Servidores SPARC M5-32 y SPARC M6-32

Guía de seguridad

Referencia: E49762-02
Julio de 2014

Tabla de contenidos

• • • Capítulo 1

Descripción de la seguridad del hardware

El aislamiento físico y el control de acceso son la base para crear la arquitectura de seguridad. Garantizar que el servidor físico esté instalado en un entorno seguro permite protegerlo contra el acceso no autorizado. Asimismo, el registro de todos los números de serie ayuda a prevenir el riesgo de robo, reventa o cadena de suministro (es decir, la inserción de componentes falsificados o peligrosos en la cadena de suministro de la organización).

En este capítulo, se proporcionan directrices generales para la seguridad del hardware de los servidores SPARC M5-32 y SPARC M6-32.

En este capítulo, se incluyen las siguientes secciones:

Restricciones de acceso

- Instale servidores y equipos relacionados en una habitación cerrada con llave y de acceso restringido.
- Si el equipo se instala en un bastidor que tiene una puerta con llave, cierre siempre la puerta hasta que se tenga que reparar algún componente dentro del bastidor. Cerrar las puertas también restringe el acceso de dispositivos de conexión o sustitución en marcha.
- Almacene unidades sustituibles en campo (FRU) o unidades sustituibles por el cliente (CRU) de repuesto en un armario cerrado. Restrinja el acceso al armario cerrado al personal autorizado.
- Verifique periódicamente el estado y la integridad de las cerraduras del bastidor y el armario de repuestos para brindar protección contra la manipulación de cerraduras o puertas abiertas, o bien, para detectar si esto ha sucedido.
- Almacene las llaves del armario en una ubicación segura con acceso limitado.
- Restrinja el acceso a consolas USB. Los dispositivos como los controladores del sistema, las unidades de distribución de energía (PDU) y los conmutadores de red pueden tener conexiones USB. El acceso físico es un método más seguro para acceder a un componente, ya que esto elimina la posibilidad de ataques basados en red.
- Conecte la consola a un KVM externo para hacer posible el acceso remoto a la consola. Generalmente, los dispositivos KVM son compatibles con la autenticación de doble factor, el control de acceso centralizado y la auditoría. Para obtener más información sobre las directrices

de seguridad y las mejores prácticas para los KVM, consulte la documentación incluida con el dispositivo KVM.

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 de hardware del equipo, como las piezas de repuesto. Utilice plumas ultravioleta o etiquetas en relieve especiales.
- 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.

Los lectores RFID inalámbricos pueden simplificar aún más el seguimiento de los activos. Para obtener más información, lea *Cómo realizar un seguimiento de sus activos del sistema Oracle Sun mediante RFID* , disponible en:

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

Unidades de disco duro

Por lo general, las unidades de disco duro se usan para almacenar información confidencial. Para proteger esta información de la divulgación no autorizada, las unidades de disco duro deberían sanearse antes de ser reutilizadas, retiradas o desechadas.

- Utilice herramientas de borrado de disco duro, como el comando **format** (1M) de Oracle Solaris, para borrar por completo todos los datos del disco duro. De manera alternativa, puede utilizar, si corresponde y están disponibles, herramientas de desmagnetización física.
- En algunos casos, la información almacenada en los discos duros posee tal nivel de confidencialidad que el único método de saneamiento apropiado es la destrucción física del disco duro por medio de la pulverización o la incineración.

Se recomienda a las organizaciones que consulten sus respectivas políticas de protección de datos para determinar el método más apropiado para sanear los discos duros.

Atención

Debido a la manera en que se gestiona el acceso a los datos, quizá no sea posible suprimir algunos de los datos en discos duros modernos (especialmente los SSD) con software de borrado de disco duro.

• • • Capítulo 2

Descripción de la seguridad del software

La mayoría de las medidas de seguridad del hardware se implementan por medio de medidas de software. En este capítulo, se proporcionan directrices generales para la seguridad del software de los servidores SPARC M5-32 y SPARC M6-32.

En este capítulo, se incluyen las siguientes secciones:

▼ Prevención del acceso no autorizado (sistema operativo Oracle Solaris)

- Utilice los comandos del sistema operativo Oracle Solaris para restringir el acceso al software de Oracle Solaris, fortalecer el sistema operativo, utilizar funciones de seguridad y proteger las aplicaciones.
  Obtenga el documento con las directrices de seguridad de Oracle Solaris correspondiente a la versión del sistema operativo que está utilizando en:
  http://www.oracle.com/goto/Solaris11/docs
  http://www.oracle.com/goto/Solaris10/docs

▼ Prevención del acceso no autorizado (Oracle ILOM)

1. Utilice los comandos de Oracle ILOM para restringir el acceso de los usuarios al software de Oracle ILOM, cambiar la contraseña predeterminada de fábrica, limitar el uso de la cuenta de superusuario root y proteger la red privada al procesador de servicio.
   Obtenga la *Guía de seguridad de Oracle ILOM* en:
   http://www.oracle.com/goto/ILOM/docs
2. Utilice los comandos de Oracle ILOM específicos de la plataforma para proteger dominios individuales mediante la creación de cuentas de usuario con roles que se aplican a un dominio físico específico.

Al asignar roles de usuario a un dominio físico, las capacidades otorgadas a ese dominio son un reflejo de los roles de usuario asignados para la plataforma, pero se limitan a los comandos ejecutados en el componente dado.

Nota

Solo los roles de usuario de administrador (**a**), de consola (**c**) y de restablecimiento (**r**) pueden asignarse a dominios físicos individuales.

Obtenga la *Guía de administración de los servidores SPARC M5-32 y SPARC M6-32* en: http://www.oracle.com/goto/M6-32/docs

▼ Prevención del acceso no autorizado (Oracle VM Server for SPARC)

- Utilice comandos de Oracle VM for SPARC para restringir el acceso al software de Oracle VM for SPARC.
  Obtenga la *Guía de seguridad de Oracle VM for SPARC* en: http://www.oracle.com/goto/VM-SPARC/docs

Restricción del acceso (OpenBoot)

En estos temas se explica cómo restringir el acceso desde el indicador de OpenBoot.

- Implementación de la protección con contraseña (OpenBoot) [8]
- Comprobación de inicios de sesión fallidos (OpenBoot) [8]
- Suministro de un banner de encendido (OpenBoot) [9]

Información relacionada

- 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

▼ Implementación de la protección con contraseña (OpenBoot)

- Establezca el parámetro del modo seguridad en **full** o **command**.
  Cuando se establece en **full**, se requiere una contraseña para realizar cualquier acción, incluidas las operaciones normales, como el inicio. Cuando se establece en **command**, no se requiere ninguna contraseña para los comandos **boot** o **go**, pero el resto de los comandos requiere contraseña. Por razones de continuidad del negocio, establezca el parámetro de modo seguridad en command, como en el siguiente ejemplo:

```
ok password
ok setenv security-mode command
ok password
```

▼ Comprobación de inicios de sesión fallidos (OpenBoot)

1. Determine si alguien ha intentando y no ha podido acceder al entorno OpenBoot mediante el parámetro **security-#badlogins**, como en el siguiente ejemplo.

```
ok printenv security-#badlogins
```

Si este comando devuelve un valor mayor que cero, se registró un intento de acceso fallido al entorno OpenBoot.

2. Restablezca el parámetro **security-#badlogins** escribiendo el siguiente comando.

```
ok setenv security-#badlogins 0
```

▼ Suministro de un banner de encendido (OpenBoot)

- Utilice los siguientes comandos para activar un mensaje de advertencia personalizado.

```
ok setenv oem-banner banner-message
ok setenv oem-banner? true
```

Firmware del sistema Oracle

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

Para obtener información sobre cómo obtener las últimas actualizaciones o parches, consulte las notas del producto del servidor.

Inicio WAN seguro

El inicio WAN admite diversos niveles de seguridad. Puede usar una combinación de funciones de seguridad compatibles con el inicio WAN para satisfacer las necesidades de la red. Una configuración más segura requiere más administración, pero también ofrece más protección para los datos del sistema.

- Para el sistema operativo Oracle Solaris 10, consulte "Configuración de la instalación del inicio WAN seguro" en la *Guía de instalación de Oracle Solaris: instalaciones basadas en red*.

  http://www.oracle.com/goto/Solaris10/docs
- Para el sistema operativo Oracle Solaris 11, consulte *Protección de la red en Oracle Solaris 11.1*.

  http://www.oracle.com/goto/Solaris11/docs