Guía de seguridad de Oracle® Hardware Management Pack

Referencia: E39908-02
Octubre de 2015

Referencia: E39908-02

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

En esta sección, se proporciona una visión general del producto Oracle Hardware Management Pack, se incluye información de la guía de seguridad y se explican los principios generales de la seguridad de las aplicaciones.

Se tratan los temas siguientes:

Descripción general del producto

Oracle Hardware Management Pack está disponible para varios servidores basados en x86 y algunos servidores basados en SPARC. Oracle Hardware Management Pack cuenta con 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 los servidores.

Con los plugins SNMP del agente de gestión de hardware, puede usar SNMP para supervisar los servidores de 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 Hardware Management Agent, consulte la *Guía del usuario de Oracle Server Management Agents*.

Puede usar Oracle Server CLI Tools para configurar servidores Oracle. CLI Tools funciona con Oracle Solaris, Oracle Linux, Oracle VM, otras variantes de Linux y sistemas operativos

Windows. Para obtener una lista de herramientas, consulte la *Guía del usuario de Oracle® Server CLI Tools*.

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 en: `http://www.oracle.com/goto/ohmp/docs`
- Para obtener información general de Oracle ILOM, consulte: `http://www.oracle.com/goto/ilom/docs`

Acerca de esta Guía de seguridad

En este documento, se proporcionan directrices generales de seguridad para Oracle Hardware Management Pack. Esta guía tiene por objetivo ayudarle a garantizar la seguridad en el uso del software con otros productos de hardware de Oracle, como conmutadores de red y tarjetas de interfaz de red.

Se tratan los temas siguientes:

- Preinstalación de Oracle Hardware Management Pack [11]
- Instalación de Oracle Hardware Management Pack [13]
- Postinstalación de Oracle Hardware Management Pack [17]

Principios básicos de seguridad

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

- 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 a través 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. Lleve un registro de las cuentas de servicio y administrador del sistema en particular, 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 registros 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. Los números de pieza de Oracle se registran electrónicamente en todas las tarjetas, módulos y placas base.

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 configuraciones de hardware y borrar datos.

Preinstalación de Oracle Hardware Management Pack

Durante la instalación y configuración inicial, utilice las funciones de seguridad del software de Oracle para seguir controlando el hardware y llevar un registro de los activos del sistema.

Se tratan los temas siguientes:

Componentes de Oracle Hardware Management Pack

Oracle Hardware Management Pack contiene una colección de herramientas de línea de comandos de gestión de hardware para configurar la RAID, el BIOS y Oracle ILOM, y para actualizar firmware. También contiene un plugin SNMP para supervisión. Oracle Hardware Management Pack también contiene un daemon o servicio que se comunica con Oracle ILOM mediante un canal interno para compartir inventarios e información del estado del servidor.

Estos plugins y herramientas se instalan en el sistema operativo host para que pueda realizar tareas de gestión de sistema directamente desde el host. Aunque Oracle Hardware Management Pack proporciona funciones útiles para gestionar un servidor de Oracle, esto es completamente opcional.

Para obtener información acerca de las funcionalidades de Oracle Hardware Management Pack, consulte las siguientes bibliotecas de documentos:

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/goto/ohmp/docs`)
- Biblioteca de documentación de Oracle ILOM (`http://www.oracle.com/goto/ilom/docs`)

Configuración de seguridad de plugin SNMP según el agente

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 Linux, se agrega un módulo al agente net-snmp, que debe instalarse previamente. Para Solaris, se agrega un módulo al agente de gestión de Solaris. Para Windows, el plugin se extiende al servicio SNMP nativo.

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. Consulte la documentación de net-snmp o el servicio SNMP de Windows para obtener instrucciones sobre cómo configurar el SNMP de manera segura. Consulte también las instrucciones de la *Guía del usuario de Oracle Server Management Agents* en el siguiente enlace:

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/goto/ohmp/docs`)

Selección de una versión de protocolo SNMP del agente SNMP

SNMP es un protocolo estándar utilizado para supervisar o gestionar un sistema. SNMPv1 y SNMPv2c no proporcionan 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. En cambio, SNMPv3 utiliza el cifrado para proporcionar un canal seguro y tiene contraseñas y nombres de usuarios 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 net-snmp (Oracle Solaris y Linux) o el servicio SNMP de Windows para obtener instrucciones sobre cómo configurar SNMPv3.

Instalación de Oracle Hardware Management Pack

Se tratan los temas siguientes:

Ejecución del instalador de Oracle Hardware Management Pack

Oracle Hardware Management Pack está conformado por un conjunto de paquetes de instalación nativa que pueden ejecutarse mediante las herramientas de instalación nativa de un sistema operativo, como RPM. Además, se puede usar un instalador basado en asistente como ayuda en la instalación. Además de agregar los paquetes nativos, el instalador también ayuda a configurar Oracle Hardware Management Pack para usarlo.

Como el instalador de Oracle Hardware Management Pack debe instalar paquetes nativos, debe ejecutarse como usuario root o administrador. Para obtener más información, consulte la *Guía de instalación de Oracle Hardware Management Pack* en el siguiente enlace:

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/goto/ohmp/docs`)

Cómo elegir la activación de la interconexión de host a ILOM

Como una alternativa más rápida a la interfaz KCS, los clientes del sistema operativo host se pueden comunicar con Oracle ILOM mediante una interconexión interna de alta velocidad.

En Oracle Hardware Management Pack, esta función se denomina "Interconexión de host a ILOM". La interfaz de Oracle ILOM hace referencia a esta función como "interconexión de host local". 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.

La conexión a Oracle ILOM mediante la interconexión de host a ILOM (interconexión de host local) 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 de host a ILOM 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 debe proporcionar un nombre de usuario y una contraseña válidos para utilizar la interconexión de host a ILOM.

En el instalador de Oracle Hardware Management Pack se incluye la opción de activar la interconexión de host a ILOM. Oracle recomienda que la interconexión de host a ILOM se active solamente si la instrucción de redes admite RFC 3927 y la capacidad de tener direcciones IPv4 locales de enlace. 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 se mantenga en estado privado. Para obtener más información, consulte la *Guía de instalación de Oracle Hardware Management Pack* en el siguiente enlace:

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/goto/ohmp/docs`)

Decisión de guardar credenciales en un archivo

A partir de Oracle Hardware Management Pack 2.3.3, esta función está desactivada.

Las herramientas `ilomconfig` y `fwupdate` que son parte de Oracle Hardware Management Pack for 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 el archivo cuando se usa `ilomconfig` o `fwupdate` para acceder a Oracle ILOM, se utilizan 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 exclusivo 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 del usuario de Oracle CLI Tools para Oracle Solaris* en el siguiente enlace.

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/goto/ohmp/docs`)

Postinstalación de Oracle Hardware Management Pack

Se tratan los temas siguientes:

Desinstalación de Oracle Hardware Management Pack

Los paquetes de Oracle Hardware Management Pack se pueden desinstalar mediante las herramientas nativas de los paquetes, como RPM, o mediante el desinstalador basado en asistente que viene con Oracle Hardware Management Pack. Cuando se usa el método lo paquetes nativos para eliminar paquetes, si anteriormente a guardado un archivo de caché de credenciales del host en 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.

El desinstalador basado en asistente elimina el archivo de credenciales. Por lo tanto, Oracle recomienda usar el desinstalador basado en asistente para desinstalar Oracle Hardware Management Pack. Para obtener más información, consulte la *Guía de instalación de Oracle Hardware Management Pack* en el siguiente enlace:

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/goto/ohmp/docs`)