Oracle Hardware Management Pack Security Guide

Part No: E27799
April 2012

ORACLE

140528@25097

Contents

Overview

This section provides an overview of the Oracle Hardware Management Pack (HMP) product, including security guide information, and explains the general principles of application security.

The following topics are covered:

Product Overview

Oracle Hardware Management Pack is available for your server, and for many other x86- based servers and some SPARC-based servers. Oracle Hardware Management Pack features two components: an SNMP monitoring agent and a family of cross-operating system command-line interface tools (CLI Tools) for managing your servers.

With the Hardware Management Agent SNMP Plugins, you can use SNMP to monitor Oracle servers and server modules in your data center with the advantage of not having to connect to two management points, the host and Oracle ILOM. This functionality enables you to use a single IP address (the host's IP) to monitor multiple servers and server modules.

Hardware Management Agent SNMP Plugins run on the host operating system of Oracle servers. The SNMP Plugins use the Oracle Hardware Storage Access Libraries to communicate with the service processor. Information about the current state of the server is fetched automatically by the Hardware Management Agent.

You can use the Oracle Server CLI Tools to configure Oracle servers. The CLI Tools work with Oracle Solaris, Oracle Linux, Oracle VM, other variants of Linux, and Windows operating systems. The following table describes the tasks that you can perform using the CLI Tools.

System Management Task From Host OS	CLI Tool
Configure BIOS settings, device boot order, and some service processor settings.	`ubiosconfig` `biosconfig`

System Management Task From Host OS	CLI Tool
Update Oracle ILOM and BIOS.	`fwupdate`
Query, update, and validate firmware versions on supported SAS storage devices, embedded SAS storage controllers, SAS storage expanders, and storage drives.	
Restore, set, and view Oracle ILOM configuration settings, as well as viewing and setting Oracle ILOM properties that are associated with network management, clock configuration, and user management.	`ilomconfig`
View or create RAID volumes on storage drives that are attached to RAID controllers, including storage arrays.	`raidconfig`
Monitor system health.	`hwmgmt`

About This Security Guide

This document provides general security guidelines for the Oracle Hardware Management Pack. This guide is intended to help you ensure security when using the software with other Oracle hardware products such as network switches and network interface cards.

The following topics are covered:

Basic Security Principles

There are four basic security principles: access, authentication, authorization, and accounting.

- Access

  Use physical and software controls to protect your hardware or data from intrusion.

  - For hardware, access limits usually mean physical access limits.
  - For software, access limits usually mean both physical and virtual means.
  - Firmware cannot be changed except through the Oracle update process.

- Authentication

  Set up all authentication features such as a password system in your platform operating systems to verify that users are who they say they are.

  Authentication provides varying degrees of security through measures such as badges and passwords. For example, ensure that personnel use employee badges properly to enter a computer room.

- Authorization

  Authorization allows company personnel to work only with hardware and software that they are trained and qualified to use.

  For example, set up a system of read/write/execute permissions to control user access to commands, disk space, devices, and applications.

- Accounting

  Customer IT personnel can use Oracle software and hardware features to monitor login activity and maintain hardware inventories.

  - Use system logs to monitor user logins. In particular, track system administrator and service accounts through system logs because these accounts can access powerful commands.
  - Periodically retire log files when they exceed a reasonable size, in accordance with the customer company policy. Logs are typically maintained for a long period, so it is essential to maintain them.
  - Use component serial numbers to track system assets for inventory purposes. Oracle part numbers are electronically recorded on all cards, modules, and motherboards.

Oracle Hardware Management Pack Security Summary

Important security items to remember when configuring all system management tools are:

- *System management products can be used to obtain a bootable root environment.*

  With a bootable root environment, you can obtain Oracle ILOM access, Oracle System Assistant access, and hard disk access.

- *System management products include powerful tools that require administrator or root privileges to run.*

  With this level of access, it is possible to change hardware configuration and erase data.

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Oracle Hardware Management Pack Preinstall

During the initial installation and setup, use Oracle software security features to control hardware and track system assets.

The following topics are covered:

Oracle Hardware Management Pack Components

Oracle Hardware Management Pack contains a collection of hardware management command-line tools for configuring RAID, BIOS, and Oracle ILOM and for updating firmware. It also contains an SNMP Plugin for monitoring. Oracle Hardware Management Pack also contains a daemon or service that communicates with Oracle ILOM over an internal channel to share inventory and health information about the server.

These tools and plugins are installed on your host operating system so you can perform system management tasks directly from the host. While the Oracle Hardware Management Pack provides useful features for managing an Oracle server, it is completely optional.

See the Sun Server Hardware Management Pack User's Guide for more information about Oracle Hardware Management Pack capabilities to help determine whether to use and install it.

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)
- For general Oracle ILOM information refer to: `http://www.oracle.com/pls/topic/lookup?ctx=ilom31`

SNMP Plugin Security Settings Based on Agent

Oracle Hardware Management Pack contains an SNMP Plugin module that extends the native SNMP agent in the host operating system to provide additional Oracle MIB capabilities. It is particularly important to note that the Oracle Hardware Management Pack does not itself contain an SNMP agent. For Linux, a module is added to the net-snmp agent, which must be previously installed. For Solaris, a module is added to the Solaris Management Agent. For Windows, the plugin extends the native SNMP service.

Likewise, any security settings related to SNMP for the Oracle Hardware Management Pack SNMP Plugin are determined by the settings of the native SNMP agent or service, and not by the plugin. See the documentation for net-snmp or the Windows SNMP service for instructions on how to configure SNMP securely.

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Choosing an SNMP Protocol Version of the SNMP Agent

SNMP is a standard protocol used to monitor or manage a system. SNMPv1/v2c provides no encryption and uses community strings as a form of authentication. Community strings are sent in cleartext over the network and are usually shared across a group of individuals, rather than being private to an individual user. SNMPv3, on the other hand, uses encryption to provide a secure channel and has individual user names and passwords. SNMPv3 user passwords are localized so that they can be stored securely on management stations.

Oracle recommends that SNMPv3 be used if supported by the native SNMP agent. See the documentation for net-snmp or the Windows SNMP service for instructions on how to configure SNMPv3.

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Oracle Hardware Management Pack Install

The following topics are covered:

Running the Oracle Hardware Management Pack Installer

The Oracle Hardware Management Pack consists of a set of native install packages that can be installed using the native install tools for an operating system, such as RPM. In addition, a wizard-based installer can be used to assist with the installation. In addition to adding the native packages, the installer also helps configure the Oracle Hardware Management Pack for use.

Because the Oracle Hardware Management Pack installer must install native packages, it must be run as root or administrator.

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Choosing to Enable the LAN Interconnect

As a faster alternative to the KCS interface, clients on the host operating system can communicate with Oracle ILOM over an internal high-speed interconnect. This interconnect is implemented by an internal Ethernet-over-USB connection, running an IP stack. Oracle ILOM and the host are given internal non-routable IP addresses for communication over this channel.

Connecting to Oracle ILOM over the LAN interconnect requires authentication, just as if the connection were coming over the network to the Oracle ILOM management port. All services or protocols exposed on the management network are made available over the LAN interconnect to the host. For example, it is possible to use a web browser on the host to access Oracle ILOM's web interface or use a Secure Shell client to connect to Oracle ILOM CLI. In all cases, a valid user name and password must be provided to use the LAN interconnect.

The Oracle Hardware Management Pack installer presents the option of enabling the LAN interconnect. Oracle recommends that the LAN interconnect be enabled only if the networking

instruction supports RFC 3927 and the ability to have link-local IPv4 addresses. Also, care should be taken to ensure that the operating system is not acting as a bridge or router. This ensures that management traffic between the host and Oracle ILOM remains private.

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Choosing to Save Credentials in a File

The ilomconfig and fwupdate tools that are part of the Oracle Hardware Management Pack can connect to Oracle ILOM using the high-speed LAN interconnect. Using the LAN interconnect instead of the slower KCS interface can dramatically improve performance of key operations, such as Oracle ILOM firmware updates.

Because the LAN interconnect requires authentication, it is necessary to authenticate to Oracle ILOM for each invocation of these tools. As a convenience, it is possible to cache the credentials in a file so that the tools can use them automatically. This prevents having to embed cleartext passwords in scripts that use the Oracle Hardware Management Pack tools.

The ilomconfig tool can be used to store the user name and password in an encrypted file that is root read-only. If this file is detected when ilomconfig or fwupdate is used to access Oracle ILOM, the cached credentials are used. Alternatively, the user name and password can be specified on the command line for each invocation of the tool.

The encryption algorithm that is used is unique to each system. If the key is discovered, however, the file could be decrypted and expose the user name and password. Oracle recommends that a unique password be created on each Oracle ILOM for this purpose such that a compromised password could not be used against other Oracle ILOM systems.

See the Sun Server Hardware Management Pack User's Guide for instructions on how to save credentials in a file.

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Oracle Hardware Management Pack Post Install

The following topics are covered:

Uninstall of Oracle Hardware Management Pack

The Oracle Hardware Management Pack packages can be uninstalled using native package tools, such as RPM, or using the wizard-based uninstaller that comes with the Oracle Hardware Management Pack. When the native package method is used to remove packages, the encrypted file that stores the cached user name and password for using over the LAN interconnected will not be deleted. This must be manually deleted.

The wizard-based uninstaller removes the credentials file. Therefore, Oracle recommends that the wizard-based installer be used to uninstall Oracle Hardware Management Pack.

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)