Guía de seguridad de Oracle® VM Server for SPARC 2.2

Referencia: E29612
Mayo de 2012

ORACLE

120709@25097

Contenido

Prefacio

La *Guía de seguridad de Oracle VM Server for SPARC 2.2* incluye información sobre cómo instalar, configurar y utilizar el software Oracle VM Server for SPARC 2.2 de manera segura.

Documentación relacionada

En la tabla siguiente se muestra la documentación disponible para la versión Oracle VM Server for SPARC 2.2 y relacionada con ella.

TABLA P–1 Documentación relacionada

Aplicación	Título
Software Oracle VM Server for SPARC 2.2	*Guía de administración de Oracle VM Server for SPARC 2.2* *Guía de seguridad de Oracle VM Server for SPARC 2.2* *Oracle VM Server for SPARC 2.2 Reference Manual* *Notas de la versión de Oracle VM Server for SPARC 2.2*
Páginas del comando man `drd`(1M) y `vntsd`(1M) de Oracle VM Server for SPARC 2.2	Manuales de referencia del SO de Oracle Solaris : ■ Oracle Solaris 10 Documentation ■ Oracle Solaris 11 Documentation
SO de Oracle Solaris : instalación y configuración	Guías de instalación y configuración del SO de Oracle Solaris : ■ Oracle Solaris 10 Documentation ■ Oracle Solaris 11 Documentation
Seguridad del SO de Oracle Solaris y Oracle VM Server for SPARC	Notas del producto de Oracle VM Server for SPARC y guías de seguridad del SO de Oracle Solaris : ■ *Secure Deployment of Oracle VM Server for SPARC* (`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/secure-ovm-sparc-deployment-294062.pdf`) ■ *Instrucciones de seguridad de Oracle Solaris 10* ■ *Directrices de seguridad de Oracle Solaris 11*

Encontrará documentación relativa al servidor, el software o SO de Oracle Solaris en `http://www.oracle.com/technetwork/indexes/documentation/index.html`. Utilice el cuadro de búsqueda para encontrar los documentos y la información que necesite.

Puede acceder al foro de debate de Oracle VM Server for SPARC en `http://forums.oracle.com/forums/forum.jspa?forumID=1047`.

Acceso al servicio de asistencia de Oracle

Los clientes de Oracle disponen de asistencia a través de Internet en el portal My Oracle Support. Si tiene alguna discapacidad auditiva, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` o `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` para obtener más información.

Convenciones tipográficas

La siguiente tabla describe las convenciones tipográficas que se usan en este libro.

TABLA P–2 Convenciones tipográficas

Tipo de letra	Significado	Ejemplo
`AaBbCc123`	Los nombres de los comandos, archivos y directorios y de la salida de ordenador en pantalla	Edite el archivo `.login`. Use `ls -a` para enumerar todos los archivos. `machine_name% tiene un mensaje.`
`AaBbCc123`	Cuando escribe, la salida en pantalla se resalta	`machine_name%` **`su`** `Contraseña:`
aabbcc123	Marcador de posición: sustituir con un nombre o un valor real	El comando para eliminar un archivo es `rm` *filename*.
AaBbCc123	Títulos de libros, nuevos términos y términos que se resaltar	Lea el capítulo 6 en la *Guía del usuario*. Un *caché* es una copia guardada localmente. *No* guarde el archivo. **Nota:** Algunos elementos con énfasis aparecen en negrita en línea.

Mensajes del shell en ejemplos de comandos

La siguiente tabla muestra los indicadores de sistema predeterminados UNIX y los indicadores de superusuario para los shells incluidos en el SO Solaris de Oracle. Tenga en cuenta que el mensaje de sistema predeterminado que se muestra en el comando varía, dependiendo de la versión de Solaris de Oracle.

TABLA P–3 Indicadores del shell

Shell	Indicador
Shell Bash, shell Korn y shell Bourne	`$`
Shell Bash, shell Korn y shell Bourne para superusuario	`#`
Shell C	`machine_name%`
Shell C para superusuario	`machine_name#`

◆ ◆ ◆ CAPÍTULO 1

Descripción general de la seguridad de Oracle VM Server for SPARC

En este capítulo, se describen las siguientes funciones de seguridad que utiliza el software de Oracle VM Server for SPARC:

Funciones de seguridad que utiliza Oracle VM Server for SPARC

El software de Oracle VM Server for SPARC es un producto de virtualización que permite ejecutar en un único sistema más de una máquina virtual (VM) de Oracle Solaris , cada una de ellas con su propio sistema operativo Oracle Solaris 10 o Oracle Solaris 11 instalado. Cada máquina virtual también se denomina *dominio lógico*. Los dominios son instancias independientes y pueden ejecutar diferentes versiones de SO de Oracle Solaris , además de varias aplicaciones de software. Por ejemplo, los dominios pueden tener diferentes revisiones de paquetes instaladas, diversos servicios activados y cuentas del sistema con contraseñas distintas. Consulte las *Instrucciones de seguridad de Oracle Solaris 10* y las *Directrices de seguridad de Oracle Solaris 11* para obtener información sobre la seguridad de Oracle Solaris .

El comando `ldm` debe ejecutarse en el dominio de control para configurar el dominio lógico y recuperar la información de estado. La limitación del acceso al dominio de control y al comando `ldm` resulta fundamental para la seguridad de los dominios que se ejecutan en el sistema. Para limitar el acceso a los datos de configuración de dominio, utilice las funciones de seguridad de Oracle VM Server for SPARC, como el control de acceso basado en roles (RBAC) y la función de Oracle Solaris para autorizaciones de `solaris.ldoms`. Consulte "Contenidos de perfil de Logical Domains Manager" de *Guía de administración de Oracle VM Server for SPARC 2.2*.

El software de Oracle VM Server for SPARC utiliza las siguientes funciones de seguridad:

- Las funciones de seguridad que están disponibles en los sistemas operativos Oracle Solaris 10 y Oracle Solaris 11 también están disponibles en los dominios que ejecutan el software de Oracle VM Server for SPARC. Consulte las *Instrucciones de seguridad de Oracle Solaris 10* y las *Directrices de seguridad de Oracle Solaris 11*.
- Las funciones de seguridad de SO de Oracle Solaris se pueden aplicar al software de Oracle VM Server for SPARC. Para obtener información completa sobre el modo de garantizar la seguridad de Oracle VM Server for SPARC, consulte *Implementación segura de Oracle VM Server for SPARC*.
- Los sistemas operativos Oracle Solaris 10 y Oracle Solaris 11 incluyen correcciones de seguridad que están disponibles para el sistema. Obtenga las correcciones para el SO Oracle Solaris 10 en forma de parches o actualizaciones de seguridad. Obtenga las correcciones para el SO Oracle Solaris 11 en forma de Actualizaciones de repositorio de asistencia (SRU, Support Repository Update).
- Para limitar el acceso a los comandos de administración de Oracle VM Server for SPARC y las consolas de dominio, y para activar la función de auditoría de Oracle VM Server for SPARC, consulte el Capítulo 3, "Seguridad de Oracle VM Server for SPARC" de *Guía de administración de Oracle VM Server for SPARC 2.2*.

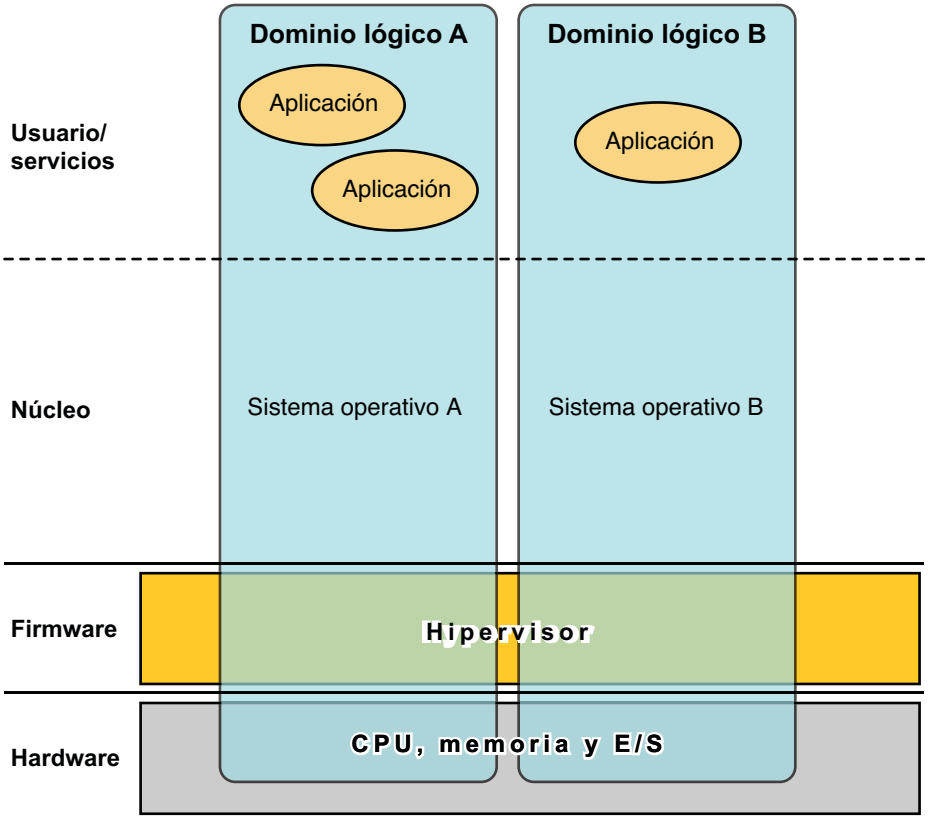
Descripción general del producto Oracle VM Server for SPARC

Oracle VM Server for SPARC ofrece funciones de virtualización empresariales de gran eficacia para los servidores SPARC T-Series de Oracle. El software Oracle VM Server for SPARC permite crear hasta 128 servidores virtuales, denominados dominios lógicos, en un solo sistema. Este tipo de configuración permite aprovechar la escala de subprocesos masiva que ofrecen los servidores SPARC T-Series y el SO de Oracle Solaris .

Un *dominio lógico* es una máquina virtual que contiene una agrupación de recursos lógica y discreta. Un dominio lógico tiene su propio sistema operativo e identidad en un sistema individual de equipo. Cada dominio lógico puede crearse, destruirse, reconfigurarse y reiniciarse de manera independiente, sin necesidad de que lleve a cabo un ciclo de energía del servidor. Puede ejecutar una gran variedad de aplicaciones de software en diferentes dominios lógicos y mantenerlos independientes por razones de seguridad y rendimiento.

Para obtener información sobre el uso del software de Oracle VM Server for SPARC, consulte la *Guía de administración de Oracle VM Server for SPARC 2.2* y el *Oracle VM Server for SPARC 2.2 Reference Manual* . Para obtener información acerca del hardware y software necesarios, consulte las *Notas de la versión de Oracle VM Server for SPARC 2.2*.

FIGURA 1–1 Hipervisor que admite dos dominios lógicos



El software de Oracle VM Server for SPARC utiliza los siguientes componentes para proporcionar la virtualización del sistema:

- **Hipervisor.** El hipervisor es una capa de firmware pequeña que proporciona una arquitectura de máquina virtualizada estable en la que se puede instalar un sistema operativo. Los servidores Sun de Oracle que usan el hipervisor ofrecen funciones de hardware para admitir el control del hipervisor sobre las actividades del sistema operativo en un dominio lógico.

  La cantidad de dominios y las capacidades de cada dominio que admite un hipervisor SPARC específico son características que dependen del servidor. El hipervisor puede asignar subconjuntos de la CPU, la memoria y los recursos de E/S del servidor a un determinado dominio lógico. Esto hace que se admitan varios sistemas operativos simultáneamente, cada uno dentro de su propio dominio lógico. Se puede volver a organizar los recursos entre dominios lógicos independientes con una granularidad arbitraria. Por ejemplo, se pueden asignar CPU a un dominio lógico con la granularidad de un subproceso de CPU.

El procesador de servicios (SP, Service Processor), también conocido como *controlador del sistema* (SC, System Controller), supervisa y ejecuta la máquina física, pero no gestiona los dominios lógicos. El Logical Domains Manager gestiona los dominios lógicos.

- **Dominio de control.** El Logical Domains Manager se ejecuta en este dominio para que pueda crear y gestionar otros dominios lógicos, y asignar recursos virtuales a otros dominios. Sólo puede haber un dominio de control por servidor. El dominio de control es el primer dominio que se crea cuando instala el software de Oracle VM Server for SPARC. El dominio de control se denomina `primary`.
- **Dominio de servicios.** El dominio de servicios proporciona servicios de dispositivos virtuales a otros dominios, como un conmutador virtual, un concentrador de consola virtual y un servidor de disco virtual. Cualquier dominio puede configurarse como un dominio de servicio.
- **Dominio de E/S.** El dominio de E/S tiene acceso directo a los dispositivos físicos de E/S, como una tarjeta de red en un controlador PCI Express (PCIe). Un dominio E/S puede poseer un complejo de raíz PCIe, o puede poseer una ranura PCIe o un dispositivo PCIe integrado usando la características de E/S directa (DIO). Consulte "Asignación de dispositivos de punto final PCIe" de *Guía de administración de Oracle VM Server for SPARC 2.2*.

  Un dominio E/S puede compartir dispositivos E/S físicos con otros dominios en forma de dispositivos virtuales cuando el dominios E/S también se usa como dominio de servicios.
- **Dominio raíz.** Un dominio raíz tiene asignada una raíz de PCIe compleja. Este dominio posee la estructura PCIe y ofrece todos los servicios relacionados con la estructura, como el manejo de error de estructura. Un dominio raíz también es un dominio E/S, ya que posee y tiene acceso directo a los dispositivos de E/S físicos.

  El número de dominios raíz que puede tener depende de la arquitectura de la plataforma. Por ejemplo, si usa un servidor Sun SPARC Enterprise T5440, de Oracle, puede tener hasta cuatro dominios raíz.
- **Dominio invitado.** Un dominio invitado es un dominio sin E/S que consume servicios de dispositivos virtuales proporcionados por uno o más dominios de servicio. El dominio invitado no tiene ningún dispositivo de E/S físico. Solamente tiene dispositivos de E/S virtuales, como discos virtuales e interfaces de red virtuales.

A menudo, un sistema de Oracle VM Server for SPARC tiene un solo dominio de control que proporciona los servicios que llevan a cabo los dominios de E/S y los dominios de servicio. Para mejorar la redundancia y la facilidad de mantenimiento de la plataforma, puede configurar más de un dominio de E/S en el sistema Oracle VM Server for SPARC.

Aplicación de los principios de seguridad general a Oracle VM Server for SPARC

Puede configurar dominios invitados de varias formas para proporcionar distintos niveles de aislamiento del dominio de invitado, uso compartido de hardware y conectividad de dominios. Estos factores contribuyen al nivel de seguridad de la configuración general de Oracle VM Server for SPARC, a la que puede aplicar algunos de los siguientes principios generales de seguridad:

- **Minimizar la superficie de ataque.**
  - Minimice los errores de configuración no intencionales mediante la creación de directrices operativas que le permitan revisar con regularidad la seguridad del sistema. Consulte la "Contramedida n.º 1: Directrices operativas" en *Implementación segura de Oracle VM Server for SPARC*.
  - Planifique cuidadosamente la arquitectura del entorno virtual para maximizar el aislamiento de los dominios. Consulte las contramedidas que se describen para la "Amenaza n.º 2: Errores en la arquitectura del entorno virtual" en *Implementación segura de Oracle VM Server for SPARC*.
  - Planifique cuidadosamente los recursos que desea asignar y determine si se van a compartir. Consulte la "Contramedida n.º 7: Asignación cuidadosa de los recursos de hardware" y la "Contramedida n.º 8: Asignación cuidadosa de los recursos compartidos" en *Implementación segura de Oracle VM Server for SPARC*.
  - Asegúrese de que los dominios lógicos estén protegidos contra la manipulación. Para ello, aplique las contramedidas que se describen para la "Amenaza n.º 4: Manipulación del entorno de ejecución" y la "Contramedida n.º 28: Aseguración del sistema operativo invitado" en *Implementación segura de Oracle VM Server for SPARC*.
  - Exponga un dominio invitado a la red *solamente* cuando sea necesario. Se pueden utilizar conmutadores virtuales para limitar la conectividad de red de un dominio invitado, *solamente* con las redes correspondientes.
  - Siga estos pasos para minimizar la superficie de ataque de Oracle Solaris 10 y Oracle Solaris 11, como se describe en las *Instrucciones de seguridad de Oracle Solaris 10* y las *Directrices de seguridad de Oracle Solaris 11*.
  - Proteja el núcleo central del hipervisor, como se describe en la "Contramedida n.º 15: Validación de formas de software y firmware" y la "Contramedida n.º 16: Validación de los módulos del núcleo" en *Implementación segura de Oracle VM Server for SPARC*.
  - Proteja el dominio de control contra los ataques de denegación de servicio. Consulte la "Contramedida n.º 17: Acceso a la consola" en *Implementación segura de Oracle VM Server for SPARC*.
  - Asegúrese de que los usuarios no autorizados no puedan ejecutar Logical Domains Manager. Consulte la "Amenaza n.º 8: Uso no autorizado de la configuración de utilidades" en *Implementación segura de Oracle VM Server for SPARC*.

- Asegúrese de que los procesos o usuarios no autorizados no puedan acceder al dominio de servicio. Consulte la "Amenaza n.º 9: Manipulación de un dominio de servicio" en *Implementación segura de Oracle VM Server for SPARC*.
- Proteja un dominio de E/S o un dominio de servicio contra los ataques de denegación de servicio. Consulte la "Amenaza n.º 10: Denegación de servicio de dominio de E/S o de dominio de servicio" en *Implementación segura de Oracle VM Server for SPARC*.
- Asegúrese de que los procesos o usuarios no autorizados no puedan acceder al dominio de E/S. Consulte la "Amenaza n.º 11: Manipulación de un dominio de E/S" en *Implementación segura de Oracle VM Server for SPARC*.
- Desactive los servicios de gestor de dominios innecesarios. El Logical Domains Manager proporciona los servicios de red necesarios para el acceso, el control y la migración de dominios. Desactive cualquiera de los siguientes servicios de red cuando no estén en uso:
  - El servicio de migración en puertos TCP `4983` y `8101`

    Para desactivar este servicio, consulte la descripción de las propiedades `ldmd/incoming_migration_enabled` y `ldmd/outgoing_migration_enabled` en la página del comando man `ldmd(1M)`.
  - La admisión del protocolo extensible de mensajería y comunicación de presencia (XMPP, Extensible Messaging and Presence Protocol) en el puerto TCP `6482`

    Para desactivar este servicio, consulte "Transporte de XML" de *Guía de administración de Oracle VM Server for SPARC 2.2*.
  - El protocolo simple de administración de red (SNMP, Simple Network Management Protocol) en el puerto UDP `161`

    Determine si desea utilizar la base de información de gestión de Oracle VM Server for SPARC (MIB, Management Information Base) para observar los dominios. Esta función requiere que el servicio SNMP esté activado. En función de las opciones que elija, siga uno de estos procedimientos:
    - **Active el servicio SNMP para utilizar la MIB de Oracle VM Server for SPARC.** Instale la MIB de Oracle VM Server for SPARC de manera segura. Consulte "Cómo instalar el paquete de software de MIB de Oracle VM Server for SPARC" de *Guía de administración de Oracle VM Server for SPARC 2.2* y "Gestión de la seguridad" de *Guía de administración de Oracle VM Server for SPARC 2.2*.
    - **Desactive el servicio SNMP.** Para desactivar este servicio, consulte "Cómo eliminar el paquete de software de MIB de Oracle VM Server for SPARC" de *Guía de administración de Oracle VM Server for SPARC 2.2*.
  - Servicio de detección en dirección de multidifusión `239.129.9.27` y puerto `64535`

    No puede desactivar este servicio mientras se ejecuta `ldmd`, el daemon de Logical Domains Manager. En su lugar, utilice la función de filtro IP de Oracle Solaris para bloquear el acceso a este servicio, que reduce al mínimo la superficie de ataque de Logical Domains Manager. El bloqueo del acceso impide el uso no autorizado de la utilidad, lo cual protege con eficacia contra los ataques de denegación de servicio y

cualquier otro intento de uso indebido de los servicios de red. Consulte el Capítulo 20, "Filtro IP en Oracle Solaris (descripción general)" de *Administración de Oracle Solaris: servicios IP* y "Uso de conjuntos de reglas de filtro IP" de *Administración de Oracle Solaris: servicios IP*.

Consulte también la "Contramedida n.° 14: Aseguración de ILOM" y la "Contramedida n.° 20: Protección de LDoms Manager" en *Implementación segura de Oracle VM Server for SPARC*.

- **Proporcionar el privilegio mínimo para llevar a cabo una operación.**
  - Aísle los sistemas en las *clases de seguridad*, que son conjuntos de sistemas invitados individuales que comparten los mismos privilegios y requisitos de seguridad. Al asignar solamente dominios invitados desde una única clase de seguridad a una única plataforma de hardware, crea una brecha de aislamiento, lo que evita que los dominios crucen a una clase de seguridad diferente. Consulte la "Contramedida n.º 2: Asignación cuidadosa de invitados a plataformas de hardware" en *Implementación segura deOracle VM Server for SPARC*.
  - Utilice RBAC para restringir la capacidad de gestionar dominios con el comando `ldm`. *Sólo* debe otorgarse esta capacidad a los usuarios que tienen que gestionar dominios. Asigne un rol que utilice el perfil de derechos de gestión de dominios lógicos a los usuarios que necesitan acceso a todos los subcomandos `ldm`. Asigne un rol que utilice el perfil de derechos de revisión de dominios lógicos sólo a los usuarios que necesitan acceder a los subcomandos relacionados con la lista de `ldm`. Consulte "Uso de perfiles de derechos y roles" de *Guía de administración de Oracle VM Server for SPARC 2.2*.
  - Use RBAC para restringir el acceso a la consola *sólo* de los dominios a los que usted, como administrador de Oracle VM Server for SPARC, debe acceder. *No* permita el acceso general a todos los dominios. Consulte "Uso de perfiles de derechos y roles" de *Guía de administración de Oracle VM Server for SPARC 2.2*.
- **Controle la actividad del sistema.**

  Active la auditoría de Oracle VM Server for SPARC. Consulte "Activación y utilización de auditoría" de *Guía de administración de Oracle VM Server for SPARC 2.2*.

Para obtener recomendaciones acerca de la implementación del software de Oracle VM Server for SPARC de una manera segura, consulte "Opciones de implementación recomendadas" en *Implementación segura de Oracle VM Server for SPARC*.

◆ ◆ ◆ CAPÍTULO 2

Instalación y configuración segura de Oracle VM Server for SPARC

En este capítulo se describen las consideraciones de seguridad relacionadas con la instalación y la configuración de Oracle VM Server for SPARC.

Instalación

El software Oracle VM Server for SPARC se instala automáticamente de manera segura como un paquete de Oracle Solaris 10 u Oracle Solaris 11. Tras completar la instalación, debe disponer de privilegios de administrador para poder configurar los dominios con las funciones de control de acceso basado en roles (RBAC), auditoría y autorización. Estas funciones no están activadas de manera predeterminada.

Configuración después de la instalación

Realice las siguientes tareas después de instalar el software Oracle VM Server for SPARC para maximizar el uso seguro:

- Configure el dominio de control con los servicios de E/S virtual requeridos, como los servicios de conmutador virtual, servidor de disco virtual y concentrador de consola virtual. Consulte Capítulo 4, "Configuración de servicios y el dominio de control" de *Guía de administración de Oracle VM Server for SPARC 2.2*.
- Configure dominios invitados. Consulte Capítulo 5, "Configuración de los dominios invitados" de *Guía de administración de Oracle VM Server for SPARC 2.2*.

  Puede usar un conmutador virtual para configurar dominios invitados por medio de una red administrativa y una red de producción. En este caso, se crea un conmutador virtual utilizando la interfaz de la red de producción como el dispositivo de red de conmutador virtual. Consulte la "Contramedida n.º 13: Red de gestión dedicada" en *Secure Deployment of Oracle VM Server for SPARC*.

La seguridad de un dominio invitado se vea amenazada cuando cualquiera de sus discos virtuales se ve amenazado. Por lo tanto, asegúrese de que los discos virtuales (almacenamiento conectado a red, archivos de imagen almacenados de manera local o discos físicos) estén almacenados en una ubicación segura.

El daemon `vntsd` está desactivado de manera predeterminada. Cuando este daemon está activado, cualquier usuario que inicia sesión en el dominio de control tiene permiso para conectarse a la consola de un dominio invitado. Para impedir este tipo de acceso, asegúrese de que el daemon `vntsd` esté desactivado o use el control de acceso basado en roles para limitar el acceso de conectividad de la consola *sólo* a los usuarios autorizados.

- De modo predeterminado, el procesador de servicio (SP) está configurado de manera segura. Para obtener información sobre cómo usar el software Integrated Lights Out Management (ILOM) para gestionar el SP, consulte la documentación correspondiente a su plataforma en `http://www.oracle.com/technetwork/documentation/sparc-tseries-servers-252697.html`.

◆ ◆ ◆ CAPÍTULO 3

Funciones de seguridad de Oracle VM Server for SPARC

En este capítulo, se proporciona una descripción general de las funciones de seguridad que utiliza el software Oracle VM Server for SPARC.

Para obtener información sobre autenticación, control de acceso y auditoría, consulte el Capítulo 3, "Seguridad de Oracle VM Server for SPARC" de *Guía de administración de Oracle VM Server for SPARC 2.2*.

Modelo de seguridad

El software Oracle VM Server for SPARC se basa en el modelo de seguridad y las funciones integradas en el SO de Oracle Solaris . Para obtener información sobre las directrices de seguridad del SO de Oracle Solaris , consulte *Directrices de seguridad de Oracle Solaris 11* y *Instrucciones de seguridad de Oracle Solaris 10*.

Configuración y uso de la autenticación

Como en una instalación completa de Oracle Solaris , cualquier usuario que tenga una cuenta puede iniciar sesión en un dominio lógico, incluido el dominio de control. El software Oracle VM Server for SPARC no se crea ninguna cuenta de usuario. Consulte "Instalación de Logical Domains Manager" de *Guía de administración de Oracle VM Server for SPARC 2.2*. Para obtener información sobre cómo proteger a los usuarios de Oracle Solaris , consulte "Protección de los usuarios" de *Directrices de seguridad de Oracle Solaris 11*.

Para utilizar Logical Domains Manager para realizar actividades de gestión de dominios en el dominio de control, un usuario debe disponer de privilegios especiales para leer y escribir datos de configuración. Consulte "Contenidos de perfil de Logical Domains Manager" de *Guía de administración de Oracle VM Server for SPARC 2.2* y "Uso de perfiles de derechos y roles" de *Guía de administración de Oracle VM Server for SPARC 2.2*.

Configuración y uso del control de acceso basado en roles (RBAC)

Puede gestionar autorizaciones y perfiles de derechos, y asignar roles a cuentas de usuario utilizando la función de control de acceso basado en roles (RBAC) del SO de Oracle Solaris . Para obtener información sobre RBAC, consulte el Capítulo 9, "Uso del control de acceso basado en roles (tareas)" de *Guía de administración del sistema: servicios de seguridad*.

Cuando se instala Logical Domains Manager se agregan las autorizaciones y los perfiles de derechos necesarios a los archivos locales. Consulte "Uso de perfiles de derechos y roles" de *Guía de administración de Oracle VM Server for SPARC 2.2*.

Para configurar usuarios, autorizaciones, perfiles de derechos y roles en un servicio de nombres, consulte *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .

Configuración y uso de la auditoría

Debe administrar y auditar una instancia de Oracle Solaris en un dominio invitado de la misma manera que lo haría con un SO de Oracle Solaris que se ejecuta en un sistema bare-metal. Puede personalizar la función de auditoría del SO de Oracle Solaris para auditar solamente las funciones y los servicios del sistema que son importantes para su entorno. Para Oracle VM Server for SPARC, asegúrese de que se audite la clase del software de virtualización. Puede realizar otras tareas relacionadas con la auditoría. Consulte "Uso del servicio de auditoría" de *Directrices de seguridad de Oracle Solaris 11* y "Auditar eventos importantes además del inicio y el cierre de sesión" de *Directrices de seguridad de Oracle Solaris 11*.

Logical Domains Manager crea eventos de auditoría y los transfiere al subsistema de auditorías de Oracle Solaris para almacenarlos y examinarlos posteriormente. El historial se guarda en un registro de que lo se ha realizado, cuándo ha sido realizado, por quién y a qué ha afectado. Tenga en cuenta que *no puede* ver la información de auditoría de todos los dominios de un sistema desde su dominio de control.

Por lo tanto, puede activar y desactivar la función de auditoría de cada dominio del sistema según la versión del SO de Oracle Solaris que se ejecute en el sistema, como se indica a continuación:

- **Sistema operativo Oracle Solaris 10**: utilice los comandos `bsmconv` y `bsmunconv`. Consulte las páginas de comando man `bsmconv(1M)` y `bsmunconv(1M)`, y la versión de Oracle Solaris 10 de *System Administration Guide: Security Services*.
- **Sistema operativo Oracle Solaris 11**: utilice el comando `audit`. Consulte la página del comando man `audit(1M)` y la versión Oracle Solaris 11 de *Guía de administración del sistema: servicios de seguridad*.

Para obtener más información, consulte "Activación y utilización de auditoría" de *Guía de administración de Oracle VM Server for SPARC 2.2*.

Configuración y uso de otras funciones de seguridad

Oracle VM Server for SPARC asegura el uso de funciones de virtualización específicas. Si se activa, el daemon `vntsd` se establece en la configuración más segura de manera predeterminada. Sólo acepta conexiones desde el dominio de control y *no* por medio de la red. Puede configurar una opción menos segura para permitir conexiones de red, si es necesario.

Al configurar `vntsd` preste atención a la aceptación de conexiones de red. Es mejor permitir sólo conexiones desde el dominio de control o desactivar `vntsd` para ofrecer una seguridad óptima. Consulte "Aplicación de los principios de seguridad general a Oracle VM Server for SPARC" en la página 13.

La función de migración de dominio de Oracle VM Server for SPARC utiliza medidas de seguridad. Logical Domains Manager en el equipo de origen acepta la solicitud de migración de un dominio y establece una conexión de red segura con Logical Domains Manager en ejecución en el equipo de destino. La migración tiene lugar una vez se ha establecido la conexión. Estas conexiones seguras se crean mediante funciones de autenticación y cifrado. Consulte "Seguridad en las operaciones de migración" de *Guía de administración de Oracle VM Server for SPARC 2.2*.

En particular, la operación de migración de dominio utiliza la capa de conexión segura (SSL, Secure Sockets Layer), de manera predeterminada, para cifrar todo el tráfico que se envía y recibe por medio de la red. Puede mejorar el rendimiento de la migración mediante la asignación de unidades criptográficas a los dominios de control de los sistemas compatibles, como los sistemas UltraSPARC T2, UltraSPARC T2 Plus, SPARC T3 y SPARC T4 de Oracle.

Cuando no se necesita la migración de dominio, puede desactivar la función de migración para evitar que el proceso de `ldmd` lleve a cabo la recepción en el puerto de migración.

◆ ◆ ◆ CAPÍTULO 4

Consideraciones de seguridad para desarrolladores

En este capítulo se proporciona información útil para desarrolladores que producen aplicaciones para el software Oracle VM Server for SPARC.

Interfaz XML de Oracle VM Server for SPARC

Puede crear programas externos que interactúan con el software Oracle VM Server for SPARC por medio del mecanismo de comunicación del lenguaje de marcado extensible (XML, Extensible Markup Language), que utiliza el protocolo de mensajería y presencia extensible (XMPP, Extensible Messaging and Presence Protocol).

Los intrusos pueden intentar aprovechar este protocolo de red para acceder a un sistema, por lo que puede considerar la posibilidad de desactivar XMPP. Para obtener información sobre la desactivación de XMPP, consulte "Transporte de XML" de *Guía de administración de Oracle VM Server for SPARC 2.2*. Para obtener información sobre los mecanismos de seguridad que utiliza Logical Domains Manager, consulte "Servidor XMPP" de *Guía de administración de Oracle VM Server for SPARC 2.2*.

◆ ◆ ◆ APÉNDICE A

Lista de comprobación para una implementación segura

En esta lista de comprobación se resumen los pasos que puede seguir para proteger el entorno de Oracle VM Server for SPARC. Los detalles se proporcionan en otros documentos, como los siguientes:

- *Guía de administración de Oracle VM Server for SPARC 2.2*
- *Oracle Solaris 10 Security Guidelines*
- *Oracle Solaris 11 Security Guidelines*
- *Secure Deployment of Oracle VM Server for SPARC*

Lista de comprobación de seguridad de Oracle VM Server for SPARC

- ❒ Lleve a cabo los pasos de protección de Oracle Solaris en los dominios invitados como lo haría en un entorno no virtualizado.
- ❒ Use los perfiles de derechos de gestión de dominios lógicos y de revisión de dominios lógicos para delegar los privilegios adecuados a los usuarios.
- ❒ Use el control de acceso basado en roles (RBAC, role-based access control) para restringir el acceso a la consola *sólo* de los dominios a los que usted, como administrador de Oracle VM Server for SPARC, debe acceder.
- ❒ Active la función de auditoría del SO de Oracle Solaris para Oracle VM Server for SPARC.
- ❒ Desactive los servicios de gestor de dominios innecesarios.
- ❒ Sólo implemente sistemas invitados de la misma clase de seguridad en una plataforma física.
- ❒ Asegúrese de que no haya ninguna conexión de red entre la administración del entorno de ejecución y los dominios invitados.
- ❒ Sólo asigne los recursos necesarios a los sistemas invitados.