

Servidores de las series SPARC y Netra SPARC T5

Guía de seguridad

Copyright © 2013 , 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 filiales 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 filiales. 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 filiales 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 filiales 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.

Tabla de contenidos

1. Seguridad de los servidores de las series SPARC y Netra SPARC T5	5
Descripción de los principios de seguridad	5
Planificación de un entorno seguro	6
Seguridad de hardware	6
Seguridad de software	6
Seguridad de firmware	7
Seguridad de OpenBoot de Oracle	7
Firmware de Oracle ILOM	7
Mantenimiento de un entorno seguro	8
Controles de hardware	8
Seguimiento de activos	8
Actualizaciones para software y firmware	8
Acceso local y remoto	8
Seguridad de datos	9
Seguridad de red	9

• • • Capítulo 1

Seguridad de los servidores de las series SPARC y Netra SPARC T5

En este documento, se proporcionan directrices de seguridad generales para los servidores SPARC T5-1B, T5-2, T5-4, T5-8 y Netra SPARC T5-1B. Esta guía tiene como objetivo ayudar a garantizar la seguridad cuando se usan estos servidores con otros productos de hardware de Oracle, como conmutadores de red y tarjetas de interfaz de red.

En este capítulo, se incluyen las siguientes secciones:

- [“Descripción de los principios de seguridad” \[5\]](#)
- [“Planificación de un entorno seguro” \[6\]](#)
- [“Mantenimiento de un entorno seguro” \[8\]](#)

Descripción de los principios de seguridad

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

• **Acceso**

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

- En el caso del hardware, los límites de acceso suelen ser 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**

Todos los sistemas operativos de la plataforma proporcionan funciones de autenticación que pueden configurarse para garantizar que los usuarios sean quienes dicen ser.

La autenticación proporciona diversos grados de seguridad a través de ciertas medidas, como el uso de insignias y contraseñas.

• **Autorización**

La autorización permite que los trabajadores de la empresa trabajen únicamente con hardware y software que estén capacitados y cualificados para utilizar. Configure un sistema de permisos de

lectura, escritura y ejecución para controlar el acceso de los usuarios a los comandos, el espacio en disco, los dispositivos y las aplicaciones.

- **Contabilidad**

Utilice las funciones de contabilidad de software y de hardware de Oracle para supervisar la actividad de inicio de sesión y conservar inventarios de hardware.

- Los inicios de sesión de los usuarios se pueden supervisar mediante los registros del sistema. Las cuentas de servicio y del administrador del sistema en concreto tienen acceso a comandos importantes y deben ser supervisadas cuidadosamente mediante los registros del sistema. Los registros se suelen conservar durante un largo período, por lo que es esencial retirar periódicamente los archivos de registro cuando exceden un tamaño razonable, de acuerdo con la política de la empresa para clientes.
- Se suele realizar un seguimiento de los activos de TI de los clientes mediante números de serie. Los números de referencia de Oracle se registran electrónicamente en las tarjetas, los módulos y las placas base, y se pueden utilizar para realizar inventarios.

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.

Seguridad de hardware

El hardware físico se puede proteger con bastante facilidad limitando el acceso al hardware y registrando los números 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, cierre siempre la puerta hasta que se tenga que reparar algún componente dentro del bastidor.
- 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 en marcha o sustitución en marcha, porque se pueden eliminar 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 al personal autorizado.

- **Registro de los números de serie**

- Mantenga un registro de los números de serie de todo el hardware.
- Realice una marca de seguridad en todos los elementos importantes del hardware del equipo, como las unidades sustituibles. Utilice plumas ultravioleta o etiquetas en relieve especiales.
- 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 emergencia del sistema. Los 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 a través de medidas de software.

- Cambie todas las contraseñas predeterminadas cuando instale un sistema nuevo. La mayoría de los equipos utilizan contraseñas predeterminadas, como **changeme**, que son muy conocidas y, por lo tanto, pueden permitir el acceso no autorizado al equipo. Además, los dispositivos, como los conmutadores de red, pueden tener varias cuentas de usuario de forma predeterminada. Asegúrese de cambiar las contraseñas de todas las cuentas.
- Limite el uso de la cuenta de superusuario root. Los perfiles de usuario de Oracle Integrated Lights Out Manager (Oracle ILOM), como `operator` y `administrator`, se deben utilizar en lugar de la cuenta de superusuario siempre que sea posible.
- Utilice una red dedicada de procesadores de servicio para separarlos de la red general.
- Consulte la documentación que se facilita con el software para activar cualquier función de seguridad disponible para el software.
- Un servidor se puede iniciar de forma segura con inicio WAN o inicio iSCSI.
 - Para una versión de Oracle Solaris 10, consulte la *Guía de instalación de Oracle Solaris: instalaciones basadas en red*.
 - Para una versión de Oracle Solaris 11, consulte *Instalación de sistemas Oracle Solaris 11* para obtener información sobre el inicio WAN y la *Guía de administración del sistema: administración básica* para obtener información sobre el inicio iSCSI.

El documento *Directrices de seguridad de Oracle Solaris* proporciona información sobre lo siguiente:

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

El documento *Directrices de seguridad de Oracle Solaris* para la versión que está utilizando se encuentra en las siguientes direcciones URL:

- <http://www.oracle.com/goto/Solaris11/docs>
- <http://www.oracle.com/goto/Solaris10/docs>

Seguridad de firmware

Todos los subcomponentes del firmware del sistema Oracle solamente se pueden actualizar juntos. El firmware del sistema Oracle utiliza un proceso de actualización de firmware controlado para impedir modificaciones del firmware no autorizadas. Únicamente el superusuario o un usuario autenticado con la autorización adecuada pueden usar el proceso de actualización.

Seguridad de OpenBoot de Oracle

El acceso a la interfaz de la línea de comandos del firmware de OpenBoot de Oracle se puede proteger con contraseña usando variables de seguridad de OpenBoot.

Para obtener información sobre la configuración de las variables de seguridad de OpenBoot, consulte el *Manual de referencia de comandos de OpenBoot 4.x* en:

- <http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfid-17069>

Firmware de Oracle ILOM

Oracle Integrated Lights Out Manager (Oracle ILOM) es un firmware de gestión de sistemas que se entrega preinstalado en el servidor, el módulo de servidor, el sistema modular y otro hardware de

Oracle. Oracle ILOM permite gestionar y supervisar de forma activa los componentes instalados en el sistema. La forma en que se usa Oracle ILOM afecta la seguridad del sistema. Para obtener más información sobre el uso de este firmware al configurar contraseñas, gestionar usuarios y aplicar funciones relacionadas con la seguridad, incluidos el shell seguro (SSH), la capa de conexión segura (SSL) y la autenticación RADIUS, consulte la documentación de Oracle ILOM:

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

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.

Controles de hardware

Algunos sistemas de Oracle se pueden configurar para ser activados y desactivados por comandos de software. Además, las unidades de distribución de energía (PDU) de algunos armarios de sistemas se pueden activar y desactivar de forma remota mediante comandos de software. La autorización para estos comandos se suele configurar 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

Los números de serie de Oracle están incrustados en firmware ubicado en tarjetas opcionales y placas bases del sistema. Estos números de serie se pueden leer mediante conexiones de red de área local para el seguimiento del inventario.

Los lectores inalámbricos de identificación por radiofrecuencia (RFID) pueden simplificar aún más el seguimiento de 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

- Busque actualizaciones con regularidad.
- 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, también contienen firmware y pueden requerir parches y actualizaciones de firmware.

Acceso local y remoto

Siga estas directrices para garantizar la seguridad del acceso local y remoto a los sistemas:

- Cree un rótulo para mencionar que el acceso no autorizado está prohibido.
- Utilice las listas de control de acceso donde 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 (servicio de autenticación remota telefónica de usuario) 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 basándose en 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.
- Las primeras versiones de SNMP no son seguras y transmiten datos de autenticación en texto no cifrado. Sólo la versión 3 de SNMP puede proporcionar transmisiones seguras.
- Algunos productos se entregan con PUBLIC definido 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 bases de datos de información de administración (MIB). Si SNMP es necesario, cambie la cadena de comunidad SNMP predeterminada a una cadena de comunidad segura.
- Active el registro y envíe los registros a un host de registro dedicado seguro.
- Configure el registro para incluir información de tiempo precisa mediante NTP y registros de hora.
- Revise registros para detectar posibles incidentes y archivarlos de acuerdo con la política de seguridad.
- Si el controlador del sistema utiliza una interfaz de explorador, asegúrese de cerrar sesión después de utilizarla.

Seguridad 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 información confidencial en discos duros.
- Para deshacerse de una unidad de disco duro vieja, destruya físicamente la unidad o borre por completo todos los datos almacenados en la unidad. La supresión de todos los archivos o el cambio de formato de la unidad eliminará únicamente las tablas de direcciones en la unidad; la información puede recuperarse de una unidad tras borrar archivos o cambiar el formato de la unidad. (Utilice software de borrado del disco duro para borrar por completo todos los datos en una unidad).

Seguridad de red

Siga estas directrices para optimizar la seguridad de red:

- La mayoría de los conmutadores permiten definir las redes de área local virtual (VLAN). Si utiliza su conmutador para definir redes 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 estos clientes y servidores.

- Gestione conmutadores 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.
- 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.
- Mantenga 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.
- Utilice una configuración de VLAN estática, cuando sea posible.
- Desactive puertos de conmutador sin usar y asígneles un número de VLAN sin usar.
- Asigne un único número VLAN nativo a los puertos de tronco.
- Limite las redes VLAN que se puedan transportar sobre un tronco a sólo 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.
- Desactive los servicios de red innecesarios, como servidores pequeños TCP o HTTP. Active servicios de red necesarios y configure estos servicios de manera segura.
- Diferentes conmutadores ofrecerán diferentes niveles de funciones de seguridad para puertos. Utilice estas funciones de seguridad para puertos si están disponibles en el conmutador:
 - MAC Locking (bloqueo MAC): consiste en relacionar una dirección MAC (Media Access Control) de uno o más dispositivos conectados con 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.
 - MAC Lockout (cierre MAC): desactiva la conexión de una dirección MAC especificada a un conmutador.
 - MAC Learning (aprendizaje MAC): utiliza la información sobre las conexiones directas de cada puerto del conmutador, por lo que el conmutador puede definir la seguridad basándose en las conexiones actuales.