Oracle® Hardware Management Pack for Oracle Solaris 11.2 安全指南

文件号码 E56552-02
2015 年 9 月

ORACLE

文件号码 E56552-02

文档可访问性

有关 Oracle 对可访问性的承诺，请访问 Oracle Accessibility Program 网站 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc。

获得 Oracle 支持

购买了支持服务的 Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如果您听力受损，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

目录

产品和应用程序安全性概述

本部分概述了 Oracle Hardware Management Pack (HMP) for Oracle Solaris 产品和基本应用程序安全性。

其中包含以下主题：

关于 Oracle Hardware Management Pack for Oracle Solaris

Oracle Hardware Management Pack for Oracle Solaris 可供许多 Oracle 基于 x86 的服务器和部分基于 SPARC 的服务器使用。Oracle Hardware Management Pack 采用两种组件（即 SNMP 监视代理和一系列命令行界面工具 (CLI Tools)）来管理您的服务器。

通过 Hardware Management Agent SNMP Plugins，您可以使用 SNMP 来监视数据中心中的 Oracle 服务器和服务器模块，其优点是不必连接到两个管理点，即主机和 Oracle ILOM。通过此功能，可以使用单个 IP 地址（主机的 IP）来监视多个服务器和服务器模块。

Hardware Management Agent SNMP Plugins 运行在 Oracle 服务器的主机操作系统上。SNMP Plugins 使用 Oracle Hardware Storage Access Libraries 与服务处理器进行通信。Hardware Management Agent 会自动获取有关服务器当前状态的信息。有关 Hardware Management Agent 的更多信息，请参阅《*Oracle Server Management Agents* 用户指南》。

您可以使用 Oracle Server CLI Tools 来配置 Oracle 服务器。有关工具列表，请参阅《*Oracle Server CLI Tools* 用户指南》。

有关功能和用法的更多信息，请参见 Oracle Hardware Management Pack for Oracle Solaris 文档。

- Oracle Hardware Management Pack for Oracle Solaris 文档库，网址为：`http://www.oracle.com/goto/ohmp/solarisdocs`
- 有关 Oracle ILOM 的一般信息，请参阅：`http://www.oracle.com/goto/ilom/docs`

基本安全原则

有四个基本安全原则：访问、验证、授权和记帐。

- 访问

  使用物理和软件控制措施来保护硬件或数据免遭入侵。

  - 对于硬件，访问限制通常是指物理访问限制。
  - 对于软件，访问限制通常是指物理和虚拟两种方式。
  - 除非通过 Oracle 更新过程，否则无法更改固件。
- 验证

  在平台操作系统中设置所有验证功能（如密码系统）以检验用户是否与其表明的身份相符。

  验证通过诸如胸卡和密码之类的措施提供不同程度的安全性。例如，确保人员正确使用员工胸卡进入计算机室。
- 授权

  授权使公司职员只能使用他们经过培训并有资格使用的硬件和软件。

  例如，建立一套读/写/执行权限的系统，以控制用户对命令、磁盘空间、设备和应用程序的访问。
- 记帐

  客户 IT 人员可以使用 Oracle 的软件和硬件功能监视登录活动并维护硬件清单。

  - 使用系统日志来监视用户登录。尤其要通过系统日志跟踪系统管理员和服务帐户，因为这些帐户可以访问功能强大的命令。
  - 根据客户公司政策，定期弃用超过合理大小的日志文件。日志通常会保留较长时间，因此妥善维护它们非常重要。
  - 使用组件序列号来跟踪系统资产以便进行盘点。在所有插卡、模块和主板上以电子方式记录了 Oracle 部件号。

Oracle Hardware Management Pack 安全性摘要

配置所有系统管理工具时要记住的重要安全事项包括：

- 系统管理产品可用于获取可引导的根环境。

  通过可引导的根环境，您可以获取对 Oracle ILOM、Oracle System Assistant 和硬盘的访问权限。
- 系统管理产品包含功能强大的工具，要求具有管理员或 *root* 特权才能运行。

  通过此访问级别，可以更改硬件配置和删除数据。

保护 Oracle Hardware Management Pack

对于 Oracle Solaris，将会预先安装最常用的 Oracle Hardware Management Pack 组件。为帮助确保安全性，可能需要其他配置。

主机到 ILOM 互连接口

通过主机到 ILOM 互连接口，主机操作系统上的客户机可以通过内部高速互连与 Oracle ILOM 进行通信。此互连通过内部 Ethernet-over-USB 连接实现，并且运行 IP 堆栈。Oracle ILOM 和主机是用于通过此通道通信的给定内部非可路由 IP 地址。在 Oracle Solaris 操作系统中，默认情况下会启用此连接。

通过主机到 ILOM 互连连接到 Oracle ILOM 需要验证，就像通过网络连接到 Oracle ILOM 管理端口一样。主机可通过 LAN 互连使用在管理网络上公开的所有服务或协议。例如，可以使用主机上的 Web 浏览器访问 Oracle ILOM Web 界面或使用安全 Shell 客户机连接到 Oracle ILOM CLI。在任何情况下，必须提供有效的用户名和密码才能使用 LAN 互连。

Oracle 建议您的网络支持 RFC 3927 并且可以具有 IPv4 链路本地地址。此外，应当小心谨慎以确保操作系统未在充当网桥或路由器。这可确保主机和 Oracle ILOM 之间通过主机到 ILOM 互连的管理通信保持私密。

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

选择在文件中保存凭证

从 *Oracle Solaris 11.2 SRU 14* 开始，此功能已被禁用。

属于 Oracle Hardware Management Pack for Oracle Solaris 一部分的 `ilomconfig` 和 `fwupdate` 工具可以使用高速主机到 ILOM 互连来连接到 Oracle ILOM。由于主机到

ILOM 互连要求验证，因此每次调用这些工具时都需要向 Oracle ILOM 进行验证。为方便起见，可以将凭证缓存在一个文件中，以便工具可以自动使用它们。这样就可以不必在使用 Oracle Hardware Management Pack 工具的脚本中嵌入明文密码。

`ilomconfig` 工具可用于在 root 只读的加密文件中存储用户名和密码。如果在使用 `ilomconfig` 或 `fwupdate` 访问 Oracle ILOM 时检测到此文件，将使用缓存的凭证。或者，可以在每次调用该工具时在命令行上指定用户名和密码。

使用的加密算法对于每个系统都是唯一的。但是，如果密钥被搜索到，文件可能会被解密并公开用户名和密码。

Oracle 建议在每个 Oracle ILOM 上创建唯一的密码，以便无法在其他 Oracle ILOM 系统上使用泄漏的密码。

有关如何在文件中保存凭证的说明，请参见《Oracle CLI Tools for Oracle Solaris 用户指南》。

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

选择 SNMP 安全设置

Oracle Hardware Management Pack 包含一个 SNMP Plugin 模块，可在主机操作系统中扩展本机 SNMP 代理，以提供其他 Oracle MIB 功能。尤其重要的是要注意，Oracle Hardware Management Pack 本身并不包含 SNMP 代理。对于 Oracle Solaris 操作系统，向 Solaris Management Agent 添加一个模块。

同样，与 Oracle Hardware Management Pack SNMP Plugin 的 SNMP 相关的任何安全性设置均由本机 SNMP 代理或服务的设置（而不是代理）来决定。SNMP 设置可能包括：

- SNMPv1/v2c。此版本不提供加密，并且使用团体字符串 (community string) 作为验证形式。团体字符串通过网络以明文形式发送，并且通常在一组用户之间共享，而不是供单个用户专用。
- SNMPv3。此版本使用加密提供安全的通道，并且具有单独的用户名和密码。SNMPv3 用户密码已本地化，以便可以安全地存储在管理站上。

Oracle 建议使用 SNMPv3（如果本机 SNMP 代理支持）。有关为 SNMPv3 配置 net-snmp 的说明，请参见 Oracle Solaris 文档。

安装或卸载 Oracle Hardware Management Pack 组件

其中包含以下主题：

安装组件

Oracle Hardware Management Pack for Oracle Solaris 包含一组预先安装的工具。未预先安装的其他 Oracle Hardware Management Pack 组件软件包可以使用 Oracle Solaris 映像包管理系统 (Image Packaging System, IPS) 进行安装。

仅具有 root 特权的管理员可以安装 Oracle Hardware Management Pack 软件包。

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

卸载组件

可以使用 Oracle Solaris `pkg uninstall` 命令卸载 Oracle Hardware Management Pack for Oracle Solaris。

注 - 卸载软件包时，如果之前为了便于使用主机到 ILOM 互连访问 Oracle ILOM，已经使用 Oracle Hardware Management Pack `ilomconfig` 命令保存了主机凭证高速缓存文件，则不会删除该文件。这种情况下，在卸载 Oracle Hardware Management Pack 软件包之前，请先运行 `ilomconfig delete credential` 命令来删除该文件。

- Oracle Hardware Management Pack for Oracle Solaris 文档库，网址为：`http://www.oracle.com/goto/ohmp/solarisdocs`