Oracle® Hardware Management Pack for Oracle Solaris 11.2 Security Guide

Part No: E52962-05
September 2015

ORACLE

Part No: E52962-05

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Référence: E52962-05

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Accès au support électronique

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Product and Application Security Overview

This section provides an overview of the Oracle Hardware Management Pack (HMP) for Oracle Solaris product and basic application security.

The following topics are covered:

About Oracle Hardware Management Pack for Oracle Solaris

Oracle Hardware Management Pack for Oracle Solaris is available for many Oracle x86- based servers and some SPARC-based servers. Oracle Hardware Management Pack features two components: an SNMP monitoring agent and a family of 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. For more information on the Hardware Management Agent, refer to the *Oracle Server Management Agents User's Guide.*.

You can use the Oracle Server CLI Tools to configure Oracle servers. For a list of tools, refer to the *Oracle Server CLI Tools User's Guide.*

See the Oracle Hardware Management Pack for Oracle Solaris documentation for more information about capabilities and usage.

- Oracle Hardware Management Pack for Oracle Solaris Documentation Library at: `http://www.oracle.com/goto/ohmp/solarisdocs`

- For general Oracle ILOM information refer to: http://www.oracle.com/goto/ilom/docs

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.

Securing Oracle Hardware Management Pack

For Oracle Solaris, the most frequently used Oracle Hardware Management Pack components come preinstalled. To help ensure security, additional configuration might be required.

The Host-to-ILOM Interconnect Interface

The Host-to-ILOM Interconnect interface allows clients on the host operating system to 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. This connection is enabled by default in Oracle Solaris operating system.

Connecting to Oracle ILOM over the Host-to-ILOM 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.

Oracle recommends that your network support 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 over the Host-to-ILOM interconnect remains private.

- Oracle Hardware Management Pack for Oracle Solaris Documentation Library: `http://www.oracle.com/goto/ohmp/solarisdocs`

Choosing to Save Credentials in a File

As of Oracle Solaris 11.2 SRU 14, this feature has been disabled.

The `ilomconfig` and `fwupdate` tools that are part of the Oracle Hardware Management Pack for Oracle Solaris can connect to Oracle ILOM using the high-speed Host-to-ILOM Interconnect. Because the Host-to-ILOM 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 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 so that a compromised password could not be used against other Oracle ILOM systems.

See the *Oracle CLI Tools for Oracle Solaris User's Guide* for instructions on how to save credentials in a file.

- Oracle Hardware Management Pack for Oracle Solaris Documentation Library: `http://www.oracle.com/goto/ohmp/solarisdocs`

Choosing SNMP Security Settings

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 Oracle Solaris operating system, a module is added to the Solaris Management Agent.

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. SNMP settings might include:

- SNMPv1/v2c. This version 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. This version 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 your Oracle Solaris documentation for instructions on configuring net-snmp for SNMPv3.

Installing or Uninstalling Oracle Hardware Management Pack Components

The following topics are covered:

Installing Components

The Oracle Hardware Management Pack for Oracle Solaris consists of a set of tools that come preinstalled. Additional Oracle Hardware Management Pack component packages that do not come preinstalled can be installed using the Oracle Solaris Image Packaging System (IPS).

Only an administrator with root privileges can install Oracle Hardware Management Pack packages.

- Oracle Hardware Management Pack for Oracle Solaris Documentation Library: `http://www.oracle.com/goto/ohmp/solarisdocs`

Uninstalling Components

The Oracle Hardware Management Pack for Oracle Solaris packages can be uninstalled using the Oracle Solaris `pkg uninstall` command.

Note - When uninstalling packages, if you have previously saved a host credentials cache file using the Oracle Hardware Management Pack `ilomconfig` command to facilitate accessing Oracle ILOM using the Host-to-ILOM interconnect, the file will not be deleted. In this case, before uninstalling Oracle Hardware Management Pack packages, run the `ilomconfig delete credential` command to delete this file.

- Oracle Hardware Management Pack for Oracle Solaris Documentation Library at: `http://www.oracle.com/goto/ohmp/solarisdocs`