres pueden ser marcas comerciales de sus respectivos propietarios.

Intel e Intel Xeon son marcas comerciales o marcas comerciales registradas de Intel Corporation. Todas las marcas comerciales de SPARC se utilizan con licencia y son marcas comerciales o marcas comerciales registradas de SPARC International, Inc. AMD, Opteron, el logotipo de AMD y el logotipo de AMD Opteron son marcas comerciales o marcas comerciales registradas de Advanced Micro Devices. UNIX es una marca comercial registrada de The Open Group.

Este software o hardware y la documentación pueden proporcionar acceso a, o información sobre contenidos, productos o servicios de terceros. Oracle Corporation o sus filiales no son responsables y por ende desconocen cualquier tipo de garantía sobre el contenido, los productos o los servicios de terceros a menos que se indique otra cosa en un acuerdo en vigor formalizado entre Ud. y Oracle. Oracle Corporation y sus filiales no serán responsables frente a cualesquiera pérdidas, costos o daños en los que se incurra como consecuencia de su acceso o su uso de contenidos, productos o servicios de terceros a menos que se indique otra cosa en un acuerdo en vigor formalizado entre Ud. y Oracle.

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 básica 7**
- Uso de las herramientas de gestión y configuración del servidor 9**
 - Seguridad de Oracle System Assistant 9
 - Seguridad de Oracle ILOM 10
 - Seguridad de Oracle Hardware Management Pack 11
- Planificación de un entorno seguro 13**
 - Directrices de seguridad del sistema operativo 13
 - Conmutadores y puertos de red 14
 - Seguridad de una VLAN 14
 - Seguridad de Infiniband 15
 - Seguridad física del hardware 15
 - Seguridad del software 16
- Mantenimiento de un entorno seguro 17**
 - Control de energía del hardware 17
 - Seguimiento de activos 17
 - Actualizaciones para software y firmware 18
 - Seguridad de red 18
 - Protección de datos y seguridad 19
 - Mantenimiento de logs 19

Seguridad básica

En este documento, se proporcionan directrices de seguridad generales para ayudarlo a proteger el servidor Oracle, las interfaces de red del servidor y los conmutadores de red conectados.

Nota - Póngase en contacto con el responsable de la seguridad de TI para conocer los requisitos de seguridad adicionales relacionados con el sistema y el entorno específico.

En esta sección, se tratan los cuatro principios de seguridad básicos que se deben respetar al utilizar el hardware y el software: acceso, autenticación, autorización y contabilidad.

■ Acceso

El acceso se refiere al acceso físico al hardware, o al acceso físico o virtual al software.

- Utilice los controles físicos y de software para proteger el hardware y los datos frente a posibles intrusiones.
- Consulte la documentación que se facilita con el software para activar cualquier función de seguridad disponible para el software.
- Instale servidores y 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 bastidor.
- Restrinja el acceso a conectores o puertos, 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 conmutadores de red proporcionan conectores y puertos.
- Restrinja el acceso a los dispositivos de conexión o intercambio en caliente, en especial, porque se pueden extraer 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 a personal autorizado.

■ Autenticación

La autenticación se refiere a garantizar que los usuarios de hardware o software sean quienes dicen ser.

- Configure las funciones de autenticación, como un sistema de contraseña en sus sistemas operativos de plataforma, para garantizar 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.
 - Para las cuentas de usuario: use listas de control de acceso cuando corresponda, establezca tiempos de espera para sesiones prolongadas y establezca niveles de privilegio para los usuarios.
 - **Autorización**

La autorización se refiere a las restricciones que se aplican al personal para trabajar con hardware o software.

 - 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**

La contabilidad se refiere a las funciones de software y hardware que se utilizan para supervisar la actividad de inicio de sesión y el mantenimiento de 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 estas cuentas pueden acceder a comandos importantes.
 - Mantenga un registro de los números de serie de todo el hardware. Utilice los números de serie de los componentes para hacer un seguimiento de los activos del sistema. Los números de referencia de Oracle se registran electrónicamente en tarjetas, módulos y placas base, y pueden utilizarse para el inventario.
 - Para detectar los componentes y realizar un seguimiento de ellos, realice una marca de seguridad en todos los elementos de hardware del equipo que sean importantes, como las unidades sustituibles en campo. Utilice plumas ultravioleta o etiquetas en relieve especiales.

Uso de las herramientas de gestión y configuración del servidor

Cuando utilice las herramientas de software y firmware para configurar y gestionar el servidor, siga estas directrices de seguridad.

- [“Seguridad de Oracle System Assistant” \[9\]](#)
- [“Seguridad de Oracle ILOM” \[10\]](#)
- [“Seguridad de Oracle Hardware Management Pack” \[11\]](#)

Seguridad de Oracle System Assistant

Oracle System Assistant es una herramienta preinstalada que lo ayuda a configurar y actualizar el hardware del servidor, y a instalar sistemas operativos compatibles, de manera local o remota. Para obtener información sobre cómo usar Oracle System Assistant, consulte la *Guía de administración de los servidores Oracle serie X5* en:

<http://www.oracle.com/goto/x86AdminDiag/docs>

La siguiente información lo ayudará a comprender los problemas de seguridad relacionados con Oracle System Assistant.

- **Oracle System Assistant contiene un entorno raíz de inicio.**

Oracle System Assistant es una aplicación que se ejecuta en una unidad flash USB interna preinstalada. Está incorporada en un entorno raíz Linux de inicio. Oracle System Assistant también proporciona la capacidad de acceder a su shell raíz subyacente. Los usuarios que tienen acceso físico al sistema o que tienen acceso remoto de teclado, video, mouse y medios de almacenamiento (KVMS) al sistema mediante Oracle ILOM podrán acceder a Oracle System Assistant y al shell raíz.

Un entorno raíz se puede utilizar para cambiar las políticas y la configuración del sistema, y para acceder a los datos almacenados en otros discos. Se recomienda que el acceso físico al servidor sea seguro, y que los privilegios de administrador y consola para los usuarios de Oracle ILOM se asignen con moderación.

- **Oracle System Assistant monta un dispositivo de almacenamiento USB al que el sistema operativo puede acceder.**

Además de ser un entorno de inicio, Oracle System Assistant también se monta como un dispositivo de almacenamiento USB (unidad flash) al que el sistema operativo del host puede acceder después de la instalación. Esto es útil cuando se accede a herramientas y controladores para el mantenimiento y la reconfiguración. El dispositivo de almacenamiento USB de Oracle System Assistant se puede leer y escribir, y podría ser utilizado por distintos virus.

Se recomienda aplicar al dispositivo de almacenamiento de Oracle System Assistant los mismos métodos utilizados para proteger discos, incluidos comprobaciones de integridad y análisis de virus regulares.

■ **Oracle System Assistant se puede desactivar.**

Oracle System Assistant es una herramienta útil para ayudar a configurar el servidor, actualizar y configurar el firmware, e instalar el sistema operativo del host. Sin embargo, si las implicancias de seguridad descritas anteriormente no son aceptables, o si la herramienta no es necesaria, Oracle System Assistant se puede desactivar. La desactivación de Oracle System Assistant implica que el sistema operativo host ya no podrá acceder al dispositivo de almacenamiento USB. Asimismo, no se podrá iniciar Oracle System Assistant.

Puede desactivar Oracle System Assistant desde la herramienta o desde BIOS. Una vez desactivada, la aplicación Oracle System Assistant solo se puede volver a activar desde la utilidad de configuración de BIOS. Se recomienda que la configuración de BIOS esté protegida con contraseña, de manera que solo los usuarios autorizados puedan volver a activar Oracle System Assistant. Para obtener información sobre cómo desactivar y volver a activar Oracle System Assistant, consulte la Guía de administración de los servidores Oracle serie X4 en:

<http://www.oracle.com/goto/x86AdminDiag/docs>

Seguridad 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 este servidor, en otros servidores x86 de Oracle y en algunos servidores SPARC de Oracle.

Utilice una red interna dedicada para el procesador de servicio (SP) de manera de separarlo de la red general. Oracle ILOM proporciona funciones de control y supervisión de servidor para administradores del sistema. Según el nivel de autorización otorgado a los administradores, estas funciones pueden incluir la habilidad de apagar el servidor, crear cuentas de usuario, montar dispositivos de almacenamiento remoto, etc. Por lo tanto, para mantener un entorno confiable y seguro para Oracle ILOM, el puerto de gestión de red dedicado o el puerto de gestión de banda lateral en el servidor debe estar siempre conectado a una red interna de confianza o a una red privada o de gestión segura.

Limite el uso de la cuenta de administrador predeterminada (root) al inicio de sesión inicial de Oracle ILOM. Esta cuenta de administrador predeterminada se proporciona solo para asistir

con la instalación de servidor inicial. Por lo tanto, para garantizar el entorno más seguro, debe cambiar la contraseña de administrador predeterminada (changeme) en la configuración inicial del sistema. Además de cambiar la contraseña para la cuenta de administrador predeterminada, se deben establecer nuevas cuentas de usuario con contraseñas únicas y niveles de autorización asignados para cada usuario nuevo de Oracle ILOM.

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, Secure Socket Layer (SSL) y Secure Shell (SSH), consulte la documentación de Oracle ILOM. Si desea obtener directrices de seguridad específicas de Oracle ILOM, consulte la *Guía de seguridad de Oracle Integrated Lights Out Manager (ILOM) 3.1*, que forma parte de la biblioteca de documentación de Oracle ILOM para la versión de Oracle ILOM que utiliza. Puede encontrar la documentación de Oracle ILOM en:

<http://www.oracle.com/goto/ILOM/docs>

Seguridad de Oracle Hardware Management Pack

Oracle Hardware Management Pack está disponible para su servidor, para muchos otros servidores x86 y para algunos servidores SPARC. Oracle Hardware Management Pack cuenta con dos componentes: un agente de supervisión SNMP y una familia de herramientas de interfaz de la línea de comandos (herramientas CLI) compatibles con distintos sistemas operativos para gestionar el servidor.

Con los complementos SNMP del agente de gestión de hardware, puede usar SNMP para supervisar los servidores de Oracle y los módulos de los servidores desde el centro de datos con la ventaja de no tener que conectarse con dos puntos de gestión, el host y Oracle ILOM. Esta funcionalidad le permite usar una dirección IP única (la dirección IP del host) para supervisar varios servidores y módulos de servidor. Los complementos SNMP se ejecutan en el sistema operativo del host de los servidores de Oracle.

Puede usar las herramientas de CLI del servidor Oracle para configurar servidores Oracle. Las herramientas de la interfaz de línea de comandos funcionan con Oracle Solaris, Oracle Linux, Oracle VM, otras variantes de los sistemas operativos Linux y Microsoft Windows.

Para obtener más información sobre estas funciones, consulte la documentación de Oracle Hardware Management Pack. Si desea obtener directrices de seguridad específicas de Oracle Hardware Management Pack, consulte la *Guía de seguridad de Oracle Hardware Management Pack (HMP)*, que forma parte de la biblioteca de documentación de Oracle Hardware Management Pack. Puede encontrar la documentación de Oracle Hardware Management Pack en:

<http://www.oracle.com/goto/OHMP/docs>

Planificación de un entorno seguro

Utilice las siguientes notas antes de la instalación y la configuración de un servidor y equipos relacionados, o después de ellas.

Se incluyen los siguientes temas:

- “Directrices de seguridad del sistema operativo” [13]
- “Conmutadores y puertos de red” [14]
- “Seguridad de una VLAN” [14]
- “Seguridad de Infiniband” [15]
- “Seguridad física del hardware” [15]
- “Seguridad del software” [16]

Directrices de seguridad del sistema operativo

Consulte los documentos del sistema operativo Oracle para obtener información sobre lo siguiente:

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

Los documentos de la guía de seguridad para los sistemas operativos Oracle compatibles forman parte de la biblioteca de documentación del sistema operativo. Para encontrar el documento de la guía de seguridad de un sistema operativo Oracle, vaya a la biblioteca de documentación del sistema operativo Oracle:

Sistema operativo	Enlace
SO Oracle Solaris	http://docs.oracle.com/cd/E23824_01/html/819-3195/index.html
Sistema operativo Oracle Linux	http://linux.oracle.com
Sistema operativo Oracle VM	http://www.oracle.com/technetwork/documentation/vm-096300.html

Para obtener más información sobre sistemas operativos de otros proveedores, como Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Windows y VMware ESXi, consulte la documentación de los proveedores.

Conmutadores y puertos de red

Diferentes conmutadores ofrecen distintos niveles de funciones de seguridad para puertos. Consulte la documentación del conmutador para aprender a realizar las tareas detalladas a continuación:

- Utilice las funciones de autenticación, autorización y contabilidad (AAA) para el acceso local y remoto al conmutador.
- Cambie todas las contraseñas de los conmutadores de la red que puedan tener múltiples contraseñas y cuentas de usuario de manera predeterminada.
- Gestione los conmutadores fuera de banda (separados del tráfico de datos). Si la gestión fuera de banda no es factible, dedique un número de red de área local virtual (VLAN) aparte para la gestión en banda.
- Utilizar la capacidad de duplicación de puertos del conmutador de la red para el acceso del sistema de detección de intrusos (IDS).
- Mantener un archivo de configuración del conmutador fuera de línea y limite el acceso sólo a administradores autorizados. El archivo de configuración debe contener comentarios descriptivos para cada opción.
- Implementar la seguridad de los puertos para limitar el acceso basándose en las direcciones MAC. Desactivar la función de enlace troncal automático en todos los puertos.
- Utilizar estas funciones de seguridad para puertos si están disponibles en el conmutador:
 - **El bloqueo de MAC** consiste en asociar una dirección MAC (Media Access Control) de uno o más dispositivos conectados a un puerto físico en un conmutador. Si bloquea un puerto del conmutador a una dirección MAC en particular, los superusuarios no pueden crear las puertas traseras en su red con peligrosos puntos de acceso.
 - El **bloqueo de MAC** desactiva la conexión de una dirección MAC especificada a un conmutador.
 - **MAC Learning** (Aprendizaje MAC): utiliza el conocimiento sobre las conexiones directas de cada puerto del conmutador de manera que el conmutador de la red pueda definir la seguridad en función de las conexiones actuales.

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 los clústeres 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 de VLAN nativo único 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 no ser así, configure los siguientes parámetros para el VTP: dominio de gestión, contraseña y eliminación. A continuación, defina VTP en modo transparente.

Seguridad de Infiniband

Mantenga los host Infiniband protegidos. Un tejido Infiniband sólo es tan seguro como su host Infiniband menos seguro.

- Tenga en cuenta que realizar una partición no protege un tejido Infiniband. La partición sólo ofrece aislamiento de tráfico Infiniband entre máquinas virtuales de un host.
- Utilice una configuración de VLAN estática, cuando sea posible.
- Desactive los puertos de conmutador no utilizados y asígneles un número de VLAN que no esté en uso.

Seguridad física 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 servidores y 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 bastidor. Cierre la puerta con llave después de realizar el servicio del equipo.
 - 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 conmutadores de red pueden tener conexiones USB.
 - Restrinja el acceso a los dispositivos de conexión o intercambio en caliente, en especial, porque se pueden extraer fácilmente.
 - 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**
 - Realice una marca de seguridad en todos los elementos importantes del hardware del equipo, 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 a la que el administrador del sistema pueda acceder fácilmente en caso de emergencias del sistema. Los documentos impresos podrían ser su única prueba para demostrar la propiedad.

Seguridad del software

La mayoría de las medidas de protección del hardware se implementan a través de medidas de software.

- Cambie todas las contraseñas predeterminadas cuando instale un sistema nuevo. La mayoría de los tipos de equipos utilizan contraseñas predeterminadas, 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 conmutadores de la red que, de manera predeterminada, pueden tener varias cuentas de usuario y contraseñas.
- Limite el uso de la cuenta de administrador predeterminada (root) a un solo usuario administrador. Siempre cree una nueva cuenta de Oracle ILOM para cada usuario nuevo. Asegúrese de que siempre se asignen una contraseña única y privilegios de nivel de autorización adecuados (operador, administrador, etc.) a cada nueva cuenta de usuario de Oracle ILOM.
- Utilice una red dedicada de procesadores de servicio para separarlos de la red general.
- Proteja el acceso a consolas USB. Los dispositivos, como los controladores del sistema, las unidades de distribución de alimentación (PDU) y los conmutadores de red, pueden tener conexiones USB, que pueden proporcionar mayor acceso que las conexiones SSH.
- Consulte la documentación que se facilita con el software para activar cualquier función de seguridad disponible para el software.
- Implemente la seguridad de los puertos para limitar el acceso basándose en las direcciones MAC. Desactive la función de enlace troncal automático en todos los puertos.

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” \[17\]](#)
- [“Seguimiento de activos” \[17\]](#)
- [“Actualizaciones para software y firmware” \[18\]](#)
- [“Seguridad de red” \[18\]](#)
- [“Protección de datos y seguridad” \[19\]](#)
- [“Mantenimiento de logs” \[19\]](#)

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 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 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 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 sus versiones de software y firmware actualizadas en el equipo de servidor.

- Consulte periódicamente si hay actualizaciones.
- Instale siempre la versión publicada más reciente del software o el firmware en su equipo.
- Instale los parches de seguridad necesarios para el software.
- Recuerde que los dispositivos, como los conmutadores de red y Express Modules, contienen firmware y pueden requerir parches y actualizaciones de firmware.

Seguridad de red

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

- 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 del protocolo simple de gestión de redes (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 predeterminada por una cadena de comunidad segura. Algunos productos tienen el valor PUBLIC establecido como cadena de comunidad SNMP predeterminada. Los atacantes pueden pedir a una comunidad que realice un mapa de red muy completo y, posiblemente, que modifiquen los valores de la base de información gestionada (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, por ejemplo, el protocolo de control de transmisiones (TCP) o el protocolo de transferencia de hipertexto (HTTP). Active los servicios de red necesarios y configure estos servicios de manera segura.
- Siga las medidas de seguridad LDAP al utilizar LDAP para acceder al sistema. Consulte la Guía de seguridad de Oracle ILOM en: <http://www.oracle.com/goto/ILOM/docs>.
- Cree un rótulo para mencionar que el acceso no autorizado está prohibido.
- Utilice listas de control de acceso cuando corresponda.
- Defina tiempos de espera para las sesiones ampliadas y defina los niveles de privilegios.
- Utilice las funciones de autenticación, autorización y contabilidad (AAA) para el acceso local y remoto a un conmutador.

- Si es posible, utilice los protocolos de seguridad de RADIUS y TACACS+:
 - RADIUS (Remote Authentication Dial in User Service) es un protocolo cliente/servidor que protege redes frente a accesos no autorizados.
 - 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.
- Utilice la capacidad de reflejo de puertos del conmutador para el acceso del sistema de detección de intrusos (IDS).
- Implemente la seguridad de los puertos para limitar el acceso en función de una dirección MAC. Deshabilite la función de enlace troncal automático en todos los puertos.

Protección de datos y seguridad

Siga estas directrices para maximizar la seguridad y la protección de los datos.

- Realice una copia de seguridad de datos importantes mediante dispositivos como discos duros externos o dispositivos de almacenamiento USB. 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 la unidad. Después suprimir los archivos o de volver a formatear una unidad, aún se puede recuperar la información de la unidad. La supresión de los archivos o el formateo de la unidad elimina únicamente las tablas de direcciones de la unidad. Utilice software de barrido del disco para borrar por completo todos los datos de una unidad.

Mantenimiento de logs

Inspeccione y mantenga los archivos log de manera periódica. Use estos métodos para proteger los archivos de registro.

- Active el registro y envíe los registros del sistema a un host de registro dedicado seguro.
- Configure el registro para incluir información de tiempo precisa mediante el protocolo de hora de red (NTP) e indicadores de fecha y hora.
- Revise los registros para detectar posibles incidentes y archívelos de acuerdo con una política de seguridad.
- Periódicamente, retire los archivos de registro cuando superen un tamaño razonable. Mantenga copias de los archivos retirados para utilizarlos en el futuro para referencia o análisis estadístico.

