Sun Server X3-2L (anteriormente Sun Fire X4270 M3)

Guía de seguridad

Referencia: E36122-02
Septiembre de 2013

Tabla de contenidos

• • • Capítulo 1

Guía de seguridad del Sun Server X3-2L

En este documento se proporcionan directrices de seguridad generales para ayudarlo a proteger el Sun Server X3-2L de Oracle, sus interfaces de red y los conmutadores de red a los que se conecta.

Nota

El servidor Sun Server X3-2L antes se denominaba Sun Fire X4270 M3. Es posible que el nombre anterior siga apareciendo en el software. El nuevo nombre del producto no indica ningún cambio en las características ni en las funciones del sistema.

Este capítulo incluye las secciones siguientes:

Descripción general del sistema

El Sun Server X3-2L es un servidor de unidad de dos bastidores (2U) empresarial que admite uno o dos procesadores, dieciséis DIMM DDR3 (ocho por procesador), seis ranuras PCIe Gen3 y ocho, doce o veinticuatro unidades de almacenamiento SAS/SATA. El servidor incluye un procesador de servicio (SP) de Oracle Integrated Lights Out Manager (Oracle ILOM) incorporado. La herramienta de configuración de servidor Oracle System Assistant también está integrada en una unidad flash USB preinstalada como parte de la configuración del servidor.

Principios de seguridad

Hay cuatro principios de seguridad básicos: acceso, autenticación, autorización y contabilidad.

- **Acceso**

  El acceso se refiere al acceso físico al hardware, o al acceso físico o virtual al software.
  - Utilice los controles físicos y de software para proteger el hardware y los datos frente a posibles intrusiones.

- Consulte la documentación que se facilita con el software para activar cualquier función de seguridad disponible para el software.
- Instale servidores y equipos relacionados en una habitación cerrada con llave y de acceso restringido.
- Si el equipo se instala en un bastidor con una puerta con llave, mantenga la puerta cerrada a menos que sea necesario reparar algún componente del bastidor.
- Restrinja el acceso a conectores o puertos, que pueden proporcionar mayor acceso que las conexiones SSH. Los dispositivos como los controladores del sistema, las unidades de distribución de energía (PDU) y los conmutadores de red proporcionan conectores y puertos.
- Restrinja el acceso a los dispositivos de conexión directa o intercambio directo en especial, porque se pueden eliminar fácilmente.
- Almacene unidades sustituibles en campo (FRU) y unidades sustituibles por el cliente (CRU) de repuesto en un armario cerrado. Restrinja el acceso al armario cerrado al personal autorizado.

- **Autenticación**

  La autenticación se refiere a garantizar que los usuarios de hardware o software sean quienes dicen ser.
  - Configure las funciones de autenticación como un sistema de contraseña en sus sistemas operativos de plataforma para garantizar que los usuarios sean quienes dicen ser.
  - Asegúrese de que el personal use las credenciales de empleado correctamente para ingresar al cuarto de computación.
  - Para las cuentas de usuario: use listas de control de acceso cuando corresponda, establezca tiempos de espera para sesiones prolongadas y establezca niveles de privilegio para los usuarios.
- **Autorización**

  La autorización se refiere a las restricciones que se aplican al personal para trabajar con hardware o software.
  - Permita al personal trabajar únicamente con productos de hardware y software para los que estén capacitados y cualificados para utilizar.
  - Establezca un sistema de permisos de lectura, escritura y ejecución para controlar el acceso del usuario a los comandos, el espacio en el disco, los dispositivos y las aplicaciones.
- **Contabilidad**

  La contabilidad se refiere a las funciones de software y hardware que se utilizan para supervisar la actividad de inicio de sesión y el mantenimiento de los inventarios de hardware.
  - Use los registros del sistema para supervisar los inicios de sesión de los usuarios. Supervise las cuentas de servicio y administrador del sistema en particular, ya que estas cuentas pueden acceder a comandos importantes.
  - Mantenga un registro de los números de serie de todo el hardware. Use los números de serie de los componentes para realizar un seguimiento de los activos del sistema. Los números de pieza de Oracle se registran electrónicamente en tarjetas, módulos y placas base.
  - Para detectar los componentes y realizar un seguimiento de ellos, realice una marca de seguridad en todos los elementos de hardware del equipo que sean importantes, como las unidades sustituibles en campo. Utilice plumas ultravioleta o etiquetas en relieve especiales.

Uso de las herramientas de gestión y configuración del servidor

Cuando utilice las herramientas de software y firmware para configurar y gestionar el servidor, siga estas directrices de seguridad.

Seguridad de Oracle System Assistant

Oracle System Assistant es una herramienta preinstalada que lo ayuda a configurar y actualizar el hardware del servidor, y a instalar sistemas operativos compatibles, de manera local o remota. Para obtener información sobre cómo usar Oracle System Assistant, consulte la *Guía de administración del servidor Sun Server X3-2L* en:

http://www.oracle.com/pls/topic/lookup?ctx=SunServerX3-2L

La siguiente información lo ayudará a comprender los problemas de seguridad relacionados con Oracle System Assistant.

- **Oracle System Assistant incluye un entorno raíz de inicio**

Oracle System Assistant es una aplicación que se ejecuta en una unidad flash USB interna preinstalada. Está incorporada en un entorno raíz Linux de inicio. Oracle System Assistant también proporciona la capacidad de acceder a su shell raíz subyacente. Los usuarios que tienen acceso físico al sistema o que tienen acceso remoto de teclado, video, mouse y medios de almacenamiento (KVMS) al sistema mediante Oracle ILOM podrán acceder a Oracle System Assistant y al shell raíz.

Un entorno raíz se puede utilizar para cambiar las políticas y la configuración del sistema, y para acceder a los datos almacenados en otros discos. Se recomienda que el acceso físico al servidor sea seguro, y que los privilegios de administrador y consola para los usuarios de Oracle ILOM se asignen con moderación.

- **Oracle System Assistant monta un dispositivo de almacenamiento USB al que el sistema operativo puede acceder**

Además de ser un entorno de inicio, Oracle System Assistant también se monta como un dispositivo de almacenamiento USB (unidad flash) al que el sistema operativo puede acceder después de la instalación. Esto es útil cuando se accede a herramientas y controladores para el mantenimiento y la reconfiguración. El dispositivo de almacenamiento USB de Oracle System Assistant se puede leer y escribir, y podría ser utilizado por distintos virus.

Se recomienda aplicar al dispositivo de almacenamiento de Oracle System Assistant los mismos métodos utilizados para proteger discos, incluidos comprobaciones de integridad y análisis de virus regulares.

- **Oracle System Assistant se puede desactivar**

Oracle System Assistant es una herramienta útil para ayudarlo a configurar el servidor, actualizar y configurar firmware, e instalar el sistema operativo host. Sin embargo, si las implicancias de seguridad descritas anteriormente no son aceptables, o si la herramienta no es necesaria, Oracle System Assistant se puede desactivar. La desactivación de Oracle System Assistant implica que el sistema operativo host ya no podrá acceder al dispositivo de almacenamiento USB. Asimismo, no se podrá iniciar Oracle System Assistant.

Puede desactivar Oracle System Assistant desde la herramienta o desde BIOS. Una vez desactivada, la aplicación Oracle System Assistant sólo se puede volver a activar desde la utilidad de configuración de BIOS. Se recomienda que la configuración de BIOS esté protegida con contraseña, de manera que sólo los usuarios autorizados puedan volver a activar Oracle System Assistant. Para obtener información

sobre cómo desactivar y volver a activar Oracle System Assistant, consulte la *Guía de administración del servidor Sun Server X3-2L*.

Seguridad de Oracle ILOM

Puede proteger, gestionar y supervisar de manera activa los componentes del sistema mediante el firmware de gestión Oracle Integrated Lights Out Manager (Oracle ILOM), que viene preinstalado en el servidor Sun Server X3-2L, en otros servidores x86 de Oracle y en algunos servidores SPARC de Oracle.

Utilice una red dedicada para el procesador de servicio a fin de separarlo de la red general. Oracle ILOM proporciona funciones de control y supervisión de servidor para administradores del sistema. Según el nivel de autorización otorgado a los administradores, estas funciones pueden incluir la habilidad de apagar el servidor, crear cuentas de usuario, montar dispositivos de almacenamiento remoto, etc. Por lo tanto, para mantener un entorno confiable y seguro para Oracle ILOM, el puerto de gestión de red dedicado o el puerto de gestión de banda lateral en el servidor debe estar siempre conectado a un red interna de confianza o a una red privada o de gestión segura.

Limite el uso de la cuenta de administrador predeterminada (**`root`**) al inicio de sesión inicial de Oracle ILOM. Esta cuenta de administrador predeterminada se proporciona sólo para asistir con la instalación de servidor inicial. Por lo tanto, para garantizar el entorno más seguro, debe cambiar la contraseña de administrador predeterminada (**`changeme`**) en la configuración inicial del sistema. Además de cambiar la contraseña para la cuenta de administrador predeterminada, se deben establecer nuevas cuentas de usuario con contraseñas únicas y niveles de autorización asignados para cada usuario nuevo de Oracle ILOM.

Consulte la documentación de Oracle ILOM para obtener más información sobre la configuración de contraseñas, la gestión de usuarios y la aplicación de funciones relacionadas con la seguridad, incluidas la autenticación de RADIUS, Secure Socket Layer (SSL) y Secure Shell (SSH). Para obtener directrices de seguridad específicas de Oracle ILOM, consulte la *Guía de seguridad de Oracle Integrated Lights Out Manager (ILOM) 3.1*, que forma parte de biblioteca de documentación de Oracle ILOM 3.1. Puede encontrar la documentación de Oracle ILOM 3.1 en:

http://www.oracle.com/pls/topic/lookup?ctx=ilom31

Seguridad de Oracle Hardware Management Pack

Oracle Hardware Management Pack está disponible para su servidor, para muchos otros servidores x86 y para algunos servidores SPARC. Oracle Hardware Management Pack presenta dos componentes: un agente de supervisión SNMP y una familia de herramientas de interfaz de línea de comandos de todo el sistema operativo para gestionar el servidor.

Con los complementos SNMP del agente de gestión de hardware, puede usar SNMP para supervisar los servidores y los módulos de servidor de Oracle en el centro de datos sin necesidad de establecer conexión con dos puntos de gestión, el host y Oracle ILOM. Esta funcionalidad le permite usar una dirección IP única (la dirección IP del host) para supervisar varios servidores y módulos de servidor. Los complementos SNMP se ejecutan en el sistema operativo del host de los servidores de Oracle.

Puede usar las herramientas de interfaz de línea de comandos del servidor de Oracle para configurar servidores de Oracle. Las herramientas de la interfaz de línea de comandos funcionan con Oracle Solaris, Oracle Linux, Oracle VM, otras variantes de los sistemas operativos Linux y Microsoft Windows.

Para obtener más información sobre estas funciones, consulte la documentación de Oracle Hardware Management Pack. Para obtener directrices de seguridad específicas de Oracle Hardware Management

Pack, consulte la *Guía de seguridad de Oracle Hardware Management Pack (HMP)*, que forma parte de la biblioteca de documentación de Oracle Hardware Management Pack. Puede encontrar la documentación de Oracle Hardware Management Pack en:

http://www.oracle.com/pls/topic/lookup?ctx=ohmp

Planificación de un entorno seguro

Utilice la siguiente información para la instalación y configuración del servidor y el equipo relacionado.

Directrices del sistema operativo Oracle

Consulte los documentos del sistema operativo Oracle para obtener información sobre lo siguiente:

- Cómo utilizar las funciones de seguridad al configurar los sistemas
- Cómo trabajar de forma segura al agregar aplicaciones y usuarios a un sistema
- Cómo proteger las aplicaciones basadas en red

Los documentos de la guía de seguridad para los sistemas operativos Oracle compatibles forman parte de la biblioteca de documentación del sistema operativo. Para encontrar el documento de la guía de seguridad de un sistema operativo Oracle, vaya a la biblioteca de documentación del sistema operativo Oracle.

- **Oracle Solaris 10 1/13** - http://www.oracle.com/goto/Solaris10/docs
- **Oracle Solaris 11.1** - http://www.oracle.com/goto/Solaris11/docs
- **Oracle Linux** - http://www.oracle.com/technetwork/documentation/ol-1861776.html
- **Oracle VM** - http://www.oracle.com/technetwork/documentation/vm-096300.html

Para obtener información acerca de los sistemas operativos de otros proveedores, como Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Windows y VMware ESXi, consulte la documentación del proveedor.

Conmutadores y puertos de red

Diferentes conmutadores ofrecen diferentes niveles de funciones de seguridad para puertos. Consulte la documentación del conmutador para saber cómo hacer lo que se indica a continuación.

- Utilice las funciones de autenticación, autorización y contabilidad (AAA) para el acceso local y remoto al conmutador.
- Cambie todas las contraseñas de los conmutadores de la red que puedan tener múltiples contraseñas y cuentas de usuario predeterminadas.
- Gestione conmutadores fuera de banda (separados del tráfico de datos). Si la gestión fuera de banda no es factible, dedique un número de red de área local virtual (VLAN) aparte para la gestión en banda.

- Utilice la capacidad de reflejo de puertos del conmutador de red para el acceso del sistema de detección de intrusos (IDS).
- Mantenga un archivo de configuración del conmutador fuera de línea y limite el acceso sólo a administradores autorizados. El archivo de configuración debe contener comentarios descriptivos para cada opción.
- Implemente la seguridad de los puertos para limitar el acceso en función de las direcciones MAC. Desactive la función de enlace troncal automático en todos los puertos.
- Utilice estas funciones de seguridad para puertos si están disponibles en su conmutador:
  - **MAC Locking** (Bloqueo MAC): consiste en asociar una dirección MAC (Media Access Control) de uno o varios dispositivos conectados a un puerto físico en un conmutador. Si bloquea un puerto del conmutador a una dirección MAC en particular, los superusuarios no pueden crear las puertas traseras en su red con peligrosos puntos de acceso.
  - **MAC Lockout** (Cierre MAC): desactiva la conexión de una dirección MAC especificada a un conmutador.
  - **MAC Learning** (Aprendizaje MAC): utiliza el conocimiento sobre las conexiones directas de cada puerto del conmutador de manera que el conmutador de la red pueda definir la seguridad en función de las conexiones actuales.

Seguridad de una VLAN

Si configura una red de área local virtual (VLAN), recuerde que las VLAN comparten el ancho de banda de la red y requieren medidas de seguridad adicionales.

- Defina las redes VLAN como clústeres sensibles de sistemas aparte del resto de la red. De esta manera se reduce la probabilidad de que los usuarios tengan acceso a la información almacenada en estos clientes y servidores.
- Asigne un único número VLAN nativo a los puertos de tronco.
- Limite las redes VLAN que se puedan transportar sobre un tronco a sólo las que sean estrictamente necesarias.
- Desactive el protocolo de enlace troncal de VLAN (VTP), si es posible. De no ser así, configure los siguientes parámetros para el VTP: dominio de gestión, contraseña y eliminación. A continuación, defina VTP en modo transparente.

Seguridad de Infiniband

Mantenga los host Infiniband protegidos. Un tejido Infiniband sólo es tan seguro como su host Infiniband menos seguro.

- Tenga en cuenta que realizar una partición no protege un tejido Infiniband. La partición sólo ofrece aislamiento de tráfico Infiniband entre máquinas virtuales de un host.
- Utilice una configuración de VLAN estática, cuando sea posible.
- Desactive puertos de conmutador sin usar y asígneles un número de VLAN sin usar.

Seguridad física del hardware

El hardware físico se puede proteger de una manera bastante simple: mediante la limitación del acceso al hardware y el registro de los números de serie.

- **Restringir el acceso**
  - Instale servidores y equipos relacionados en una habitación cerrada con llave y de acceso restringido.

- Si el equipo se instala en un bastidor con una puerta con llave, mantenga la puerta cerrada a menos que sea necesario reparar algún componente del bastidor. Después de trabajar con los equipos, cierre la puerta.
- Restrinja el acceso a las conexiones USB, que pueden proporcionar mayor acceso que las conexiones SSH. Los dispositivos, como los controladores del sistema, las unidades de distribución de energía (PDU) y los conmutadores de red pueden tener conexiones USB.
- Restrinja el acceso a los dispositivos de conexión directa o intercambio directo en especial, porque se pueden eliminar fácilmente.
- Almacene las unidades sustituibles en campo (FRU) o las unidades sustituibles por el cliente (CRU) de repuesto en un armario cerrado. Restrinja el acceso al armario cerrado al personal autorizado.

- **Registro de los números de serie**
  - Realice una marca de seguridad en todos los elementos importantes del hardware del equipo, como las unidades sustituibles en campo. Utilice plumas ultravioleta o etiquetas en relieve especiales.
  - Mantenga un registro de los números de serie de todo el hardware.
  - Mantenga las licencias y las claves de activación de hardware en una ubicación segura y de fácil acceso para el administrador del sistema en caso de emergencia del sistema. Los documentos impresos podrían ser su única prueba para demostrar la propiedad.

Seguridad de software

La mayoría de las medidas de protección del hardware se implementan a través de medidas de software.

- Cuando instale un sistema nuevo, cambie todas las contraseñas predeterminadas. La mayoría de los tipos de equipos utilizan contraseñas predeterminadas, como **changeme**, que son muy conocidas y, por lo tanto, permiten el acceso no autorizado al equipo.
- Cambie todas las contraseñas de los conmutadores de la red que puedan tener múltiples contraseñas y cuentas de usuario predeterminadas.
- Limite el uso de la cuenta de administrador predeterminada (**root**) a un solo usuario administrador. Siempre cree una nueva cuenta de Oracle ILOM para cada usuario nuevo. Asegúrese de que siempre se asignen una contraseña única y privilegios de nivel de autorización adecuados (operador, administrador, etc.) a cada nueva cuenta de usuario de Oracle ILOM.
- Utilice una red dedicada de procesadores de servicio para separarlos de la red general.
- Proteja el acceso a conexiones USB. Los dispositivos, como las controladoras del sistema, las unidades de distribución de alimentación (PDU) y los conmutadores de red, pueden tener conexiones USB, que pueden proporcionar mayor acceso que las conexiones SSH.
- Consulte la documentación que se facilita con el software para activar cualquier función de seguridad disponible para el software.
- Implemente la seguridad de los puertos para limitar el acceso basándose en las direcciones MAC. Desactive la función de enlace troncal automático en todos los puertos.

Mantenimiento de un entorno seguro

Después de la instalación y configuración inicial, utilice las funciones de seguridad del hardware y software de Oracle para seguir controlando el hardware y realizando el seguimiento de los activos del sistema.

- “Control de energía de hardware” [12]

Control de energía de hardware

Puede usar software para encender y apagar algunos sistemas de Oracle. Las unidades de distribución de energía (PDU) de algunos armarios de sistemas pueden activarse y desactivarse de manera remota. La autorización para estos comandos se suele configurar durante la configuración del sistema y normalmente está limitada a los administradores del sistema y al personal de mantenimiento. Consulte la documentación de su sistema o armario para obtener más información.

Seguimiento de activos

Utilice los números de serie para realizar un seguimiento del inventario. Oracle incrusta números de serie en el firmware en tarjetas opcionales y placas base del sistema. Puede leer estos números de serie mediante conexiones de red de área local.

También puede utilizar lectores de identificación de frecuencia de radio (RFID) para simplificar aún más el seguimiento de activos. Las notas del producto de Oracle, *Cómo realizar un seguimiento de sus activos del sistema Oracle Sun mediante RFID*, están disponibles en:

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

Actualizaciones para software y firmware

Mantenga sus versiones de software y firmware actualizadas en el equipo de servidor.

- Busque actualizaciones con regularidad.
- Instale siempre la versión publicada más reciente del software o el firmware.
- Instale los parches de seguridad necesarios para el software.
- Recuerde que los dispositivos como los conmutadores de red también contienen firmware y pueden requerir parches y actualizaciones de firmware.

Acceso de red

Siga estas directrices para garantizar el acceso local y remoto a los sistemas.

- Limite la configuración remota a direcciones IP específicas mediante SSH en lugar de Telnet. Telnet acepta nombres de usuario y contraseñas en texto no cifrado y, como consecuencia, permite potencialmente que todos los miembros del segmento LAN vean las credenciales de inicio de sesión. Defina una contraseña segura para SSH.
- Utilice la versión 3 del protocolo simple de gestión de redes (SNMP) para proporcionar transmisiones seguras. Las primeras versiones de SNMP no son seguras y transmiten datos de autenticación en texto no cifrado.
- Si SNMP es necesario, cambie la cadena de comunidad SNMP predeterminada por una cadena de comunidad segura. Algunos productos tienen el valor PUBLIC establecido como cadena de comunidad SNMP predeterminada. Los atacantes pueden pedir a una comunidad que realice un

mapa de red muy completo y, posiblemente, que modifiquen los valores de bases de datos de información de gestión (MIB).

- Siempre cierre sesión después de usar el controlador del sistema, si este utiliza una interfaz de explorador.
- Desactive los servicios de red no necesarios, como el protocolo de control de transmisión (TCP) o el protocolo de transferencia de hipertexto (HTTP). Active servicios de red necesarios y configure estos servicios de manera segura.
- Siga las medidas de seguridad LDAP al utilizar LDAP para acceder al sistema. Consulte la *Guía de seguridad de Oracle ILOM* en: http://www.oracle.com/goto/ILOM/docs.
- Cree un rótulo para mencionar que el acceso no autorizado está prohibido.
- Utilice las listas de control de acceso donde corresponda.
- Defina tiempos de espera para las sesiones ampliadas y defina los niveles de privilegios.
- Utilice las funciones de autenticación, autorización y contabilidad (AAA) para el acceso local y remoto a un conmutador.
- Si es posible, utilice los protocolos de seguridad de RADIUS y TACACS+:
  - RADIUS (Remote Authentication Dial in User Service) es un protocolo cliente/servidor que protege redes frente a accesos no autorizados.
  - TACACS+ (Terminal Access Controller Access-Control System) es un protocolo que permite a un servidor de acceso remoto comunicarse con un servidor de autentificación para determinar si un usuario tiene acceso a la red.
- Utilice la capacidad de duplicación de puertos del conmutador para el acceso del sistema de detección de intrusos (IDS).
- Implemente la seguridad de los puertos para limitar el acceso basándose en una dirección MAC. Deshabilite la función de enlace troncal automático en todos los puertos.

Protección de datos

Siga estas directrices para maximizar la seguridad y la protección de los datos.

- Realice una copia de seguridad de datos importantes mediante dispositivos como discos duros externos o dispositivos de almacenamiento USB. Almacene los datos copiados en una segunda ubicación segura fuera del sitio.
- Utilice software de cifrado de datos para guardar de manera segura información confidencial en discos duros.
- Para deshacerse de una unidad de disco duro vieja, destruya físicamente la unidad o borre por completo todos los datos almacenados en la unidad. Después de que se suprimen los archivos o se reformatea la unidad, la información aún se puede recuperar a partir de una unidad. Al suprimir los archivos o reformatear la unidad, se eliminan solamente las tablas de direcciones de la unidad. Utilice software de borrado del disco duro para borrar por completo todos los datos en una unidad.

Mantenimiento de registro

Inspeccione y mantenga sus archivos de registro regularmente. Utilice estos métodos para proteger los archivos de registro.

- Active la generación de registros y envíe registros del sistema a un host de registro dedicado seguro.
- Configure la generación de registros para que se incluya la información de tiempo precisa mediante NTP y registros de hora.
- Revise registros para detectar posibles incidentes y archivarlos de acuerdo con una política de seguridad.

- Periódicamente, retire los archivos de registro cuando superen un tamaño razonable. Mantenga copias de los archivos retirados para utilizarlos en el futuro para referencia o análisis estadístico.