Guía de seguridad de los servidores SPARC M8 y SPARC M7

Referencia: E55218-02
Septiembre de 2017

Referencia: E55218-02

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

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 proteger el servidor contra el acceso no autorizado. De manera similar, el registro de todos los números de serie ayuda a evitar el uso no autorizado de los componentes de hardware.

En estas secciones, se proporcionan directrices generales de seguridad de hardware para los servidores.

Restricciones de acceso

- Instale servidores y equipos similares en una habitación cerrada con llave y de acceso restringido.
- Si el equipo se instala en un rack con una puerta con llave, cierre siempre la puerta hasta que se tenga que reparar algún componente de dentro del rack. Cerrar las puertas también restringe el acceso de dispositivos de conexión o intercambio en caliente.
- Almacene las piezas de repuesto en un armario cerrado. Restrinja el acceso al armario cerrado a personal autorizado.
- Verifique periódicamente el estado y la integridad de las cerraduras del rack y el armario de repuestos para brindar protección contra la manipulación de cerraduras o puertas abiertas accidentalmente, 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 alimentación (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

Evite el uso de componentes de hardware no autorizados realizando un registro exhaustivo de todos los números de serie a medida que los componentes se reciben y se incorporan al inventario. Antes de instalar o usar cualquier componente, asegúrese de confirmar su autenticidad comparando el número de serie con el que se registró cuando se recibió el componente. Siga estas prácticas para proteger el hardware:

- 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 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 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.

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`

Unidades de disco duro

Con frecuencia, las unidades de disco duro y de estado sólido se usan para almacenar información confidencial. Para proteger esta información contra la divulgación no autorizada, sanee los discos duros antes de reutilizarlos, retirarlos o desecharlos.

- Use herramientas de borrado de disco duro, como el comando `format` (1M) de Oracle Solaris, para borrar por completo todos los datos del disco duro.
- Las organizaciones deberán consultar sus respectivas políticas de protección de datos para determinar el método más apropiado para sanear los discos duros.
- Si es necesario, aproveche el servicio de retención de dispositivos y datos de clientes de Oracle.

http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf

Descripción de la seguridad del software

La mayoría de las medidas de seguridad del hardware se implementan por medio de medidas de software. En estas secciones, se proporcionan directrices generales de seguridad de software para los servidores.

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

- **Use los comandos del sistema operativo Oracle Solaris para restringir el acceso al software de Oracle Solaris, fortalecer el sistema operativo, usar funciones de seguridad y proteger las aplicaciones.**

  Obtenga el documento *Directrices de seguridad de Oracle Solaris* para la versión que está usando en:

  - `http://www.oracle.com/goto/solaris11/docs`
  - `http://www.oracle.com/goto/solaris10/docs`

▼ Prevención del acceso no autorizado (Oracle ILOM)

1. **Use 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 del procesador de servicio.**

   Obtenga la *Guía de seguridad de Oracle ILOM* en:

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

2. **Siempre que sea posible, use 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) se pueden asignar a dominios físicos individuales.

   Obtenga la *Guía de administración de los servidores SPARC M8 y SPARC M7* en:

   http://docs.oracle.com/cd/E55211_01/

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

- **Use 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 de acceso (OBP)

En estos temas, se describe cómo restringir el acceso al indicador de OBP.

Para obtener información sobre la configuración de las variables de seguridad de OpenBoot, consulte la documentación de OpenBoot en:

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

▼ Implementación de la protección con contraseña

- **Si aún no ha configurado una contraseña, realice este paso.**

```
{0} ok password
New password (8 characters max):
Retype new password: password
```

La contraseña puede tener hasta ocho caracteres. Si introduce más de ocho caracteres, se usarán solamente los primeros ocho caracteres. Se aceptan todos los caracteres imprimibles. No se aceptan caracteres de control.

Nota - La configuración de la contraseña en cero desactiva la seguridad y trata el parámetro `security-mode` como si estuviera configurado en `none`. Sin embargo, no cambia la configuración.

▼ Activación del modo de seguridad

1. **Configure el parámetro `security-mode` en `full` o `command`.**

   Cuando está configurado en `full`, se requiere una contraseña para realizar cualquier acción, como `boot`. Cuando se configura 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, configure el parámetro `security-mode` en `command`, como en el siguiente ejemplo.

```
{0} ok setenv security-mode command
{0} ok
```

2. **Obtenga el indicador de modo de seguridad.**

   Después de configurar el modo de seguridad como se describe arriba, puede obtener el indicador de modo de seguridad en una de dos maneras.

   - **Use los comandos `logout` y `login`.**

```
{0} ok logout
Type boot , go (continue), or login (command mode)
>
> login
Firmware Password: password
Type help for more information
{0} ok
```

     Para salir del modo de seguridad, use los nombres `logout` y `login`.

   - **Use el comando `reset-all`.**

```
{0} ok reset-all
```

Este comando restablece el sistema. Cuando el sistema regresa, OpenBoot se dirige al indicador de modo de seguridad. Para volver a iniciar sesión en el indicador del comando (o para salir del modo de seguridad), use los nombres `logout` y `login` y, a continuación, introduzca la contraseña, como se describe arriba.

Desactivación del modo de seguridad

1. **Configure el parámetro `security-mode` en `none`.**

   ```
   {0} ok setenv security-mode none
   ```

2. **Configure la contraseña en longitud cero; para ello, presione Intro después de los dos indicadores de contraseña.**

Comprobación de inicios de sesión con fallo (OBP)

1. **Determine si alguien ha intentado 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 Ø, se registró un intento de acceso fallido al entorno OpenBoot.

2. **Para restablecer el parámetro, escriba:**

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

Suministro de un banner de encendido

Aunque no es un control preventivo o exploratorio directo, se puede usar un banner por estos motivos:

- Para indicar propiedad.
- Para advertir a los usuarios acerca del uso aceptable del servidor.
- Para indicar que el acceso o las modificaciones a los parámetros de OpenBoot están restringidos al personal autorizado.

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

```
{0} ok setenv oem-banner banner-message
{0} ok setenv oem-banner? true
```

El mensaje del banner puede tener hasta 68 caracteres. Se aceptan todos los caracteres imprimibles.

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 actualizaciones o los parches más recientes, consulte las notas del producto en la siguiente dirección:

http://docs.oracle.com/cd/E55211_01/

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 cumplir con las necesidades de la red. Una configuración más segura requiere más administración, pero también protege los datos del sistema en mayor medida.

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

  Consulte http://www.oracle.com/goto/solaris10/docs.
- Para el sistema operativo Oracle Solaris 11, consulte *Protección de la red en Oracle Solaris*.

  Consulte http://www.oracle.com/goto/solaris11/docs.