

Sun Server X4-8

Guía de seguridad

ORACLE®

Referencia: E55452-01
Junio de 2014

Copyright © 2014, 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 comunique por escrito.

Si este software o la documentación relacionada se entrega al Gobierno de EE.UU. o a cualquier entidad que adquiera licencias en nombre del Gobierno de EE.UU. se 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 ofrecer acceso a contenidos, productos o servicios de terceros o información sobre los mismos. Ni Oracle Corporation ni sus subsidiarias serán responsables de ofrecer cualquier tipo de garantía sobre el contenido, los productos o los servicios de terceros y renuncian explícitamente a ello. Oracle Corporation y sus subsidiarias no se harán responsables de las pérdidas, los costos o los daños en los que se incurra como consecuencia del acceso o el uso de contenidos, productos o servicios de terceros.

Contenido

Seguridad básica	5
Acceso	5
Autenticación	6
Autorización	6
Cuentas y auditoría	6
 Uso seguro de las herramientas de configuración y gestión del servidor	 9
Seguridad de Oracle System Assistant	9
Seguridad de Oracle ILOM	10
Seguridad de Oracle Hardware Management Pack	12
 Planificación de un entorno seguro	 13
Protección mediante contraseñas	13
Directrices de seguridad del sistema operativo	14
Puertos y conmutadores de red	14
Seguridad de VLAN	15
Seguridad de Infiniband	16
 Mantenimiento de un entorno seguro	 17
Control de energía	17
Seguimiento de activos	17
Actualizaciones de software y firmware	18
Seguridad de red	18
Protección de datos y seguridad	19
Mantenimiento de logs	20

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.

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.

Existen principios de seguridad básicos que debe cumplir al utilizar todo el hardware y software. En esta sección, se describen los cuatro principios de seguridad básicos:

- “Acceso” [5]
- “Autenticación” [6]
- “Autorización” [6]
- “Cuentas y auditoría” [6]

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 contra posibles intrusiones.
- Cambie todas las contraseñas predeterminadas cuando instale un sistema nuevo. La mayoría de los tipos de equipos utilizan contraseñas predeterminadas, como changeme, que son ampliamente conocidas y, por lo tanto, es posible que permitan el acceso no autorizado al hardware o software.
- Consulte la documentación incluida con el software para activar las funciones de seguridad disponibles para el software.
- Instale servidores y equipos relacionados en una habitación cerrada con llave y con 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 físico a los puertos USB, puertos de red y consolas del sistema. Los servidores y los conmutadores de red tienen puertos y conexiones de consola que ofrecen acceso directo al sistema.

- Restrinja la capacidad para reiniciar el sistema mediante la red.
- Restrinja el acceso a los dispositivos de conexión en marcha o sustitución en marcha particularmente, ya que pueden extraerse con facilidad.
- 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 indica la manera en que se identifica un usuario, generalmente mediante información confidencial, como nombre de usuario y contraseña. La autenticación garantiza que los usuarios del hardware o software sean quienes dicen ser.

- Configure las funciones de autenticación como un sistema de contraseña en los sistemas operativos de la 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 equipos.
- Para las cuentas de usuario: use listas de control de acceso cuando corresponda, establezca tiempos de espera para sesiones prolongadas y establezca niveles de privilegios para los usuarios.

Autorización

La autorización permite que los administradores controlen las tareas que puede realizar un usuario o los privilegios que puede utilizar. El personal únicamente puede realizar las tareas y usar los privilegios que le han sido asignados. La autorización se refiere a las restricciones que se aplican al personal para trabajar con el hardware o software.

- Permita que el personal trabaje únicamente con el hardware y el software para los cuales fueron capacitados y entrenados.
- 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.

Cuentas y auditoría

La función de cuentas y auditoría implica mantener un registro de la actividad de un usuario en el sistema. Los servidores Oracle tienen funciones de software y hardware que permiten que los administradores supervisen la actividad de inicio de sesión y mantengan inventarios de hardware.

- Use los logs del sistema para supervisar los inicios de sesión de los usuarios. Supervise las cuentas de servicio y administrador del sistema particularmente, ya que esas cuentas permiten acceder a comandos que, si se ejecutan de forma incorrecta, pueden dañar el sistema u originar la pérdida de datos. El acceso y los comandos deben supervisarse cuidadosamente mediante los logs del sistema.
- Registre los números de serie de todo el hardware. Utilice los números de serie de los componentes para realizar 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 ultravioletas o etiquetas en relieve especiales.

Uso seguro de las herramientas de configuración y gestión del servidor

Siga estas directrices de seguridad al utilizar herramientas de software y firmware para configurar y gestionar el servidor:

- “Seguridad de Oracle System Assistant” [9]
- “Seguridad de Oracle ILOM” [10]
- “Seguridad de Oracle Hardware Management Pack” [12]

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.

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 admitidos. Para obtener información sobre cómo usar Oracle System Assistant, consulte la *Guía de administración de los servidores Oracle serie X4*:

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

La siguiente información describe los problemas de seguridad relacionados con Oracle System Assistant.

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

Oracle System Assistant es una aplicación que se ejecuta en una unidad flash USB interna preinstalada. Oracle System Assistant está incorporado en un entorno raíz Linux de inicio. Oracle System Assistant también proporciona la capacidad de acceder al shell raíz subyacente. Los usuarios que tienen acceso físico al sistema o que tienen acceso remoto KVMs (teclado, video, mouse y almacenamiento) al sistema mediante Oracle ILOM pueden 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. Para aumentar la seguridad, proteja el acceso físico al servidor y asigne privilegios de administrador y consola para los usuarios de Oracle ILOM con moderación.

El shell de Oracle System Assistant está diseñado para permitir que los usuarios con los privilegios adecuados usen las herramientas de la CLI de Oracle Hardware Management Pack para la gestión del sistema. El shell no está diseñado para proporcionar servicios de red. Los servicios de red están desactivados de forma predeterminada para garantizar el nivel más alto de seguridad y no deben activarse.

- **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 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 permite operaciones de lectura y escritura, por lo que posiblemente se vea afectado por distintos virus.

Para una mayor seguridad, se recomienda proteger el dispositivo de almacenamiento de Oracle System Assistant con los mismos métodos de protección utilizados para los discos, incluidos los análisis periódicos de virus y la comprobación de integridad.

- **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 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. Después de desactivar Oracle System Assistant, el sistema operativo host ya no tiene acceso al dispositivo de almacenamiento USB y los usuarios no podrán iniciar Oracle System Assistant.

Puede desactivar Oracle System Assistant desde la herramienta o desde el BIOS. Una vez desactivado, Oracle System Assistant solamente se puede volver a activar desde la utilidad de configuración del BIOS. Se recomienda proteger con contraseña la utilidad de configuración del BIOS, de modo que solamente los usuarios autorizados puedan volver a activar Oracle System Assistant.

- **Consulte la documentación de Oracle System Assistant.**

Para obtener información sobre las funciones de 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 activamente los componentes del sistema mediante el firmware de gestión de Oracle Integrated Lights Out Manager (Oracle ILOM), que está incrustado en los servidores x86 de Oracle y en servidores SPARC de Oracle. Según el nivel de autorización otorgado a los administradores del sistema, estas funciones pueden incluir la capacidad de apagar el servidor, crear cuentas de usuario, montar dispositivos de almacenamiento remoto, etc.

- **Use una red interna segura de confianza.**

Independientemente de que establezca una conexión de gestión física con Oracle ILOM mediante el puerto serie local, el puerto de gestión de red dedicado o el puerto de red de datos estándar, es fundamental que este puerto físico del servidor siempre esté conectado a una red interna de confianza o a una red privada o de gestión segura dedicada.

Nunca conecte el procesador de servicio (SP) de Oracle ILOM a una red pública, como Internet. Debe mantener el tráfico de gestión del SP de Oracle ILOM en una red de gestión separada y solamente otorgar acceso a los administradores del sistema.

- **Limite el uso de la cuenta de administrador predeterminada.**

Limite el uso de la cuenta de administrador predeterminada (root) al primer inicio de sesión en Oracle ILOM. Esta cuenta de administrador predeterminada se proporciona únicamente para brindar ayuda con la instalación inicial del servidor. Por lo tanto, para garantizar el entorno más seguro, debe cambiar la contraseña de administrador predeterminada (changeme) como parte de la configuración inicial del sistema. Si un usuario obtiene acceso a la cuenta de administrador predeterminada, podrá acceder libremente a todas las funciones de Oracle ILOM. Además, establezca nuevas cuentas de usuario con contraseñas únicas y asigne niveles de autorización (roles de usuario) para cada usuario nuevo de Oracle ILOM.

- **Considere cuidadosamente los riesgos al conectar el puerto serie a un servidor de terminales.**

Los dispositivos de terminal no siempre proporcionan los niveles adecuados de autorización o autenticación de usuarios requeridos para proteger la red contra intrusiones maliciosas. Para proteger el sistema contra intrusiones de red no deseadas, no establezca una conexión serie (puerto serie) a Oracle ILOM mediante cualquier tipo de dispositivo de redirección de red, como un servidor de terminales, a menos que el servidor tenga controles de acceso suficientes.

Además, determinadas funciones de Oracle ILOM, como el restablecimiento de contraseñas y el menú Preboot (Preinicio), únicamente están disponibles mediante el puerto serie físico. La conexión de un puerto serie a una red mediante un servidor de terminales no autenticado elimina la necesidad de acceso físico y disminuye la seguridad asociada con estas funciones.

- **El acceso al menú Preboot (Preinicio) requiere acceso físico al servidor.**

El menú Preboot (Preinicio) de Oracle ILOM es una utilidad eficaz que ofrece una manera de restablecer Oracle ILOM a los valores predeterminados y de actualizar el firmware si Oracle ILOM deja de responder. Una vez que se restablece Oracle ILOM, el usuario debe pulsar un botón en el servidor (predeterminado) o escribir una contraseña. La propiedad de presencia de Oracle ILOM controla este comportamiento (`check_physical_presence=true`). Para contar con máxima seguridad al acceder al menú Preboot (Preinicio), no cambie la configuración predeterminada (`true`), de modo que el acceso al menú Preboot (Preinicio) siempre requiera acceso físico al servidor.

- **Consulte la documentación de Oracle ILOM.**

Consulte la documentación de Oracle ILOM para obtener más información sobre la configuración de contraseñas, la gestión de usuarios y la aplicación de funciones

relacionadas con la seguridad. Para obtener directrices de seguridad específicas de Oracle ILOM, consulte la *Guía de seguridad de Oracle ILOM*, que forma parte de la biblioteca de documentación de Oracle ILOM. 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 de Oracle y para algunos servidores SPARC de Oracle. Oracle Hardware Management Pack cuenta con dos componentes: un agente de supervisión SNMP y una familia de herramientas de interfaz de línea de comandos (herramientas de CLI) compatibles con distintos sistemas operativos para gestionar el servidor.

- **Use los plugins de SNMP del agente de gestión de hardware.**

SNMP es un protocolo estándar utilizado para supervisar o gestionar un sistema. Con los plugins de SNMP del agente de gestión de hardware, puede usar SNMP para supervisar los servidores Oracle en el centro de datos, sin necesidad de conectarse a 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.

Los plugins de SNMP se ejecutan en el sistema operativo host de los servidores Oracle. El plugin de SNMP extiende el agente SNMP nativo en el sistema operativo host a fin de proporcionar capacidades adicionales de MIB de Oracle. Oracle Hardware Management Pack no incluye un agente SNMP. Para Linux, se agrega un módulo al agente net-snmp. Para Oracle Solaris, se agrega un módulo a Oracle Solaris Management Agent. Para Microsoft Windows, el plugin extiende el servicio SNMP nativo. La configuración de seguridad relacionada con SNMP para Oracle Hardware Management Pack es determinada por la configuración de un servicio o agente SNMP nativo, no por el plugin.

Tenga en cuenta que SNMPv1 y SNMPv2c no proporcionan cifrado y utilizan cadenas comunitarias como forma de autenticación. SNMPv3 es más seguro y es la versión recomendada, ya que utiliza el cifrado para proporcionar un canal seguro, además de contraseñas y nombres de usuario y contraseñas individuales.

- **Consulte la documentación de Oracle Hardware Management Pack.**

Para obtener más información sobre estas funciones, consulte la documentación de Oracle Hardware Management Pack. Para conocer las 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

Antes de la llegada del sistema, debe haber implementadas directrices de seguridad. Después de la llegada del sistema, las directrices de seguridad deben revisarse y ajustarse periódicamente para adaptarse a los requisitos de seguridad de la organización. Utilice la información de esta sección antes de la instalación y la configuración de un servidor y los equipos relacionados, y durante estas tareas.

En esta sección, se tratan los siguientes temas:

- [“Protección mediante contraseñas” \[13\]](#)
- [“Directrices de seguridad del sistema operativo” \[14\]](#)
- [“Puertos y conmutadores de red” \[14\]](#)
- [“Seguridad de VLAN” \[15\]](#)
- [“Seguridad de Infiniband” \[16\]](#)

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.

Protección mediante contraseñas

Las contraseñas son un aspecto importante de la seguridad, ya que una contraseña mal elegida puede originar el acceso no autorizado a los recursos de la empresa. La implementación de mejores prácticas de gestión de contraseñas garantiza que los usuarios cumplan con un conjunto de directrices para crear y proteger sus contraseñas. Los componentes típicos de una política de contraseñas deben definir:

- Longitud y seguridad de la contraseña
- Duración de la contraseña
- Práctica común de la contraseña

Aplique las siguientes prácticas estándar para la creación de contraseñas complejas y seguras:

- No cree una contraseña que contenga el nombre de usuario, el nombre del empleado o apellidos.
- No elija contraseñas que se adivinen fácilmente.
- No cree contraseñas que contengan una cadena consecutiva de números, como 12345.

- No cree contraseñas que contengan una palabra o cadena que se pueda descubrir fácilmente mediante una simple búsqueda en Internet.
- No permita que los usuarios vuelvan a utilizar la misma contraseña en varios sistemas.
- No permita que los usuarios vuelvan a utilizar contraseñas anteriores.

Cambie las contraseñas periódicamente. Esto ayuda a evitar actividades maliciosas y garantiza que las contraseñas cumplan con las políticas de contraseñas actuales.

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 admitidos 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
Sistema operativo Oracle Solaris	http://docs.oracle.com/cd/E23824_01/html/819-3195/index.html
Sistema operativo Oracle Linux	http://www.oracle.com/technetwork/documentation/ol-1-1861776.html
Oracle VM	http://www.oracle.com/technetwork/documentation/vm-096300.html

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

Puertos y conmutadores de red

Los conmutadores de red ofrecen diferentes niveles de funciones de seguridad para puertos. Consulte la documentación del conmutador para aprender a realizar lo siguiente:

- Utilizar las funciones de autenticación, autorización y cuentas para el acceso local y remoto al conmutador.

- Cambiar todas las contraseñas de los conmutadores de red que puedan tener varias cuentas de usuario y contraseñas de forma predeterminada.
- Gestionar conmutadores fuera de banda (separados del tráfico de datos). Si la gestión fuera de banda no es posible, asigne un número de red de área local virtual (VLAN) separado para la gestión en banda.
- Utilice la capacidad de duplicación de puertos del conmutador de la red para el acceso del sistema de detección de intrusos (IDS).
- Mantenga un archivo de configuración del conmutador fuera de línea y limite el acceso solo a administradores autorizados. El archivo de configuración debe contener comentarios descriptivos para cada opción.
- 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.
- Utilice 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.
 - El **aprendizaje MAC** utiliza el conocimiento sobre las conexiones directas de cada puerto del conmutador de manera que el conmutador de red pueda definir la seguridad en función de las conexiones actuales.

Seguridad de 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.

- Al usar VLAN, separe los 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 de VLAN nativo único a los puertos de enlace troncal.
- Limite las VLAN que se pueden transportar mediante un enlace troncal a las que son estrictamente necesarias.
- Desactive el protocolo de enlace troncal (VTP) de VLAN, si es posible. De lo contrario, configure lo siguiente para el VTP: dominio de gestión, contraseña y eliminación. A continuación, defina VTP en modo transparente.
- Utilice configuraciones de VLAN estáticas, cuando sea posible.
- Desactive los puertos de conmutador no utilizados y asígneles un número de VLAN que no esté en uso.

Seguridad de Infiniband

Mantenga los host Infiniband protegidos. Un tejido Infiniband tiene la misma seguridad que el host Infiniband menos seguro.

Tenga en cuenta que la partición no protege a un tejido Infiniband. La partición solamente ofrece aislamiento de tráfico Infiniband entre máquinas virtuales en un host.

Mantenimiento de un entorno seguro

Después de la instalación y la configuración iniciales, use las funciones de seguridad de hardware y software de Oracle para seguir controlando los activos de hardware y software.

- [“Control de energía” \[17\]](#)
- [“Seguimiento de activos” \[17\]](#)
- [“Actualizaciones de software y firmware” \[18\]](#)
- [“Seguridad de red” \[18\]](#)
- [“Protección de datos y seguridad” \[19\]](#)
- [“Mantenimiento de logs” \[20\]](#)

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.

Control de energía

Puede usar software para encender y apagar algunos sistemas Oracle. Las unidades de distribución de energía (PDU) de algunos armarios del sistema pueden activarse y desactivarse de manera remota. La autorización de estos comandos suele definirse durante la configuración del sistema y generalmente está limitada a los administradores del sistema y al personal del servicio de asistencia.

Consulte la documentación del sistema o el armario para obtener más información.

Seguimiento de activos

Utilice los números de serie para realizar un seguimiento del inventario. Oracle incrusta 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 (LAN).

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 de software y firmware

Las mejoras de seguridad están incluidas en los parches y las nuevas versiones de software. La gestión de parches preventiva y eficaz es una parte fundamental de la seguridad del sistema. Para mejores prácticas de seguridad, actualice el sistema con la versión de software más reciente y todos los parches de seguridad necesarios.

- Busque periódicamente actualizaciones de software y parches de seguridad.
- 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 conmutadores de red también contienen firmware y pueden requerir parches y actualizaciones de firmware.

Seguridad de red

Una vez que las redes se configuraron según los principios de seguridad, es necesario realizar una revisión y un mantenimiento periódicos.

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, puede permitir que todos los miembros del segmento de red de área local (LAN) vean las credenciales de inicio de sesión. Defina una contraseña segura para SSH.
- Utilice la versión 3 del protocolo simple de administración 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 solicitar a una comunidad que realice un mapa de red muy completo y, posiblemente, que modifique los valores de la base de información gestionada (MIB).
- Siempre cierre la sesión después de usar el controlador del sistema si este controlador utiliza una interfaz de explorador.
- Desactive los servicios de red innecesarios, por ejemplo, el protocolo de control de transmisión (TCP) o el protocolo de transferencia de hipertexto (HTTP). Active los servicios de red necesarios y configure estos servicios de manera segura.

- Cree un mensaje de banner que aparezca durante el inicio de sesión para indicar que el acceso no autorizado está prohibido. Puede informar a los usuarios sobre reglas o políticas importantes. El banner se puede utilizar para advertir a los usuarios sobre restricciones de acceso especiales para un sistema determinado o para recordar a los usuarios sobre políticas de contraseñas o uso apropiado.
- Utilice listas de control de acceso para aplicar restricciones, cuando corresponda.
- Establezca tiempos de espera para sesiones prolongadas y establezca niveles de privilegios.
- Utilice las funciones de autenticación, autorización y cuentas para el acceso local y remoto a un conmutador.
- Si es posible, utilice los protocolos de seguridad de 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.
- Siga las medidas de seguridad de LDAP al utilizar LDAP para acceder al sistema.
- Utilice la capacidad de reflejo de puertos del conmutador para el acceso del sistema de detección de intrusos (IDS).
- Implemente la seguridad de puertos para limitar el acceso según una dirección MAC. Desactive la función de enlace troncal automático en todos los puertos.

Para obtener más información sobre la seguridad de red, consulte la *Guía de seguridad de Oracle ILOM*, que forma parte de la biblioteca de documentación de Oracle ILOM. Puede encontrar la documentación de Oracle ILOM en:

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

Protección de datos y seguridad

Siga estas directrices para maximizar la seguridad y la protección de datos:

- Realice una copia de seguridad de los datos importantes mediante dispositivos como unidades de disco duro externas o dispositivos de almacenamiento USB. Almacene la copia de seguridad de los datos 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 log:

- Active el registro y envíe los logs del sistema a un host de log dedicado seguro.
- Configure el registro para incluir información de tiempo precisa mediante el protocolo de tiempo de red (NTP) y registros de hora.
- Realice análisis periódicos planificados de logs de dispositivos de red para detectar accesos o actividad de red inusuales.
- Revise los logs para detectar posibles incidentes y archívelos de acuerdo con una política de seguridad.
- Retire periódicamente los archivos log cuando exceden un tamaño razonable. Mantenga copias de los archivos retirados para utilizarlos en el futuro para referencia o análisis estadístico.