Guía de seguridad de los servidores de las series SPARC y Netra SPARC S7-2

Referencia: E77184-01
Junio de 2016

Referencia: E77184-01

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. Asegurarse 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 estas secciones, se proporcionan directrices de seguridad de hardware generales para los servidores de las series SPARC y Netra SPARC S7-2.

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 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 en caliente o de intercambio en caliente.
- 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.
- 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 del hardware del equipo, como las piezas de repuesto. Utilice plumas ultravioletas 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 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

Por lo general, las unidades de disco duro 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.

- Utilice herramientas de borrado de disco, como el comando `format` (1M) de Oracle Solaris, para borrar por completo todos los datos del disco duro.
- 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.
- 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 de seguridad de software generales para los servidores de las series SPARC y Netra SPARC S7-2.

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)

- **Utilice los comandos de Oracle ILOM para restringir el acceso 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

▼ 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 describe cómo restringir el acceso desde el símbolo del sistema de OpenBoot.

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 todavía no estableció una contraseña, realice este paso.**

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

La contraseña puede tener entre uno y ocho caracteres. Si escribió más de ocho caracteres, solo se usarán los primeros ocho caracteres. Se aceptan todos los caracteres imprimibles. No se aceptan los caracteres de control.

Nota - Al establecer la contraseña en cero caracteres, se desactiva la seguridad y se considera el parámetro `security-mode` como si estuviese establecido en `none`. Sin embargo, esto no cambia la configuración.

▼ Activación del modo de seguridad

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

Cuando se establece en `full`, se requiere una contraseña para realizar cualquier acción, incluidas las operaciones normales, como `boot`. 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 `security-mode` en `command`, como en el siguiente ejemplo:

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

2. Obtenga el símbolo del sistema del modo de seguridad.

Después de configurar el modo de seguridad como se describe anteriormente, puede obtener el símbolo del sistema del modo de seguridad de dos formas.

- **Use las palabras `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`, como se muestra en el ejemplo.

- **Use la palabra `reset-all`.**

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

  Esta palabra restablece el sistema. Una vez que se restablece, OpenBoot va al símbolo del sistema del modo de seguridad. Para volver a iniciar sesión en el símbolo del sistema (o salir del modo de seguridad), use los nombres `logout` y `login`, y luego introduzca la contraseña como se describe anteriormente.

Desactivación del modo de seguridad

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

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

2. **Establezca la contraseña con una longitud de cero caracteres escribiendo Return después de ambos símbolos del sistema de la contraseña.**

Comprobación de inicios de sesión con error

1. **Determine si alguien intentó acceder al entorno de OpenBoot, pero no pudo, mediante el parámetro `security-#badlogins`, como en el siguiente ejemplo.**

```
{0} ok printenv security-#badlogins
```

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

2. **Restablezca el parámetro escribiendo el siguiente comando.**

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

Suministro de un banner de encendido

Si bien no se trata de un control exploratorio ni preventivo directo, un banner se puede usar para los siguientes motivos:

- transmitir propiedad;
- advertir a los usuarios sobre el uso aceptable del servidor;
- indicar que el acceso o las modificaciones a los parámetros de OpenBoot está restringido a personal autorizado.

- **Utilice 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 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 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*.
- Para el sistema operativo Oracle Solaris 11, consulte *Protección de la red en Oracle Solaris 11.3*.

Inicio verificado

El inicio verificado se puede utilizar para verificar los bloques de inicio del sistema y los módulos del núcleo de Oracle Solaris antes de cargarlos en el sistema. Utilice Oracle ILOM para activar el inicio verificado y para especificar de qué manera debe responder el sistema cuando se produce un error en el control de verificación. La activación del inicio verificado puede evitar que ocurran cambios perjudiciales en los bloques de inicio del sistema o los módulos del núcleo de Oracle Solaris.

Consulte la información sobre la configuración de las propiedades de inicio verificado de SPARC en la *Guía del administrador para configuración y mantenimiento de Oracle ILOM*.