Guía de seguridad de Oracle® VM Server for SPARC 3.5

Referencia: E86370
Agosto de 2017

Referencia: E86370

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

Uso de esta documentación

- **Visión general**: proporciona información sobre cómo utilizar el software Oracle VM Server for SPARC 3.5 de manera segura.
- **Destinatarios:** administradores del sistema que administran la seguridad en servidores SPARC virtualizados.
- **Conocimientos necesarios**: los administradores del sistema de dichos servidores deben tener un conocimiento de trabajo de los sistemas UNIX y el sistema operativo Oracle Solaris (SO Oracle Solaris).

Biblioteca de documentación del producto

La documentación y los recursos para este producto y los productos relacionados se encuentran disponibles en http://www.oracle.com/technetwork/documentation/vm-sparc-194287.html.

Comentarios

Envíenos comentarios acerca de esta documentación mediante http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CAPÍTULO 1

Descripción general de la seguridad de Oracle VM Server for SPARC

Aunque la cantidad de recomendaciones de seguridad que se incluyen en este documento dé una impresión diferente, la instalación típica de Oracle VM Server for SPARC ya incluye una buena protección contra el uso no autorizado. Existe una pequeña superficie de ataque y hay cierto grado de riesgo latente, aunque es poco probable que se produzca una explotación. Así como puede optar por instalar una alarma antirobo para proteger su hogar, además de usar otros elementos disuasivos, como cerraduras especiales en las puertas, puede tomar medidas de seguridad de red adicionales que reduzcan la posibilidad de que surjan problemas imprevistos y ayuden a minimizar posibles daños.

En este capítulo, se tratan los siguientes temas de seguridad 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 físico varias máquinas virtuales (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 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 *Oracle Solaris 10 Security Guidelines* y las *Oracle Solaris 11 Security Guidelines* para obtener información sobre la seguridad de Oracle Solaris .

El comando `ldm` invoca al Administrador de dominios lógicos y debe ejecutarse en el dominio de control para configurar dominios 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 los derechos de Oracle Solaris para consolas y las autorizaciones de `solaris.ldoms`. Consulte "Logical Domains Manager Profile Contents" de *Guía de administración de Oracle VM Server for SPARC 3.5*.

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 *Oracle Solaris 10 Security Guidelines* y las *Oracle Solaris 11 Security Guidelines*.
- Las funciones de seguridad de SO Oracle Solaris se pueden aplicar al software de Oracle VM Server for SPARC. Para obtener información completa sobre cómo garantizar la seguridad de Oracle VM Server for SPARC, consulte "Seguridad en un entorno virtualizado" [15] y "Defensa contra ataques" [17].
- 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 obtener información acerca de cómo limitar el acceso a las consolas de dominio y los comandos de administración de Oracle VM Server for SPARC, consulte el Capítulo 2, "Oracle VM Server for SPARC Security" de *Guía de administración de Oracle VM Server for SPARC 3.5*.

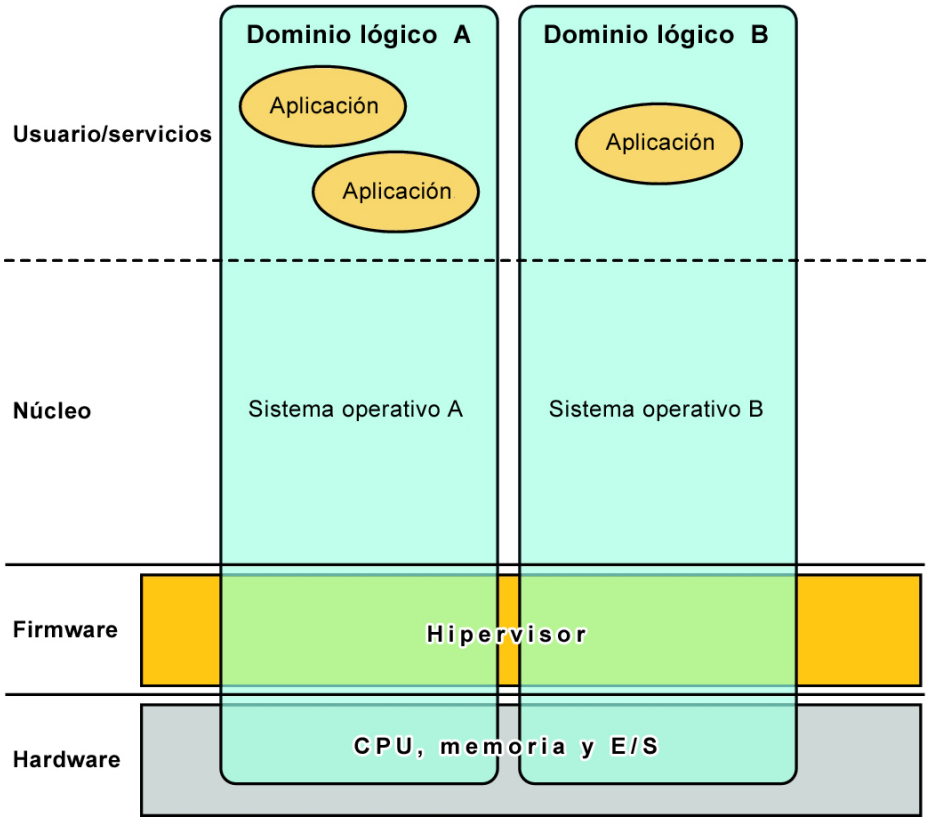
Descripción general del producto Oracle VM Server for SPARC

Oracle VM Server for SPARC proporciona capacidades de virtualización empresariales de gran eficacia para servidores SPARC T-Series, además del servidor SPARC M5 y Servidores de Fujitsu M10. El software Oracle VM Server for SPARC permite crear muchos servidores virtuales, llamados dominios lógicos, en un solo sistema. Este tipo de configuración permite aprovechar la escala de subprocesos masiva que ofrecen los servidores SPARC y el SO 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 *Guía de administración de Oracle VM Server for SPARC 3.5* y *Oracle VM Server for SPARC 3.5 Reference Manual*. Para obtener información sobre el hardware y el software necesarios, consulte *Guía de instalación de Oracle VM Server for SPARC 3.5*.

FIGURA 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 servicio* (SP), también conocido como *controlador de sistema* (SC), supervisa y ejecuta la máquina física. El Administrador de dominios lógicos es el que gestiona los dominios lógicos, no el SP.
- **Dominio de control.** El Administrador de dominios lógicos se ejecuta en este dominio y le permite crear y gestionar otros dominios lógicos, y asignar recursos virtuales a otros dominios. Solo 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 servicio.** 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 de E/S puede poseer un complejo de raíz PCIe o puede poseer una ranura PCIe o un dispositivo PCIe integrado mediante el uso de la característica de E/S directa (DIO, direct I/O). Consulte "Creating an I/O Domain by Assigning PCIe Endpoint Devices" de *Guía de administración de Oracle VM Server for SPARC 3.5*.

  Un dominio de E/S puede compartir dispositivos E/S físicos con otros dominios en forma de dispositivos virtuales cuando el dominios de E/S también se usa como dominio de servicios.
- **Dominio raíz.** Un dominio raíz tiene asignada una raíz de PCIe compleja. Este dominio posee el tejido PCIe del complejo de raíz y ofrece todos los servicios relacionados con el tejido, como el manejo de error de tejido. Un dominio raíz también es un dominio de 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 SPARC T4-4, 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 global de la configuración de Oracle VM Server for SPARC. Para obtener recomendaciones sobre la implementación del software Oracle VM Server for SPARC de manera segura, consulte “Seguridad en un entorno virtualizado” [15] y “Defensa contra ataques” [17].

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 evaluar con regularidad la seguridad del sistema. Consulte “Contramedida: creación de directrices operativas” [20].
  - Planifique cuidadosamente la arquitectura del entorno virtual para maximizar el aislamiento de los dominios. Consulte las contramedidas establecidas para “Amenaza: errores en la arquitectura del entorno virtual” [20].
  - Planifique cuidadosamente los recursos que desea asignar y determine si se van a compartir. Consulte “Contramedida: asignación cuidadosa de los recursos de hardware” [23] y “Contramedida: asignación cuidadosa de los recursos compartidos” [23].
  - Asegúrese de que los dominios lógicos estén protegidos contra la manipulación mediante la aplicación de las contramedidas establecidas para “Amenaza: manipulación del entorno de ejecución” [24] y “Contramedida: protección del SO del dominio invitado” [38].

- “Contramedida: protección de rutas de acceso interactivo” [25].
- “Contramedida: minimización del SO Oracle Solaris ” [25].
- “Contramedida: refuerzo de la protección del SO Oracle Solaris ” [26].
- “Contramedida: refuerzo de la protección del Administrador de dominios lógicos” [32].
- “Contramedida: uso de la separación de roles y el aislamiento de aplicaciones” [26], donde se describe la importancia asignar roles de funcionalidad a los distintos dominios y de asegurarse de que el dominio de control ejecute software que proporcione la infraestructura requerida para alojar dominios invitados. Debe ejecutar aplicaciones que otros sistemas pueden ejecutar en los dominios invitados que están diseñados para este propósito.
- “Contramedida: configuración de una red de gestión dedicada” [26], donde se describe una configuración de red más avanzada que conecta los servidores con SP a una red de gestión dedicada para proteger los SP del acceso a la red.

- 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 *Oracle Solaris 10 Security Guidelines* y las *Oracle Solaris 11 Security Guidelines*.
- Proteja el núcleo central del hipervisor, como se describe en “Contramedida: validación de firmas de software y firmware” [29] y “Contramedida: validación de los módulos de núcleo” [30].
- Proteja el dominio de control contra los ataques de denegación de servicio. Consulte “Contramedida: protección del acceso a la consola” [31].
- Asegúrese de que los usuarios no autorizados no puedan ejecutar Administrador de dominios lógicos. Consulte “Amenaza: uso no autorizado de utilidades de configuración” [31].
- Asegúrese de que los procesos o usuarios no autorizados no puedan acceder al dominio de servicio. Consulte “Amenaza: manipulación de un dominio de servicio” [34].
- Proteja un dominio de E/S o un dominio de servicio contra los ataques de denegación de servicio. Consulte “Amenaza: situación de denegación de servicio de un dominio de E/S o un dominio de servicio” [36].
- Asegúrese de que los procesos o usuarios no autorizados no puedan acceder al dominio de E/S. Consulte “Amenaza: manipulación de un dominio de E/S” [37].
- Desactive los servicios de administrador de dominios innecesarios. El Administrador de dominios lógicos proporciona los servicios de red necesarios para el acceso, el control y la migración de dominios. Consulte “Contramedida: refuerzo de la protección del Administrador de dominios lógicos” [32] y “Contramedida: protección de Oracle ILOM” [28].

- **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 barrera de aislamiento, lo que evita que los dominios crucen a una clase de seguridad diferente. Consulte "Contramedida: asignación cuidadosa de dominios invitados a plataformas de hardware" [20].
  - Utilice derechos para restringir la capacidad de gestionar dominios con el comando `ldm`. *Solo* 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 solo a los usuarios que necesitan acceder a los subcomandos relacionados con la lista de `ldm`. Consulte "Using Rights Profiles and Roles" de *Guía de administración de Oracle VM Server for SPARC 3.5*.
  - Use derechos para restringir el acceso a la consola *solo* de los dominios a los que usted, como administrador de Oracle VM Server for SPARC, debe acceder gestionar. *No* permita el acceso general a todos los dominios. Consulte "Controlling Access to a Domain Console by Using Rights" de *Guía de administración de Oracle VM Server for SPARC 3.5*.

Seguridad en un entorno virtualizado

A fin de proteger con eficacia el entorno virtualizado de Oracle VM Server for SPARC, el sistema operativo y los servicios que se ejecuten en cada dominio, además de reducir los efectos de una infracción, separe los servicios implementándolos en diferentes dominios.

El entorno de Oracle VM Server for SPARC utiliza un hipervisor para virtualizar la CPU, la memoria y los recursos de E/S para los dominios lógicos. Cada dominio es un servidor virtualizado discreto que debe protegerse contra posibles ataques.

Un entorno virtualizado permite consolidar varios servidores en un servidor por medio del uso compartido de recursos de hardware. En Oracle VM Server for SPARC, la CPU y los recursos de memoria se asignan de manera exclusiva a cada dominio, lo cual impide el abuso derivado del uso excesivo de la CPU o la asignación de memoria. Por lo general, los dominios de servicio proporcionan el disco y los recursos de red a muchos dominios invitados.

Al evaluar la seguridad, *siempre* suponga que el entorno tiene una falla de la que un atacante se puede aprovechar. Por ejemplo, un atacante podría aprovecharse de los puntos vulnerables del hipervisor para usurpar un sistema por completo, incluidos los dominios invitados. Por lo tanto,

siempre se deben implementar los sistemas de modo que se minimice el riesgo de daños en caso de que se produzca una infracción de seguridad.

Entorno de ejecución

El entorno de ejecución incluye los siguientes componentes:

- **Hipervisor**: firmware de específico de la plataforma que virtualiza el hardware y depende fundamentalmente del soporte de hardware que está integrado en la CPU.
- **Dominio de control**: dominio especializado que configura el hipervisor y ejecuta el Administrador de dominios lógicos, que gestiona los dominios lógicos.
- **Dominio raíz o dominio de E/S**: dominio que posee algunos o todos los dispositivos de E/S disponibles de la plataforma y los comparte con otros dominios.
- **Dominio de servicio**: dominio que ofrece servicios a otros dominios. Un dominio de servicio puede dar acceso a la consola a otros dominios o proporcionar discos virtuales. Un dominio de servicio que proporciona acceso al disco virtual a otros dominios también es un dominio de E/S.

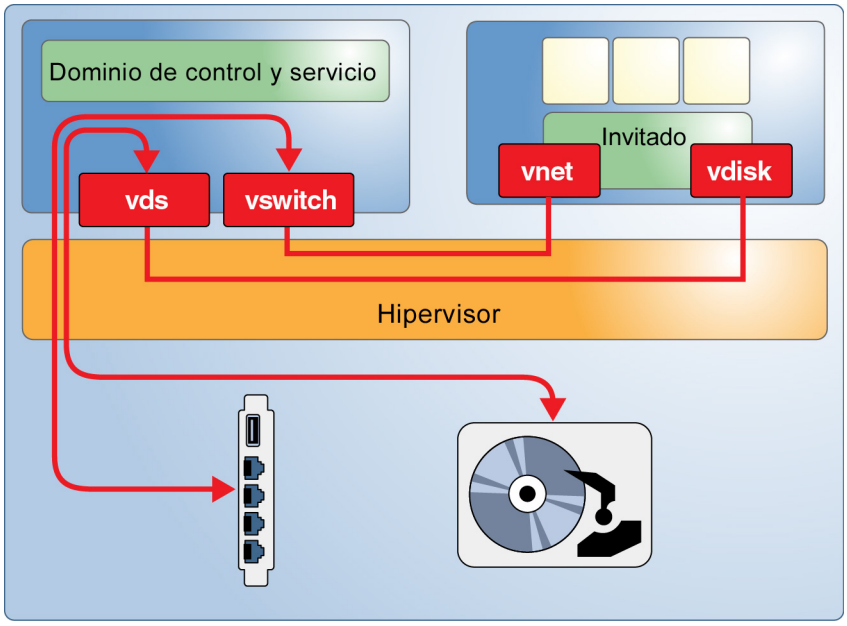
Para obtener más información sobre estos componentes, consulte Figura 1, “Hipervisor que admite dos dominios lógicos” y las descripciones de componentes más detalladas.

Puede mejorar la facilidad de mantenimiento para configuraciones de E/S redundante mediante la configuración de un segundo dominio de E/S. También puede utilizar un segundo dominio de E/S para aislar el hardware y evitar infracciones de seguridad. Para obtener información sobre las opciones de configuración, consulte *Guía de administración de Oracle VM Server for SPARC 3.5*.

Protección del entorno de ejecución

Oracle VM Server for SPARC tiene varios puntos vulnerables al ataque en el entorno de ejecución. En Figura 2, “Ejemplo de entorno de Oracle VM Server for SPARC”, se muestra una configuración sencilla de Oracle VM Server for SPARC en la que el dominio de control proporciona servicios de discos y de redes a un dominio invitado. Estos servicios se implementan por medio de los daemons y los módulos de núcleo que se ejecutan en el dominio de control. El Administrador de dominios lógicos asigna canales de dominio lógico (LDC) para cada servicio y también un cliente para facilitar la comunicación de punto a punto entre ellos. Un atacante puede aprovecharse de un error en cualquiera de los componentes para vulnerar el aislamiento de los dominios invitados. Por ejemplo, un atacante podría ejecutar un código arbitrario en el dominio de servicio o alterar las operaciones normales en la plataforma.

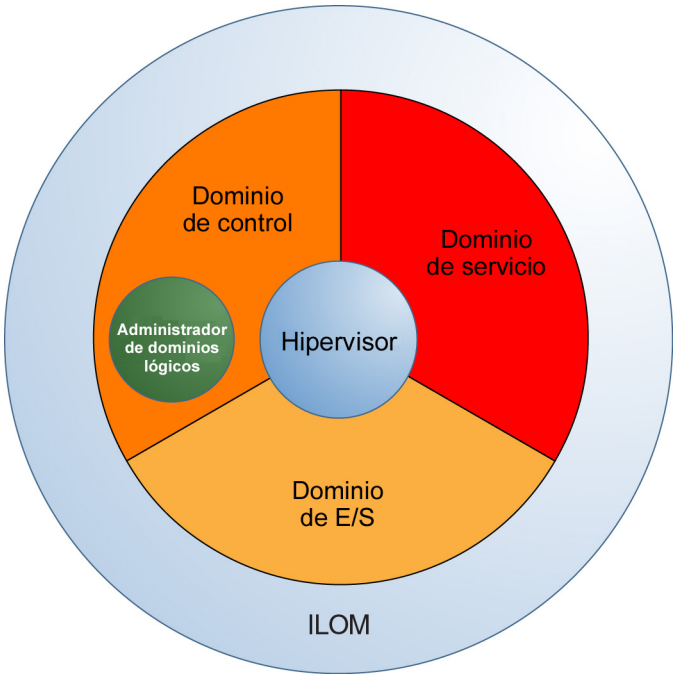
FIGURA 2 Ejemplo de entorno de Oracle VM Server for SPARC



Defensa contra ataques

La figura siguiente muestra los componentes de virtualización que constituyen el “entorno de ejecución” de Oracle VM Server for SPARC. Estos componentes no están estrictamente separados. La configuración más sencilla es combinar todas estas funciones en un único dominio. El dominio de control también puede actuar como un dominio de E/S y un dominio de servicio para otros dominios.

FIGURA 3 Componentes del entorno de ejecución



Es posible que un atacante intente vulnerar el aislamiento del sistema y manipular el hipervisor u otro componente del entorno de ejecución para acceder a un dominio invitado. Por eso debe proteger cada dominio invitado del mismo modo que protegería cualquier servidor independiente.

En el resto de este capítulo, se presentan posibles amenazas y las distintas medidas que puede tomar para hacerles frente. Cada uno de estos ataques tiene por objeto traspasar o eliminar el aislamiento de los diferentes dominios que se ejecutan en una sola plataforma. En las siguientes secciones, se describen las amenazas que puede recibir cada parte de un sistema de Oracle VM Server for SPARC:

- “Entorno operativo” [19]
- “Entorno de ejecución” [24]
- “Oracle ILOM” [27]
- “Hipervisor” [29]
- “Dominio de control” [30]

- “Administrador de dominios lógicos” [31]
- “Dominio de E/S” [36]
- “Dominio de servicio” [34]
- “Dominios invitados” [38]

Entorno operativo

El entorno operativo incluye los sistemas físicos y sus componentes, y también a los arquitectos de centros de datos, los administradores y los miembros de la organización de TI. Una infracción de seguridad se puede producir en cualquier punto del entorno operativo.

Mediante la virtualización, se coloca una capa de software entre el hardware real y los dominios invitados que ejecutan los servicios de producción, lo cual eleva la complejidad. Por lo tanto, debe planificar cuidadosamente, configurar el sistema virtual y considerar los errores humanos. Además, debe tener en cuenta que los atacantes pueden intentar acceder al entorno operativo mediante el uso de "ingeniería social".

En las siguientes secciones, se describen las distintas amenazas contra las que tendrá que luchar en el nivel del entorno operativo.

Amenaza: errores involuntarios de configuración

El principal problema de seguridad en un entorno virtualizado es mantener el servidor aislado separando segmentos de redes, segregando el acceso administrativo e implementando servidores en clases de seguridad, que son grupos de dominios que tienen los mismos privilegios y requisitos de seguridad.

Configure cuidadosamente los recursos virtuales a fin de evitar los siguientes errores:

- Crear canales de comunicación innecesarios entre los dominios invitados de producción y el entorno de ejecución
- Crear acceso innecesario a segmentos de red
- Crear conexiones no intencionales entre las clases de seguridad discretas
- Migrar un dominio invitado a la clase de seguridad equivocada de manera no intencional
- Asignar hardware insuficiente, lo cual puede ocasionar una sobrecarga inesperada de los recursos
- Asignar discos o dispositivos de E/S al dominio incorrecto

Contramedida: creación de directrices operativas

Antes de empezar, defina cuidadosamente las directrices operativas para su entorno de Oracle VM Server for SPARC. En estas directrices, se describen las siguientes tareas y su modo de ejecución:

- Gestión de parches para todos los componentes del entorno
- Implementación de los cambios de manera segura, que incluya un seguimiento y esté claramente definida
- Comprobación de los archivos de registro con una frecuencia regular
- Supervisión de la integridad y la disponibilidad del entorno

Debe realizar comprobaciones con regularidad para asegurarse de que estas directrices permanezcan actualizadas y sean adecuadas, y para verificar que se estén cumpliendo en las operaciones diarias.

Además de estas directrices, puede que se requieran muchas otras medidas técnicas para reducir el riesgo de que se realicen acciones no intencionales. Consulte “Administrador de dominios lógicos” [31].

Amenaza: errores en la arquitectura del entorno virtual

Cuando mueve un sistema físico a un entorno virtualizado, por lo general, puede mantener la misma configuración de almacenamiento si utiliza los LUN originales. Sin embargo, la configuración de red debe adaptarse al entorno virtualizado, y la arquitectura resultante puede diferir considerablemente de la arquitectura utilizada en el sistema físico.

Debe tener en cuenta cómo mantener el aislamiento de las clases de seguridad discretas y sus necesidades. Además, tenga en cuenta el hardware compartido de la plataforma y los componentes compartidos, como los conmutadores de red y los conmutadores SAN.

Para maximizar la seguridad de su entorno, asegúrese de mantener el aislamiento de los dominios invitados y las clases de seguridad. Cuando diseñe la arquitectura, anticípese a posibles errores y ataques, e implemente líneas de defensa. Un buen diseño ayuda a limitar posibles problemas de seguridad, además de controlar la complejidad y los costos.

Contramedida: asignación cuidadosa de dominios invitados a plataformas de hardware

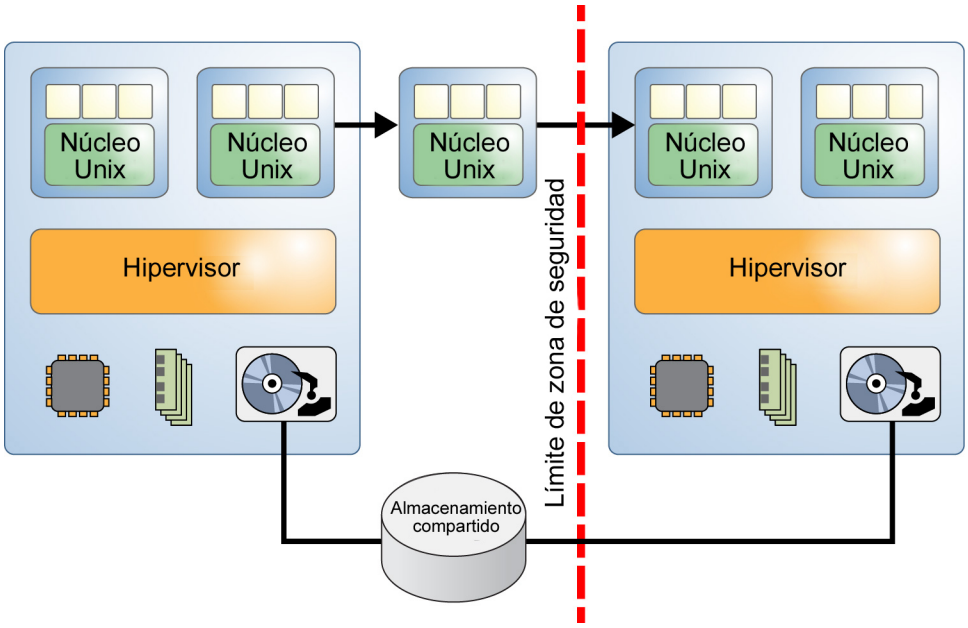
Use clases de seguridad, que son grupos de dominios que tienen los mismos privilegios y requisitos de seguridad, para aislar dominios individuales entre sí. Mediante la asignación de dominios invitados que estén en la misma clase de seguridad a una determinada plataforma

de hardware, incluso una brecha de aislamiento evita que el ataque alcance a otra clase de seguridad.

Contramedida: planificación de la migración de dominios de Oracle VM Server for SPARC

La función de migración de dominio en tiempo real puede vulnerar el aislamiento si un dominio invitado se migra de manera inadvertida a una plataforma asignada a una clase de seguridad diferente, como se muestra en la figura siguiente. Por lo tanto, de planificar cuidadosamente la migración de dominio invitado a fin de garantizar que no se permita realizar una migración que traspase los límites de las clases de seguridad.

FIGURA 4 Migración de dominio que traspasa los límites de seguridad



Para minimizar o eliminar la vulnerabilidad de seguridad que presenta la operación de migración, debe intercambiar e instalar manualmente todos los certificados de host generados por `ldmd` fuera de banda entre cada par de equipos de origen y de destino. Para obtener información sobre cómo configurar los certificados SSL, consulte "Configuring SSL Certificates for Migration" de *Guía de administración de Oracle VM Server for SPARC 3.5*.

Contramedida: configuración correcta de conexiones virtuales

La pérdida de registro de todas las conexiones de red virtual puede hacer que un dominio obtenga acceso erróneo a un segmento de red. Por ejemplo, un acceso que burle el firewall o una clase de seguridad.

Para reducir el riesgo de errores de implementación, planifique cuidadosamente y documente todas las conexiones virtuales y físicas del entorno. Optimice el plan de conexión de dominio para obtener más simplicidad y mejor capacidad de gestión. Documente claramente el plan y compruebe la precisión de la implementación en función del plan antes de entrar en producción. Incluso una vez que su entorno virtual esté en producción, verifique la implementación en función del plan con regularidad.

Contramedida: uso de etiquetas en VLAN

Puede utilizar etiquetas en VLAN para consolidar varios segmentos Ethernet en una única red física. Esta función también está disponible para los conmutadores virtuales. Para mitigar los riesgos que conllevan los errores de software en la implementación de los conmutadores virtuales, configure un conmutador virtual por VLAN y NIC física. Si desea agregar protección contra errores en el controlador Ethernet, no utilice VLAN con etiquetas. Sin embargo, la probabilidad de que se produzcan estos errores es baja, ya que esta vulnerabilidad de VLAN con etiquetas es muy conocida. Las pruebas de intrusiones en los servidores Sun SPARC T-Series de Oracle con el software Oracle VM Server for SPARC no mostraron esta vulnerabilidad.

Contramedida: uso de aplicaciones de seguridad virtuales

Las aplicaciones de seguridad, como los filtros de paquetes y los firewalls, son instrumentos de aislamiento y protegen el aislamiento de las clases de seguridad. Estas aplicaciones son vulnerables a las mismas amenazas que cualquier otro dominio invitado, de modo que su uso no garantiza una protección completa contra una brecha de aislamiento. Por lo tanto, tenga en cuenta todos los aspectos de riesgo y seguridad antes de decidir si desea virtualizar un servicio así.

Amenaza: efectos secundarios del uso compartido de recursos

El uso compartido de recursos en un entorno virtualizado puede provocar ataques de denegación de servicio (DoS), lo cual sobrecarga un recurso hasta que se afecta negativamente otro componente, por ejemplo, otro dominio.

En un entorno de Oracle VM Server for SPARC, solamente algunos recursos pueden verse afectados por un ataque de denegación de servicio. La CPU y los recursos de memoria se asignan exclusivamente a cada dominio invitado, lo cual impide la mayoría de los ataques de denegación de servicio. Incluso la asignación exclusiva de estos recursos puede ralentizar un dominio invitado mediante lo siguiente:

- Hiperpaginación de las áreas de caché que se comparten entre hilos y se asignan a dos dominios invitados
- La sobrecarga del ancho de banda de la memoria

A diferencia de la CPU y los recursos de memoria, el disco y los servicios de red, generalmente, se comparten entre dominios invitados. Estos servicios se proporcionan a los dominios invitados mediante uno o más dominios de servicio. Analice detalladamente cómo asignar y distribuir estos recursos entre los dominios invitados. Tenga en cuenta que cualquier configuración que permita alcanzar el máximo rendimiento y uso de recursos a la vez minimiza el riesgo de efectos secundarios.

Evaluación: efectos secundarios del uso compartido de recursos

Se puede saturar un enlace de red o se puede sobrecargar un disco, ya sea que estén asignados exclusivamente a un dominio o se compartan entre dominios. Estos ataques afectan la disponibilidad de un servicio mientras dure el ataque. El blanco de ataque no se ve comprometido, y no se pierden datos. Los efectos de esta amenaza se pueden minimizar fácilmente, pero debe tenerla en cuenta aunque esté limitada a los recursos de red y de disco en Oracle VM Server for SPARC.

Contramedida: asignación cuidadosa de los recursos de hardware

Asegúrese de asignar solamente los recursos de hardware necesarios para dominios invitados. Asegúrese de anular la asignación de un recurso cuando ya no sea necesario; por ejemplo, un puerto de red o una unidad de DVD que se requiera solamente durante una instalación. Si esto se pone en práctica, se minimiza la cantidad de puntos de entrada que puede usar un atacante.

Contramedida: asignación cuidadosa de los recursos compartidos

Los recursos de hardware compartidos, como los puertos de red física, pueden ser un blanco vulnerable a los ataques de denegación de servicio. Para limitar el impacto de los ataques de denegación de servicio a un único grupo de dominios invitados, determine con cuidado qué dominios invitados comparten qué recursos de hardware.

Por ejemplo, los dominios invitados que comparten recursos de hardware se pueden agrupar según tengan la misma disponibilidad o los mismos requisitos de seguridad. Además de esta agrupación, puede aplicar diferentes tipos de controles de recursos.

Debe tener en cuenta cómo compartir los recursos de red y de disco. Puede mitigar los problemas separando el acceso al disco mediante rutas de acceso físico dedicado o servicios de disco virtual dedicado.

Resumen: efectos secundarios del uso compartido de recursos

Todas las contramedidas descritas en esta sección requieren que se comprendan todos los detalles técnicos de su implementación y sus consecuencias para la seguridad. Planifique con cuidado, elabore bien la documentación y mantenga la arquitectura tan simple como sea posible. Asegúrese de comprender las consecuencias del hardware virtualizado, de modo que pueda prepararse para implementar el software Oracle VM Server for SPARC de manera segura.

Los dominios lógicos pueden combatir los efectos de uso compartido de la CPU y la memoria, y en realidad el uso compartido es poco. No obstante, es conveniente aplicar controles de recursos, como la gestión de recursos de Solaris en los dominios invitados. El uso de estos controles brinda protección contra el mal comportamiento de la aplicación, ya sea en entornos virtuales o en entornos no virtualizados.

Entorno de ejecución

En la Figura 3, “Componentes del entorno de ejecución”, se muestran los componentes del entorno de ejecución. Cada componente proporciona determinados servicios que, en conjunto, forman la plataforma general en la que se ejecutarán los dominios invitados de producción. Configurar correctamente los componentes es de vital importancia para la integridad del sistema.

Todos los componentes del entorno de ejecución pueden ser puntos vulnerables para un atacante. En esta sección, se describen las amenazas que podrían afectar a cada componente en el entorno de ejecución. Algunas amenazas y contramedidas se pueden aplicar a más de un componente.

Amenaza: manipulación del entorno de ejecución

Mediante la manipulación del entorno de ejecución, puede obtener el control de diversas maneras. Por ejemplo, puede instalar firmware manipulado en Oracle ILOM para buscar en todos los dominios invitados de E/S desde adentro de un dominio de E/S. Mediante tal ataque,

se puede acceder al sistema y cambiarle la configuración. Un atacante que asume el control de un dominio de control de Oracle VM Server for SPARC puede volver a configurar el sistema de cualquier manera y un atacante que asume el control de un dominio de E/S puede hacer cambios en dispositivos de almacenamiento conectados, como los discos de inicio.

Evaluación: manipulación del entorno de ejecución

Un atacante que logre acceder a Oracle ILOM o a cualquier dominio en el entorno de ejecución puede leer y manipular todos los datos que están disponibles para el dominio. Este acceso se puede obtener mediante la red o por medio de un error en la pila de virtualización. Es difícil perpetrar un ataque así, ya que, por lo general, no se puede atacar a Oracle ILOM y a los dominios de manera directa.

Las contramedidas para protegerse contra la manipulación del entorno de ejecución son la práctica de seguridad estándar y deben implementarse en todos los sistemas. Las prácticas de seguridad estándar presentan una capa de protección adicional de todo el entorno de ejecución que reduce aún más el riesgo de intrusiones y manipulación.

Contramedida: protección de rutas de acceso interactivo

Asegúrese de crear *solamente* cuentas que sean necesarias para las aplicaciones que se ejecutan en el sistema.

Asegúrese de que las cuentas que son necesarias para la administración estén protegidas mediante la autenticación basada en claves o contraseñas seguras. Estas claves o contraseñas no se deben compartir entre diferentes dominios. Asimismo, considere la posibilidad de implementar la autenticación de dos factores o la "regla de dos personas" para tomar ciertas medidas.

No utilice el inicio de sesión anónimo como `root` para garantizar la total rastreabilidad y responsabilidad de los comandos que se ejecutan en el sistema. En su lugar, utilice derechos para otorgar acceso a administradores individuales *solamente* para las funciones que ellos pueden llevar a cabo. Asegúrese de que el acceso a redes administrativas siempre use cifrado, como SSH, y de que la estación de trabajo de un administrador se trate como un sistema de alta seguridad.

Contramedida: minimización del SO Oracle Solaris

Cualquier software que esté instalado en un sistema puede estar en peligro. Por lo tanto, sebe asegurarse de instalar *solamente* el software necesario para minimizar las posibilidades de vulneración.

Contramedida: refuerzo de la protección del SO Oracle Solaris

Además de instalar una versión minimizada del SO Oracle Solaris , configure los paquetes a fin de “reforzar” la protección del software contra los ataques. Primero, ejecute servicios de red limitados para desactivar eficazmente todos los servicios de red, salvo SSH. Esta política es el comportamiento predeterminado en los sistemas Oracle Solaris 11. Para obtener información sobre cómo proteger el SO Oracle Solaris , consulte *Oracle Solaris 10 Security Guidelines* y *Oracle Solaris 11 Security Guidelines*.

Contramedida: uso de la separación de roles y el aislamiento de aplicaciones

Según la necesidad, las aplicaciones de producción están conectadas a otros sistemas y, como resultado, están más expuestas a ataques externos. *No* implemente aplicaciones de producción en un dominio que forme parte del entorno de ejecución. En su lugar, asegúrese de implementarlas *solamente* en dominios invitados que no tengan más privilegios.

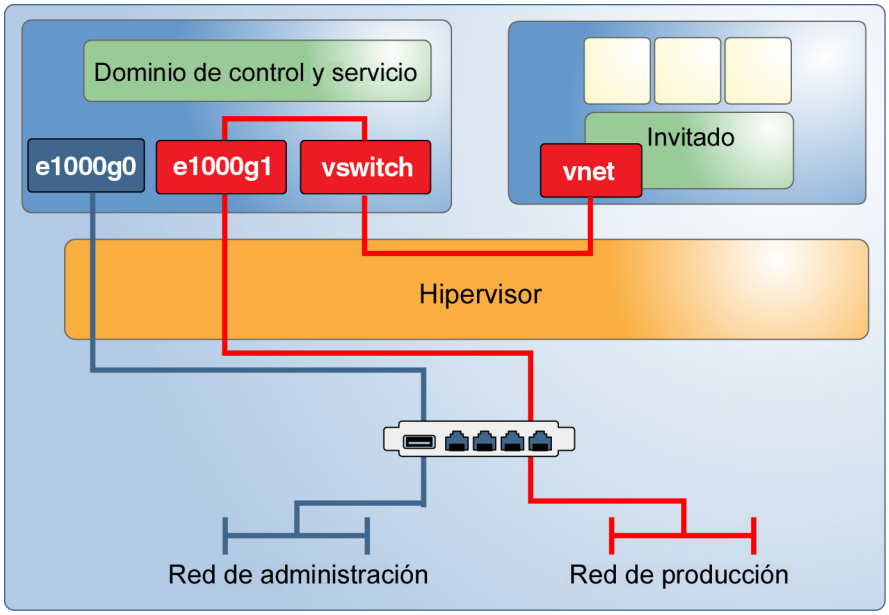
El entorno de ejecución solo debe proporcionar la infraestructura necesaria para estos dominios invitados. La separación del entorno de ejecución de las aplicaciones de producción permite implementar la granularidad en la administración de privilegios. Un administrador de dominio invitado de producción no requiere acceso al entorno de ejecución y un administrador del entorno de ejecución no necesita acceso a los dominios invitados de producción. Si es posible, asigne los distintos roles del entorno de ejecución, como el dominio de control y el dominio de E/S, en diferentes dominios. Este tipo de configuración reduce la magnitud del daño que puede generarse si cualquiera de estos dominios recibe un ataque.

También puede ampliar la separación de roles en el entorno de red que se utiliza para conectar los distintos servidores.

Contramedida: configuración de una red de gestión dedicada

Conecte todos los servidores que estén equipados con procesadores de servicio (SP) a una red de gestión dedicada. Esta configuración también se recomienda para los dominios del entorno de ejecución. Si los dominios estarán en red, alójelos en su propia red dedicada. *No* conecte los dominios del entorno de ejecución directamente en las redes que se asignan a los dominios de producción. Aunque puede realizar todo el trabajo administrativo mediante una única conexión de consola que está disponible mediante el SP de Oracle ILOM, esta configuración complica la administración de modo tal que no se puede llevar a la práctica. Si se separan las redes de administración y de producción, se obtiene protección contra intrusiones y manipulaciones. Con esta separación, también se elimina la posibilidad de ataque en el entorno de ejecución de los dominios invitados por la red compartida.

FIGURA 5 Red de gestión dedicada



Oracle ILOM

Todos los sistemas Oracle SPARC actuales incluyen un controlador integrado del sistema (Oracle ILOM), que tiene las siguientes capacidades:

- Gestiona los controles básicos del entorno, como la velocidad del ventilador y la energía del chasis
- Permite actualizar el firmware
- Proporciona la consola del sistema para el dominio de control

Puede acceder a Oracle ILOM mediante una conexión serie o, para acceder mediante un puerto de red, puede usar SSH, HTTP, HTTPS, SNMP o IPMI. Los Servidores de Fujitsu M10 utilizan XSCF en lugar de {ILOM:} para realizar funciones similares.

Amenaza: total denegación del servicio del sistema

Un atacante que obtiene control de Oracle ILOM puede poner en peligro el sistema de muchas maneras, incluidas las siguientes:

- Cortando el suministro de energía de todos los dominios invitados en ejecución
- Instalando firmware manipulado para obtener acceso a al menos a un dominio invitado

Estos escenarios se aplican a cualquier sistema que tenga un dispositivo controlador. En un entorno virtualizado, los daños pueden ser mucho mayores que en un entorno físico porque muchos dominios que se alojan en el mismo contenedor del sistema pueden estar en riesgo.

Del mismo modo, un atacante que asume el control del dominio de control o de un dominio de E/S puede desactivar fácilmente todos los dominios invitados dependientes y cerrar así los servicios de E/S correspondientes.

Evaluación: total denegación del servicio del sistema

Generalmente, Oracle ILOM se conecta a una red administrativa que debe estar bien protegida y aislada de las redes de producción normales.

Asimismo, un atacante puede vulnerar un dominio de servicio desde la red o por un error en la pila de virtualización y, a continuación, bloquear un dominio invitado de E/S o cerrar el sistema. Aunque los daños son limitados porque los datos no se pierden ni se ponen en riesgo, una gran cantidad de dominios invitados pueden verse afectados. Por lo tanto, establezca protección contra esta amenaza latente para limitar los posibles daños.

Contramedida: protección de Oracle ILOM

Como el procesador de servicio del sistema, Oracle ILOM controla funciones críticas, como el suministro de energía del chasis, las configuraciones de inicio de Oracle VM Server for SPARC y el acceso de la consola al dominio de control. Las siguientes medidas permiten proteger a Oracle ILOM:

- Colocar el puerto de red de Oracle ILOM en un segmento de red que esté separado de la red administrativa, que se utiliza para los dominios en el entorno de ejecución.
- Desactivar todos los servicios que no sean necesarios para realizar operaciones, como HTTP, IPMI, SNMP, HTTPS y SSH.
- Configurar cuentas de administrador personales y dedicadas que otorguen solamente los derechos requeridos. Para maximizar la responsabilidad de las acciones realizadas por los administradores, asegúrese de crear cuentas de administrador personales. Este tipo de acceso es especialmente importante para el acceso a la consola, las actualizaciones de firmware y la gestión de configuraciones de inicio.

Hipervisor

El hipervisor es la capa de firmware que implementa y controla la virtualización del hardware real. El hipervisor incluye los siguientes componentes:

- El hipervisor real, que se implementa en el firmware y es compatible con las CPU de los sistemas.
- Los módulos de núcleo que se ejecutan en el dominio de control para configurar el hipervisor.
- Los módulos de núcleo y los daemons que se ejecutan en los dominios de E/S y los dominios de servicio para proporcionar E/S virtualizada, y los módulos de núcleo que se comunican por medio de canales de dominio lógico (LDC).
- Los módulos de núcleo y los controladores de dispositivos que se ejecutan en los dominios invitados para acceder a dispositivos de E/S virtualizados y los módulos de núcleo que se comunican por medio de los LDC.

Amenaza: vulneración del aislamiento

Un atacante puede usurpar los dominios invitados o todo el sistema vulnerando el entorno de tiempo de ejecución aislado que proporciona el hipervisor. Potencialmente, esta amenaza puede causar los daños más graves en el sistema.

Evaluación: vulneración del aislamiento

El diseño de un sistema modular puede mejorar el aislamiento mediante el otorgamiento de diferentes niveles de privilegios a los dominios invitados, el hipervisor y el dominio de control. Cada módulo funcional se implementa en un módulo de núcleo, controlador de dispositivo o daemon configurable e independiente. Esta modularidad requiere API limpias y protocolos de comunicación simples, lo cual reduce el riesgo de errores en general.

Incluso si parece poco probable que se vulnere un error, con los daños potenciales un atacante puede tomar el control de todo el sistema.

Contramedida: validación de firmas de software y firmware

Aunque se pueden descargar el firmware del sistema y los parches del sistema operativo directamente desde un sitio web de Oracle, estos parches se pueden manipular. Antes de instalar el software, asegúrese de verificar las sumas de comprobación MD5 de los paquetes de software. Oracle publica las sumas de comprobación de todo el software descargable.

Contramedida: validación de los módulos de núcleo

Oracle VM Server for SPARC utiliza varios módulos de núcleo y controladores para implementar la virtualización general del sistema. Los módulos de núcleo y la mayoría de los archivos binarios que se distribuyen con el SO Oracle Solaris incluyen una firma digital. Utilice la utilidad `elfsign` para comprobar la firma digital de cada módulo de núcleo y controlador. Puede utilizar el comando `pkg verify` de Oracle Solaris 11 para comprobar la integridad del archivo binario de Oracle Solaris . Consulte `https://blogs.oracle.com/cmt/entry/solaris_fingerprint_database_how_it`.

Primero, debe establecer la integridad de la utilidad `elfsign`. Use la herramienta básica de creación de informes de auditoría (BART) para automatizar el proceso de verificación de firma digital. En Integrating BART and the Solaris Fingerprint Database in the Solaris 10 Operating System (`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-005-bart-solaris-fp-db-276999.pdf`), se describe cómo combinar la BART y la base de datos de huellas de Solaris para realizar automáticamente comprobaciones de integridad similares. Aunque la base de datos de huellas se haya discontinuado, los conceptos que se describen en este documento se pueden poner en práctica de un modo similar mediante el uso de `elfsign` y la BART.

Puede usar la función de inicio verificado como una contramedida para validar los módulos de núcleo. Para configurar la validación automatizada de los módulos de núcleo en el momento del inicio, establezca las políticas de inicio verificado en Oracle ILOM. Consulte los documentos de su plataforma específica en `http://docs.oracle.com/en/hardware/`. Para validar módulos de núcleo en el dominio de control, establezca las políticas de inicio verificado en Oracle ILOM. Para validar los módulos de núcleo en los dominios invitados, utilice Administrador de dominios lógicos para establecer las políticas de inicio verificado.

Dominio de control

El dominio de control, que a menudo tiene los roles de un dominio de E/S y un dominio de servicio, se deben mantener a salvo porque puede modificar la configuración del hipervisor, el cual controla todos los recursos de hardware conectados.

Amenaza: denegación de servicio de dominio de control

El cierre del dominio de control puede provocar una denegación de servicio de las herramientas de configuración. Debido a que el dominio de control solo es necesario para realizar cambios de configuración, los dominios invitados no se ven afectados si acceden a su red y sus recursos de disco por medio de otros dominios de servicio.

Evaluación: denegación de servicio de dominio de control

Atacar al dominio de control mediante la red equivale a atacar cualquier otra instancia de SO Oracle Solaris que esté correctamente protegida. El daño que ocasiona el cierre o la similar denegación de servicio del dominio de control es relativamente bajo. Sin embargo, los dominios invitados se ven afectados si el dominio de control también actúa como dominio de servicio para estos dominios invitados.

Contramedida: protección del acceso a la consola

Evite la configuración del acceso de redes administrativas al entorno de ejecución de los dominios. Este escenario requiere el uso del servicio de consola de Oracle ILOM para el dominio de control para realizar todas las tareas de administración. El acceso de consola a todos los otros dominios se puede seguir usando mediante el servicio `vntsd` que está en ejecución en el dominio de control.

Analice esta opción en detalle. Aunque esta opción reduce el riesgo de recibir ataques por la red administrativa, solo un administrador a la vez puede acceder a la consola.

Para obtener información sobre cómo configurar `vntsd` de manera segura, consulte "How to Enable the Virtual Network Terminal Server Daemon" de *Guía de administración de Oracle VM Server for SPARC 3.5*.

Administrador de dominios lógicos

El Administrador de dominios lógicos se ejecuta en el dominio de control y se utiliza para configurar el hipervisor y crear y configurar todos los dominios y sus recursos de hardware. Asegúrese de que se registre y controle el uso del Administrador de dominios lógicos.

Amenaza: uso no autorizado de utilidades de configuración

Es posible que un atacante tome el control del ID de usuario de un administrador o que un administrador de un grupo diferente obtenga acceso no autorizado a otro sistema.

Evaluación: uso no autorizado de utilidades de configuración

Asegúrese de que un administrador no tenga el acceso innecesario a un sistema mediante la implementación de una gestión de identidades que esté bien mantenida. Asimismo, implemente un control de acceso estricto y detallado, y otras medidas, como la regla de dos personas.

Contramedida: aplicación de la regla de dos personas

Considere la posibilidad de implementar una regla de dos personas para el Administrador de dominios lógicos y otras herramientas administrativas mediante el uso de derechos. Esta regla protege contra ataques de ingeniería social, cuentas de administrador riesgosas y errores humanos.

Contramedida: uso de derechos para el Administrador de dominios lógicos

Mediante el uso de derechos para el comando `ldm`, puede implementar un control de acceso específico y mantener una rastreabilidad completa. Para obtener información sobre la configuración de los derechos, consulte *Guía de administración de Oracle VM Server for SPARC 3.5*. El uso de derechos protege contra errores humanos porque no todas las funciones del comando `ldm` están disponibles para todos los administradores.

Contramedida: refuerzo de la protección del Administrador de dominios lógicos

Desactive los servicios de administrador de dominios innecesarios. El Administrador de dominios lógicos proporciona los servicios de red necesarios para el acceso, el control y la migración de dominios. La desactivación de los servicios de red reduce la superficie de ataque del Administrador de dominios lógicos al mínimo requerido para que funcione normalmente. Este escenario permite combatir los ataques de denegación de servicio y cualquier otro intento de uso indebido de los servicios de red.

Nota - A pesar de que desactivar los servicios de administrador de dominios ayuda a minimizar la superficie de ataque, no se pueden conocer de antemano todos los efectos secundarios que pueden llegar a afectar a una configuración dada.

Desactive cualquiera de los siguientes servicios de red cuando no estén en uso:

- Servicio de migración en el puerto TCP `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 obtener información sobre cómo desactivar este servicio, consulte "XML Transport" de *Guía del desarrollador de Oracle VM Server for SPARC 3.5*.

La desactivación de XMPP impide el funcionamiento de algunas herramientas de gestión y funciones de Oracle VM Server for SPARC clave. Consulte “Interfaz XML de Oracle VM Server for SPARC” [43].

- El protocolo simple de administración de red (SNMP, Simple Network Management Protocol) en el puerto UDP `161`

  Determine si desea utilizar Base de datos de información de administración (MIB) de Oracle VM Server for SPARC 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 MIB de Oracle VM Server for SPARC.** Instale MIB de Oracle VM Server for SPARC de manera segura. Consulte “How to Install the Oracle VM Server for SPARC MIB Software Package” de *Guía del usuario de la base de información de gestión de Oracle VM Server for SPARC 3.5* y Capítulo 3, “Managing Security” de *Guía del usuario de la base de información de gestión de Oracle VM Server for SPARC 3.5*.
  - **Desactive el servicio SNMP.** Para obtener información sobre cómo desactivar este servicio, consulte “How to Remove the Oracle VM Server for SPARC MIB Software Package” de *Guía del usuario de la base de información de gestión de Oracle VM Server for SPARC 3.5*.
- Servicio de detección en dirección de multidifusión `239.129.9.27` y puerto `64535`

Nota - Tenga en cuenta que el mecanismo de descubrimiento también es utilizado por el daemon `ldmd` para detectar colisiones cuando se asignan direcciones MAC automáticamente. Si desactiva el servicio de detección, la detección de colisiones de direcciones MAC no funcionará y la asignación automática de direcciones MAC no funcionará correctamente.

No puede desactivar este servicio mientras se ejecuta `ldmd`, el daemon de Administrador de dominios lógicos. 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 Administrador de dominios lógicos. 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 Capítulo 20, “IP Filter in Oracle Solaris (Overview)” de *Oracle Solaris Administration: IP Services* y “Using IP Filter Rule Sets” de *Oracle Solaris Administration: IP Services*.

Consulte también “Contramedida: protección de Oracle ILOM” [28].

Dominio de servicio

Un dominio de servicio proporciona algunos servicios virtuales a los dominios invitados del sistema. Es posible que entre dichos servicios se incluya un conmutador virtual, un disco virtual o un servicio de consola virtual.

En Figura 6, “Ejemplo de dominio de servicio”, se muestra un ejemplo de un dominio de servicio que ofrece servicios de consola. A menudo el dominio de control aloja los servicios de consola y, por lo tanto, también es un dominio de servicio. Los dominios del entorno de ejecución a menudo combinan las funciones de un dominio de control, un dominio de E/S y un dominio de servicio en uno o dos dominios.

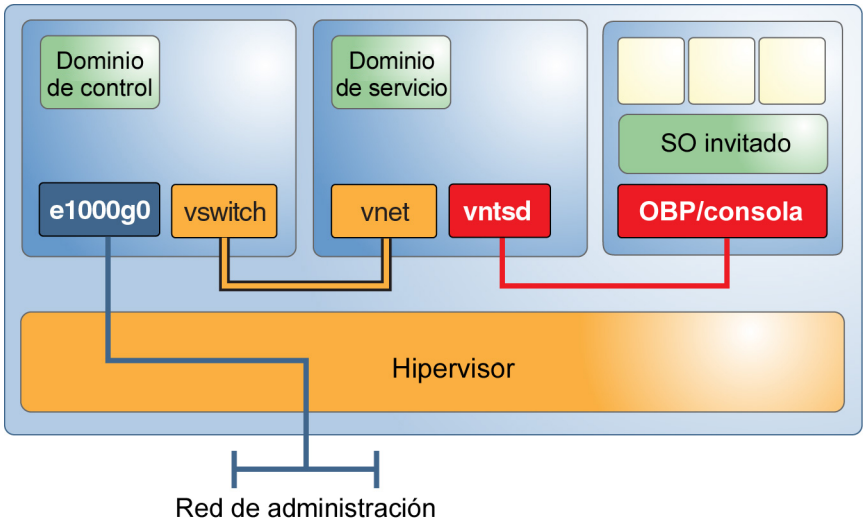
Amenaza: manipulación de un dominio de servicio

Un atacante que obtiene el control de un dominio de servicio puede manipular los datos o escuchar cualquier comunicación que se lleve a cabo mediante los servicios ofrecidos. Este control puede incluir el acceso a la consola en dominios invitados, el acceso a los servicios de red o el acceso a los servicios de disco.

Evaluación: manipulación de un dominio de servicio

Aunque las estrategias de ataque son las mismas para un ataque al dominio de control, los posibles daños son menores porque el atacante no puede modificar la configuración del sistema. Los daños resultantes pueden incluir el robo o la manipulación de datos que se ofrezcan por medio del dominio de servicio, pero no la manipulación de las fuentes de los datos. Según el servicio, puede que se requiera que el atacante intercambie los módulos de núcleo.

FIGURA 6 Ejemplo de dominio de servicio



Contramedida: dominios de servicios separados por la granularidad

Si es posible, establezca que cada dominio de servicio ofrezca solamente *un* servicio a sus clientes. Esta configuración garantiza que solo un servicio quede en riesgo si se vulnera un dominio de servicio. Sin embargo, debe asegurarse de evaluar la importancia de este tipo de configuración en función de la complejidad adicional. Tenga en cuenta que es muy recomendable tener dominios de E/S redundantes.

Contramedida: aislamiento de dominios de servicio y dominios invitados

Puede aislar los dominios de servicio de Oracle Solaris 10 y Oracle Solaris 11 de los dominios invitados. Las siguientes soluciones se muestran en el orden preferido de implementación:

- Asegúrese de que el dominio de servicio y el dominio invitado no compartan el mismo puerto de red. Además, no conecte ninguna interfaz de conmutador virtual en el dominio de servicio. Para los dominios de servicio de Oracle Solaris 11, no conecte ninguna VNIC en los puertos físicos que se utilizan para los conmutadores virtuales.

- Si debe utilizar el mismo puerto de red para el SO Oracle Solaris 10 y el SO Oracle Solaris 11, coloque el tráfico del dominio de E/S en una VLAN que no sea utilizada por los dominios invitados.
- Si no puede implementar ninguna de las soluciones anteriores, no conecte el conmutador virtual en el SO Oracle Solaris 10 y aplique los filtros IP en el SO Oracle Solaris 11.

Contramedida: restricción del acceso a las consolas virtuales

Asegúrese de que el acceso a las consolas virtuales individuales se limite *solamente* a los usuarios que deban acceder a ellos. Esta configuración garantiza que ningún administrador tenga acceso a todas las consolas, lo cual impide que se acceda a consolas que no se hayan asignado a una cuenta riesgosa. Consulte "How to Create Default Services" de *Guía de administración de Oracle VM Server for SPARC 3.5*.

Dominio de E/S

Cualquier dominio que tiene acceso directo a dispositivos físicos de E/S, como puertos de red o discos, es un dominio de E/S. Para obtener información sobre la configuración de dominios de E/S, consulte Capítulo 6, "Configuring I/O Domains" de *Guía de administración de Oracle VM Server for SPARC 3.5*.

Un dominio de E/S también puede ser un dominio de servicio si proporciona servicios de E/S a los dominios invitados, lo cual proporciona a los dominios el acceso al hardware.

Amenaza: situación de denegación de servicio de un dominio de E/S o un dominio de servicio

Un atacante que bloquea los servicios de E/S de un dominio de E/S se asegura de que todos los dominios invitados dependientes queden igualmente bloqueados. Para que un ataque de denegación de servicio se realice con éxito puede que se sobrecargue la red back-end o la infraestructura de discos, o que se introduzca un fallo en el dominio. Cualquiera de estos ataques puede forzar el dominio para que se bloquee o emita un aviso grave. Del mismo modo, un atacante que suspende servicios del dominio de servicio hace que cualquier dominio invitado que dependa de estos servicios se cuelgue inmediatamente. Si el dominio invitado se cuelga, su funcionamiento se reanuda cuando se reanuda el servicio de E/S.

Evaluación: situación de denegación de servicio de un dominio de E/S o un dominio de servicio

Los ataques de denegación de servicio suelen realizarse en la red. Dicho ataque puede realizarse con éxito si los puertos de red están abiertos para la comunicación, y el tráfico de red puede ocasionar un desborde. Una pérdida de servicio resultante bloquea los dominios invitados dependientes. Un ataque similar a los recursos de disco podría realizarse por medio de la infraestructura SAN o con un ataque al dominio de E/S. El único daño que se ocasiona es la detención temporal de todos los dominios invitados dependientes. Aunque el impacto de las tareas de denegación de servicio podría ser considerable, los datos no se pierden ni quedan en riesgo, y la configuración del sistema permanece intacta.

Contramedida: configuración granular de los dominios de E/S

La configuración de varios dominios de E/S reduce el impacto de que un dominio falle o esté en riego. Puede asignar ranuras PCIe individuales a un dominio invitado para darle capacidades de dominio de E/S. Si el dominio raíz que posee el bus PCIe se bloquea, el bus se restablece, lo cual ocasiona posteriormente un bloqueo del dominio que se había asignado a la ranura individual. Esta función no elimina por completo la necesidad de tener dos dominios raíz que tengan cada uno un bus PCIe independiente.

Contramedida: configuración de dominios raíz y hardware redundantes

La alta disponibilidad contribuye también a mejorar la seguridad porque garantiza que los servicios puedan soportar los ataques de denegación de servicio. Oracle VM Server for SPARC implementa metodologías de alta disponibilidad, como el uso de los discos redundantes y los recursos de red en dominios de E/S redundantes. Esta opción de configuración permite realizar actualizaciones sucesivas de los dominios de E/S y protege contra el impacto de un fallo del dominio de E/S que se ocasione por un ataque certero de denegación de servicio. Gracias a SR-IOV, los dominios invitados pueden tener acceso directo a los dispositivos de E/S individuales. Sin embargo, si SR-IOV no es una opción factible, considere la posibilidad de crear dominios de E/S redundantes. Consulte “Contramedida: dominios de servicios separados por la granularidad” [35].

Amenaza: manipulación de un dominio de E/S

Un dominio de E/S tiene acceso directo a dispositivos back-end, por lo general, discos, a los cuales virtualiza para luego ofrecerlos a los dominios invitados. Si un atacante logra su objetivo, obtiene acceso completo a estos dispositivos y puede leer los datos confidenciales o manipular el software en los discos de inicio de los dominios invitados.

Evaluación: manipulación de un dominio de E/S

Es tan probable que se realice un ataque certero al dominio de E/S como a un dominio de servicio o al dominio de control. El dominio de E/S es un blanco atractivo porque brinda acceso potencial a una gran cantidad de dispositivos de disco. Por lo tanto, tenga en cuenta esta amenaza cuando trabaje con datos confidenciales en un dominio invitado que se ejecute en discos virtualizados.

Contramedida: protección de discos virtuales

Cuando un dominio de E/S se encuentra en riesgo, el atacante tiene acceso total a los discos virtuales del dominio invitado.

Para proteger el contenido de los discos virtuales, haga lo siguiente:

- **Cifrado de los contenidos de los discos virtuales.** En los sistemas Oracle Solaris 10, puede utilizar una aplicación que cifra sus propios datos, como `pgp`/`gpg` o los espacios de tablas cifrados de Oracle 11g. En los sistemas Oracle Solaris 11, puede utilizar conjuntos de datos cifrados ZFS para proporcionar cifrado transparente de todos los datos almacenados en el sistema de archivos.
- **Distribución de los datos en varios discos virtuales en diferentes dominios de E/S.** Un dominio invitado puede crear un volumen en bandas (RAID 1/RAID 5), con bandas en varios discos virtuales que se obtienen de dos dominios de E/S. El atacante tendría dificultades para hacer uso de la parte de los datos que está disponible si uno de estos dominios de E/S se encuentra en riesgo.

Dominios invitados

Aunque los dominios invitados no forman parte del entorno de ejecución, son el blanco de ataque más probable porque están conectados a la red. Un atacante que vulnera un sistema virtualizado puede atacar el entorno de ejecución.

Contramedida: protección del SO del dominio invitado

El sistema operativo en el dominio invitado suele ser la primera línea de defensa contra cualquier ataque. Con la excepción de los ataques que se originan en el centro de datos, un atacante debe acceder a un dominio invitado que tenga conexiones externas antes de intentar vulnerar el aislamiento del dominio invitado y capturar el entorno completo. Por lo tanto, debe reforzar la protección del sistema operativo del dominio invitado.

Para reforzar más la protección del sistema operativo, puede implementar la aplicación en Zona de Solaris, lo cual coloca una capa adicional de aislamiento entre el servicio de red de la aplicación y el sistema operativo del dominio invitado. Si se efectúa ataque certero en el servicio, se pone en riesgo solo la zona, y no el sistema operativo subyacente. Esto impide que el atacante logre expandir el control más allá de los recursos que están asignados a la zona. Como consecuencia, finalmente resulta más difícil vulnerar el aislamiento del dominio invitado. Para obtener información sobre cómo proteger el SO huésped, consulte *Oracle Solaris 10 Security Guidelines* y *Oracle Solaris 11 Security Guidelines*.

♦ ♦ ♦ 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 del software 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 11. Una vez finalizada la instalación, debe disponer de privilegios de administrador para poder configurar los dominios con las funciones de derechos 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 3, “Setting Up Services and the Control Domain” de *Guía de administración de Oracle VM Server for SPARC 3.5*.
- Configure los dominios invitados. Consulte Capítulo 4, “Setting Up Guest Domains” de *Guía de administración de Oracle VM Server for SPARC 3.5*.

  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 “Contramedida: configuración de una red de gestión dedicada” [26].

  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 los derechos para limitar el acceso de conectividad de la consola *solo* 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 Oracle Integrated Lights Out Management (Oracle 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

Consideraciones de seguridad para desarrolladores

En este capítulo, se proporciona información 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 de lenguaje extensible de marcas (XML). El XML utiliza el protocolo extensible de mensajería y comunicación de presencia (XMPP). La interfaz XML solo admite el protocolo de seguridad de la capa de transporte (TLS) versión 1.2.

Un intruso puede intentar aprovechar este protocolo de red para acceder a un sistema, por lo que debe considerar la posibilidad de desactivar el XMPP. Para obtener información sobre cómo desactivar XMPP, consulte "XML Transport" de *Guía del desarrollador de Oracle VM Server for SPARC 3.5*. Para obtener información sobre los mecanismos de seguridad que utiliza Administrador de dominios lógicos, consulte "XMPP Server" de *Guía del desarrollador de Oracle VM Server for SPARC 3.5*.

La desactivación de XMPP impide que Oracle VM Manager u Ops Center gestionen el sistema e impide que use alguna función de Oracle VM Server for SPARC clave como uno de los siguientes comandos:

- `ldm migrate-domain`
- `ldm init-system`
- `ldm remove-core -g`
- `ldm add-memory`
- `ldm set-memory`
- `ldm remove-memory`
- `ldm grow-socket`
- `ldm shrink-socket`

- `ldm set-socket`
- `ldm list-socket`

♦ ♦ ♦ 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 para *Guía de administración de Oracle VM Server for SPARC 3.5*
- *Oracle Solaris 10 Security Guidelines*
- *Oracle Solaris 11 Security Guidelines*

Lista de comprobación de seguridad de Oracle VM Server for SPARC

- Lleve a cabo los pasos de protección de SO 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 derechos para restringir el acceso a la consola de los dominios a los que *solo usted*, como administrador de Oracle VM Server for SPARC, debe acceder.
- Desactive los servicios de administrador de dominios innecesarios.
- Solo implemente dominios invitados de la misma clase de seguridad en una plataforma física.
- Asegúrese de que no haya ninguna conexión de red entre la red de administración del entorno de ejecución y los dominios invitados.
- Solo asigne los recursos necesarios a los dominios invitados.