Guía de seguridad de Oracle® Hardware Management Pack para Oracle Solaris 11.2

Referencia: E56556-02
Septiembre de 2015

Referencia: E56556-02

Accesibilidad a la documentación

Para obtener información acerca del compromiso de Oracle con la accesibilidad, visite el sitio web del Programa de Accesibilidad de Oracle en `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Acceso a Oracle Support

Los clientes de Oracle que hayan adquirido servicios de soporte disponen de acceso a soporte electrónico a través de My Oracle Support. Para obtener información, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` o `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si tiene problemas de audición.

Contenido

Descripción general del producto y de la seguridad de las aplicaciones

En esta sección, se ofrece una descripción general del producto Oracle Hardware Management Pack (HMP) para Oracle Solaris y de la seguridad básica de las aplicaciones.

Se tratan los temas siguientes:

Acerca de Oracle Hardware Management Pack para Oracle Solaris

Oracle Hardware Management Pack para Oracle Solaris está disponible para varios servidores Oracle x86 y para algunos servidores basados en SPARC. Oracle Hardware Management Pack cuenta con dos componentes: un agente de supervisión SNMP y una familia de herramientas de la interfaz de la línea de comandos para gestionar los servidores.

Con los plugins SNMP del agente de gestión de hardware, puede usar SNMP para supervisar los servidores Oracle y los módulos de los servidores desde el centro de datos con la ventaja de no tener que conectarse 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 plugins SNMP del agente de gestión de hardware se ejecutan en el sistema operativo host de los servidores Oracle. Los plugins SNMP utilizan las bibliotecas de acceso de almacenamiento de hardware de Oracle para comunicarse con el procesador de servicio. El agente de gestión de hardware recupera automáticamente la información sobre el estado actual del servidor. Para obtener más información sobre el agente de gestión de hardware, consulte la *Guía del usuario de los agentes de gestión de Oracle Server*.

Puede usar las herramientas de la CLI del servidor Oracle para configurar servidores Oracle. Para obtener una lista de herramientas, consulte la *Guía del usuario de las herramientas de CLI de Oracle Server.*

Para obtener más información sobre las funciones y el uso, consulte la documentación de Oracle Hardware Management Pack para Oracle Solaris.

- Biblioteca de documentación de Oracle Hardware Management Pack para Oracle Solaris disponible en: http://www.oracle.com/goto/ohmp/solarisdocs
- Para obtener información general de Oracle ILOM, consulte: http://www.oracle.com/goto/ilom/docs

Principios básicos de seguridad

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

- Acceso

  Utilice los controles físicos y de software para proteger el hardware o los datos frente a posibles intrusiones.

  - En hardware, los límites de acceso se consideran límites de acceso físicos.
  - En 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

  Configure las funciones de autenticación como un sistema de contraseña en sus sistemas operativos de plataforma para verificar que los usuarios sean quienes dicen ser.

  La autenticación proporciona diversos grados de seguridad por medio de ciertas medidas, como el uso de insignias y contraseñas. Por ejemplo, asegúrese de que el personal use las credenciales de empleado correctamente para ingresar al cuarto de computación.
- Autorización

  La autorización permite que los trabajadores de la empresa trabajen únicamente con hardware y software que estén capacitados y cualificados para utilizar.

  Por ejemplo, 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.
- Control

  El personal de TI del cliente puede usar las funciones de software y de hardware de Oracle para supervisar la actividad de conexión y mantener los inventarios de hardware.

  - Use los logs del sistema para supervisar el inicio de sesión de los usuarios. En particular, lleve un registro de las cuentas de servicio y administrador del sistema mediante los logs del sistema, ya que estas cuentas pueden acceder a comandos importantes.
  - De manera periódica, retire los archivos log cuando excedan un tamaño razonable, de acuerdo con la política de la empresa del cliente. Normalmente los logs se mantienen durante un largo período, por lo que es esencial mantenerlos.

- Use los números de serie de los componentes para llevar un registro de los activos del sistema con fines de inventario. Todas las tarjetas, los módulos y las placas base tienen números de referencia de Oracle registrados de manera electrónica.

Resumen de seguridad de Oracle Hardware Management Pack

A continuación, se mencionan elementos importantes de seguridad que hay que tener en cuenta en el momento de configurar todas las herramientas de gestión del sistema:

- *Los productos de gestión del sistema pueden usarse para obtener un entorno raíz de inicio.*

  Con un entorno raíz de inicio, puede obtener acceso a Oracle ILOM, a Oracle System Assistant y a discos duros.
- *Los productos de gestión del sistema incluyen potentes herramientas que requieren privilegios de usuario root o administrador para ejecutarlas.*

  Con este nivel de acceso, es posible cambiar la configuración de hardware y borrar datos.

Seguridad de Oracle Hardware Management Pack

Para Oracle Solaris, los componentes de Oracle Hardware Management Pack usados con más frecuencia vienen preinstalados. A fin de garantizar la seguridad, quizá se requieran valores de configuración adicionales.

Interfaz de interconexión de host a ILOM

La interfaz de interconexión de host a ILOM permite a los clientes del sistema operativo host comunicarse con Oracle ILOM por medio de una interconexión interna de alta velocidad. Esta interconexión es implementada por una conexión interna de Ethernet por USB ejecutando una pila de IP. Se asignan direcciones IP no enrutables internas a Oracle ILOM y al host para que se comuniquen mediante este canal. Esta conexión se activa de forma predeterminada en el sistema operativo Oracle Solaris.

La conexión a Oracle ILOM mediante la interconexión de host a ILOM requiere autenticación, como si la conexión fuese por la red hacia el puerto de gestión de Oracle ILOM. Todos los servicios o protocolos expuestos en la red de gestión están disponibles mediante la interconexión LAN para el host. Por ejemplo, es posible utilizar un explorador web en el host para acceder a la interfaz web de Oracle ILOM o utilizar un cliente de shell seguro para conectarse a la interfaz de la línea de comandos de Oracle ILOM. En todos los casos, se deben proporcionar una contraseña y un nombre de usuario válidos para utilizar la interconexión LAN.

Oracle recomienda que la red admita RFC 3927 y la capacidad para tener direcciones IPv4 local de vínculo. Además, se deben tomar medidas para garantizar que el sistema operativo no actúe como puente o enrutador. Así se garantiza que el tráfico de gestión entre el host y Oracle ILOM mediante la interconexión de host a ILOM se mantenga privado.

- Biblioteca de documentación de Oracle Hardware Management Pack para Oracle Solaris: `http://www.oracle.com/goto/ohmp/solarisdocs`

Decisión de guardar credenciales en un archivo

A partir de Oracle Solaris 11.2 con SRU 14, esta función está desactivada.

Las herramientas `ilomconfig` y `fwupdate` que son parte de Oracle Hardware Management Pack para Oracle Solaris pueden conectarse a Oracle ILOM mediante la interconexión de host a ILOM de alta velocidad. Como la interconexión de host a ILOM requiere autenticación, es necesario realizar la autenticación en Oracle ILOM cada vez que se invocan estas herramientas. Si resulta conveniente, se pueden almacenar en caché las credenciales de un archivo para que las herramientas puedan usarlas de manera automática. De este modo se evita la necesidad de incorporar contraseñas de texto no cifrado en secuencias de comandos que utilicen herramientas de Oracle Hardware Management Pack.

La herramienta `ilomconfig` puede usarse para almacenar el nombre de usuario y la contraseña en un archivo cifrado que sea de solo lectura root. Si se detecta este archivo cuando se utiliza `ilomconfig` o `fwupdate` para acceder a Oracle ILOM, se usan las credenciales almacenadas en caché. De manera alternativa, se puede especificar el nombre de usuario y la contraseña en la línea de comandos para cada invocación de la herramienta.

El algoritmo de cifrado que se usa es único para cada sistema. Sin embargo, si se descubre la clave, el archivo podría ser descifrado, y el nombre de usuario y la contraseña quedarían expuestos.

A tal fin, Oracle recomienda crear una contraseña exclusiva para cada Oracle ILOM, de modo que la contraseña expuesta no se pueda usar en otros sistemas Oracle ILOM.

Consulte la *Guía de usuario de las herramientas de la CLI de Oracle para Oracle Solaris* para obtener instrucciones sobre cómo guardar credenciales en un archivo.

- Biblioteca de documentación de Oracle Hardware Management Pack para Oracle Solaris: `http://www.oracle.com/goto/ohmp/solarisdocs`

Elección de opciones de configuración de seguridad de SNMP

Oracle Hardware Management Pack contiene un módulo de plugins SNMP que extiende el agente SNMP nativo en el sistema operativo host a fin de proporcionar capacidades adicionales de Oracle MIB. Es de vital importancia destacar que Oracle Hardware Management Pack no contiene un agente SNMP por sí solo. Para el sistema operativo Oracle Solaris, se agrega un módulo al agente de gestión de Solaris.

Asimismo, se determina cualquier configuración de seguridad en relación con SNMP para el plugin SNMP de Oracle Hardware Management Pack mediante la configuración de un servicio

o agente SNMP, no por el plugin. Entre las opciones de configuración de SNMP, se incluyen las siguientes:

- SNMPv1/v2c. Esta versión no ofrece cifrado y utilizan cadenas de comunidad como modo de autenticación. Las cadenas comunitarias se envían en texto no cifrado por la red y, generalmente, se comparten entre un grupo de personas, en lugar de pertenecer exclusivamente a un usuario particular.
- SNMPv3. Esta versión utiliza el cifrado para proporcionar un canal seguro y tiene contraseñas y nombres de usuario individuales. Las contraseñas de usuarios de SNMPv3 están localizadas, por lo que se pueden almacenar de manera segura en estaciones de gestión.

Oracle recomienda que se use SNMPv3 si el agente SNMP nativo lo admite. Consulte la documentación de Oracle Solaris para obtener instrucciones sobre cómo configurar net-snmp para SNMPv3.

Instalación o desinstalación de componentes de Oracle Hardware Management Pack

Se tratan los temas siguientes:

Instalación de componentes

Oracle Hardware Management Pack para Oracle Solaris está formado por un conjunto de herramientas que vienen preinstaladas. Se pueden instalar paquetes de componentes adicionales de Oracle Hardware Management Pack que no vienen preinstalados mediante Image Packaging System (IPS) de Oracle Solaris.

Solo un administrador con privilegios de usuario root puede instalar paquetes de Oracle Hardware Management Pack.

- Biblioteca de documentación de Oracle Hardware Management Pack para Oracle Solaris: `http://www.oracle.com/goto/ohmp/solarisdocs`

Desinstalación de componentes

Los paquetes de Oracle Hardware Management Pack para Oracle Solaris pueden desinstalarse mediante el comando `pkg uninstall`.

Nota - Cuando se desinstalan paquetes, si anteriormente ha guardado un archivo de caché de credenciales del host mediante el comando `ilomconfig` de Oracle Hardware Management Pack para facilitar el acceso a Oracle ILOM mediante la interconexión de host a ILOM, no se suprimirá el archivo. En este caso, antes de desinstalar los paquetes de Oracle Hardware Management Pack, ejecute el comando `ilomconfig delete credential` para suprimir este archivo.

- Biblioteca de documentación de Oracle Hardware Management Pack para Oracle Solaris disponible en: `http://www.oracle.com/goto/ohmp/solarisdocs`