Sistema SuperCluster

Guía de seguridad

Referencia: E48459-01
Julio de 2013

Tabla de contenidos

• • • Capítulo 1

Guía de seguridad del sistema SuperCluster

Este documento proporciona directrices de seguridad generales para ayudarlo a proteger los productos de hardware de Oracle, como servidores, conmutadores de red, tarjetas de interfaz de red, etc.

Este capítulo incluye las secciones siguientes:

Descripción de los principios de seguridad

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

- Acceso

  Los controles físicos y de software son necesarios para proteger el hardware y sus datos frente a posibles intrusiones.
  - En el caso del hardware, los límites de acceso suelen ser límites de acceso *físicos*.
  - En el caso del software, el acceso está limitado por medios físicos y virtuales.
  - El firmware no se puede cambiar, excepto por medio del proceso de actualización de Oracle.
- Autenticación

  Todos los sistemas operativos de la plataforma proporcionan funciones de autenticación que pueden configurarse para garantizar que los usuarios son quienes dicen ser.

  La autenticación proporciona diversos grados de seguridad mediante medidas como el uso de insignias y contraseñas.
- Autorización

  La autorización permite a los trabajadores de la empresa que trabajen únicamente con hardware y software que estén capacitados y cualificados para utilizar. Para este fin, los administradores del sistema crean sistemas 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

  Las funciones de software y de hardware de Oracle permiten que el servicio informático supervise la actividad de conexión y que mantenga los inventarios de hardware.

  - Las conexiones de usuario se pueden supervisar mediante los registros del sistema. El administrador del sistema y las cuentas de servicio en concreto tienen acceso a comandos importantes y deben ser supervisados cuidadosamente mediante los registros del sistema. Normalmente los registros se mantienen durante un largo período de tiempo, por lo que es esencial retirar periódicamente los archivos de registro cuando excedan un tamaño razonable, de acuerdo con la política de la empresa del cliente.
  - Generalmente se realiza un seguimiento de los activos del cliente de TI mediante números de serie. Los números de referencia de Oracle se registran electrónicamente en todas las tarjetas, módulos y placas base, y pueden utilizarse para efectos de inventario.

Planificación de un entorno seguro

Utilice las siguientes notas antes de la instalación y la configuración de un servidor y equipos relacionados, o después de ellas.

Seguridad de 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.

- Para 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, cierre siempre la puerta hasta que se tenga que reparar algún componente de dentro del bastidor.
  - Los dispositivos de conexión directa o intercambio directo se extraen fácilmente y requieren sobre todo una accesibilidad restringida.
  - 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.
- Para registrar 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 se instala un sistema nuevo, cambie todas las contraseñas predeterminadas. La mayoría de los equipos utilizan contraseñas predeterminadas, como **changeme**, que son muy conocidas y, por lo tanto, pueden permitir el acceso no autorizado al equipo. Además, los dispositivos como los

conmutadores de red pueden tener varias cuentas de usuario de manera predeterminada. Asegúrese de cambiar todas las contraseñas de cuentas.

- Limite el uso de la cuenta de superusuario `root`. Las cuentas de Oracle Integrated Lights Out Manager (Oracle ILOM), como `ilom-operator` e `ilom-admin`, deben utilizarse en lugar de la cuenta de superusuario siempre que sea posible.
- Utilice una red dedicada de procesadores de servicio para separarlos de la red general.
- Durante el proceso de instalación de Oracle Solaris, se le solicitará que cree una cuenta y una contraseña de usuario, así como una contraseña **root** para el sistema. Como parte del proceso, debe asumir la función de usuario **root**. Si desea cambiar la configuración de esta cuenta, puede eliminar la cuenta de usuario **root** y traspasar la función raíz a un usuario con menos privilegios.
- Proteja el acceso a consolas USB. Los dispositivos, como los controladores del sistema, las unidades de distribución de alimentación (PDU) y los conmutadores de red, pueden tener conexiones USB, 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.
- Un servidor se puede iniciar de forma segura con inicio WAN o inicio iSCSI. Para obtener más información, consulte la *Guía de instalación de Oracle Solaris: instalaciones basadas en red*, correspondiente a su versión de Oracle Solaris.

En el documento Oracle Solaris Security Guidelines se proporciona información sobre:

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

Los documentos de directrices de seguridad de Oracle Solaris se pueden encontrar aquí:

- http://www.oracle.com/technetwork/indexes/documentation/index.html#sys_sw

Seguridad de firmware

Las cuentas de usuario normales no pueden editar OpenBoot PROM (OBP) u otro firmware de Oracle. El sistema operativo Oracle Solaris utiliza un proceso de actualización de firmware controlado para impedir modificaciones del firmware no autorizadas. Sólo el superusuario puede utilizar el proceso de actualización.

Para obtener información sobre la configuración de las variables de seguridad de OBP, consulte el *Manual de referencia de comandos de OpenBoot 4.x* en:

- http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069

Firmware de Oracle ILOM

Oracle Integrated Lights Out Manager (Oracle ILOM) es un firmware de gestión de sistemas que se entrega preinstalado en algunos servidores SPARC. Oracle ILOM permite gestionar y supervisar de forma activa los componentes instalados en el sistema. La forma en que se usa Oracle ILOM afecta la seguridad del sistema. Para obtener más información sobre el uso de este firmware al configurar contraseñas, gestionar usuarios y aplicar funciones relacionadas con la seguridad, incluidos el shell seguro (SSH), la capa de conexión segura (SSL) y la autenticación RADIUS, consulte la documentación de Oracle ILOM:

- http://www.oracle.com/pls/topic/lookup?ctx=E19860-01

Mantenimiento de un entorno seguro

El hardware y el software de Oracle proporcionan un número de funciones de seguridad que supervisan los activos de seguimiento y hardware.

Controles de hardware

Algunos sistemas de Oracle se pueden configurar para ser activados y desactivados por comandos de software. Además, las unidades de distribución de energía (PDU) de algunos armarios de sistemas se pueden activar y desactivar de forma remota mediante comandos de software. 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

Los números de serie de Oracle están incrustados en firmware ubicado en tarjetas opcionales y placas bases del sistema. Estos números de serie se pueden leer mediante conexiones de red de área local para el seguimiento del inventario.

Los lectores inalámbricos de identificación por radiofrecuencia (RFID) pueden simplificar aún más el seguimiento de activos. Las notas del producto de Oracle, *Cómo realizar un seguimiento de los activos del sistema Oracle Sun mediante RFID*, están disponibles en:

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

Software y firmware

- Instale siempre la versión publicada más reciente del software o el firmware en su equipo. Los dispositivos como los conmutadores de red contienen firmware y pueden requerir parches y actualizaciones de firmware.
- Instale los parches de seguridad necesarios para el software.

Acceso local y remoto

Siga estas directrices para garantizar la seguridad del acceso local y remoto a los sistemas:

- 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 (servicio de autenticación remota telefónica de usuario) es un protocolo cliente/servidor que protege redes frente a accesos no autorizados.
  - TACACS+ (sistema de control de acceso mediante controlador de acceso desde terminales) 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 reflejo 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. Desactive la función de enlace troncal automático en todos los puertos.
- 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.
- Una vez terminada la configuración de su sistema SuperCluster el instalador deshabilitará todas las claves SSH y también caducará todas las contraseñas como una medida de seguridad para el sistema. Si no desea que se desactiven las claves SSH o que caduquen las contraseñas, póngase en contacto con el instalador al final de la instalación de sistema SuperCluster.
- Las primeras versiones de SNMP no son seguras y transmiten datos de autenticación en texto no cifrado. Sólo la versión 3 de SNMP puede proporcionar transmisiones seguras.
- Algunos productos se entregan con PUBLIC definido 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 administración (MIB). Si SNMP es necesario, cambie la cadena de comunidad SNMP predeterminada a una cadena de comunidad segura.
- Active el registro y envíe los registros a un host de registro dedicado seguro.
- Configure el registro para incluir información de tiempo precisa mediante NTP y registros de hora.
- Revise registros para detectar posibles incidentes y archivarlos de acuerdo con la política de seguridad.
- Si el controlador del sistema utiliza una interfaz de explorador, asegúrese de cerrar sesión después de utilizarla.

Seguridad de datos

Siga estas directrices para optimizar la seguridad de los datos:

- Realice una copia de seguridad de datos importantes mediante dispositivos, como discos duros externos, pen drives o memorias extraíbles. 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. La supresión de todos los archivos o el cambio de formato de la unidad eliminará únicamente las tablas de direcciones en la unidad: la información puede recuperarse de una unidad tras borrar archivos o cambiar el formato de la unidad. (Utilice software de borrado del disco duro para borrar por completo todos los datos en una unidad).

Seguridad de red

Siga estas directrices para optimizar la seguridad de red:

- La mayoría de los conmutadores permiten definir las redes de área local virtual (VLAN). Si utiliza su conmutador para definir redes VLAN, separe los clusters sensibles de sistemas 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.
- Gestione conmutadores fuera de banda (separados del tráfico de datos). Si la gestión fuera de banda no es factible, dedique un número VLAN independiente de gestión en banda.

- 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.
- 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.
- Utilice una configuración de VLAN estática, cuando sea posible.
- Desactive puertos de conmutador sin usar y asígneles un número de VLAN sin usar.
- 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.
- Desactive los servicios de red innecesarios, como servidores pequeños TCP o HTTP. Active servicios de red necesarios y configure estos servicios de manera segura.
- Diferentes conmutadores ofrecerán diferentes niveles de funciones de seguridad para puertos. Utilice estas funciones de seguridad para puertos si están disponibles en el conmutador:
  - MAC Locking (bloqueo MAC): consiste en atar una dirección MAC (Media Access Control) de uno o más 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 la información sobre las conexiones directas de cada puerto del conmutador, por lo que el conmutador puede definir la seguridad basándose en las conexiones actuales.

Guías de seguridad relacionadas

Los componentes de software y hardware utilizados en sistema SuperCluster también pueden tener guías de seguridad específicas del producto. A continuación, se muestra una lista de componentes utilizados en sistema SuperCluster y dónde se pueden encontrar, si las hay, las guías de seguridad específicas del producto para dichos componentes:

- Servidor SPARC T4-4:

  http://www.oracle.com/pls/topic/lookup?ctx=E23411_01
- Servidor SPARC T5-8:

  http://www.oracle.com/pls/topic/lookup?ctx=E35078_01
- Dispositivo Sun ZFS Storage 7320:

  http://www.oracle.com/pls/topic/lookup?ctx=ZFS_Storage_7x20_2011.1
- Conmutador Sun Datacenter InfiniBand Switch 36:

  http://www.oracle.com/pls/topic/lookup?ctx=E19197-01
- Servidor de almacenamiento Exadata: Documentación instalada en el directorio en el servidor de almacenamiento Exadata **/opt/oracle/cell/doc**

- Sistema operativo Oracle Solaris:

  http://www.oracle.com/technetwork/documentation/index.html#sys_sw