

Oracle® Hardware Management Pack 安全 指南

ORACLE®

文件号码 E39912-02
2015 年 10 月

文件号码 E39912-02

版权所有 © 2014, 2015, Oracle 和/或其附属公司。保留所有权利。

本软件和相关文档是根据许可证协议提供的，该许可证协议中规定了关于使用和公开本软件和相关文档的各种限制，并受知识产权法的保护。除非在许可证协议中明确许可或适用法律明确授权，否则不得以任何形式、任何方式使用、拷贝、复制、翻译、广播、修改、授权、传播、分发、展示、执行、发布或显示本软件和相关文档的任何部分。除非法律要求实现互操作，否则严禁对本软件进行逆向工程设计、反汇编或反编译。

此文档所含信息可能随时被修改，恕不另行通知，我们不保证该信息没有错误。如果贵方发现任何问题，请书面通知我们。

如果将本软件或相关文档交付给美国政府，或者交付给以美国政府名义获得许可证的任何机构，则适用以下注意事项：

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

本软件或硬件是为了在各种信息管理应用领域内的一般使用而开发的。它不应被应用于任何存在危险或潜在危险的应用领域，也不是为此而开发的，其中包括可能会产生人身伤害的应用领域。如果在危险应用领域内使用本软件或硬件，贵方应负责采取所有适当的防范措施，包括备份、冗余和其它确保安全使用本软件或硬件的措施。对于因在危险应用领域内使用本软件或硬件所造成的一切损失或损害，Oracle Corporation 及其附属公司概不负责。

Oracle 和 Java 是 Oracle 和/或其附属公司的注册商标。其他名称可能是各自所有者的商标。

Intel 和 Intel Xeon 是 Intel Corporation 的商标或注册商标。所有 SPARC 商标均是 SPARC International, Inc 的商标或注册商标，并应按照许可证的规定使用。AMD、Opteron、AMD 徽标以及 AMD Opteron 徽标是 Advanced Micro Devices 的商标或注册商标。UNIX 是 The Open Group 的注册商标。

本软件或硬件以及文档可能提供了访问第三方内容、产品和服务的方式或有关这些内容、产品和服务的信息。除非您与 Oracle 签订的相应协议另行规定，否则对于第三方内容、产品和服务，Oracle Corporation 及其附属公司明确表示不承担任何种类的保证，亦不对其承担任何责任。除非您和 Oracle 签订的相应协议另行规定，否则对于因访问或使用第三方内容、产品或服务所造成的任何损失、成本或损害，Oracle Corporation 及其附属公司概不负责。

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

概述	7
产品概述	7
关于本安全指南	8
基本安全原则	8
Oracle Hardware Management Pack 安全性摘要	9
Oracle Hardware Management Pack 安装前	11
Oracle Hardware Management Pack 组件	11
基于代理的 SNMP Plugin 安全性设置	11
选择 SNMP 代理的 SNMP 协议版本	12
Oracle Hardware Management Pack 安装	13
运行 Oracle Hardware Management Pack 安装程序	13
选择启用主机到 ILOM 互连	13
选择在文件中保存凭证	14
Oracle Hardware Management Pack 安装后	15
卸载 Oracle Hardware Management Pack	15

概述

本部分概述了 Oracle Hardware Management Pack 产品（包括安全指南信息），并介绍了应用程序安全性的一般原则。

其中包括以下主题：

- “产品概述” [7]
- “关于本安全指南” [8]
- “基本安全原则” [8]
- “Oracle Hardware Management Pack 安全性摘要” [9]

产品概述

Oracle Hardware Management Pack 可供许多基于 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 监视代理和一系列跨操作系统的命令行界面工具 (CLI Tools)）来管理服务器。

使用 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。CLI Tools 适用于 Oracle Solaris、Oracle Linux、Oracle VM、其他 Linux 变体和 Windows 操作系统。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 文档库，网址为：<http://www.oracle.com/goto/ohmp/docs>

- 有关 Oracle ILOM 的一般信息，请参阅：<http://www.oracle.com/goto/ilom/docs>

关于本安全指南

本文档提供了有关 Oracle Hardware Management Pack 的一般安全准则。本指南的目的在于帮助您在对其他 Oracle 硬件产品（例如网络交换机和网络接口卡）使用该软件时确保安全性。

其中包括以下主题：

- [Oracle Hardware Management Pack 安装前 \[11\]](#)
- [Oracle Hardware Management Pack 安装 \[13\]](#)
- [Oracle Hardware Management Pack 安装后 \[15\]](#)

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。
 - 除非执行 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。

Oracle Hardware Management Pack 安装前

初始安装和设置期间，可以使用 Oracle 软件安全功能来控制硬件和跟踪系统资产。

其中包括以下主题：

- “Oracle Hardware Management Pack 组件” [11]
- “基于代理的 SNMP Plugin 安全性设置” [11]
- “选择 SNMP 代理的 SNMP 协议版本” [12]

Oracle Hardware Management Pack 组件

Oracle Hardware Management Pack 包含一组硬件管理命令行工具，用于配置 RAID、BIOS 和 Oracle ILOM 以及更新固件。它还包含一个 SNMP Plugin 用于进行监视。Oracle Hardware Management Pack 还包含一个用于通过内部通道与 Oracle ILOM 通信的守护进程或服务，以共享有关服务器的清单和运行状况信息。

这些工具和插件安装在您的主机操作系统上，以便您可以直接从主机执行系统管理任务。虽然 Oracle Hardware Management Pack 可提供用于管理 Oracle 服务器的有用功能，但完全是可选的。

有关 Oracle Hardware Management Pack 功能的更多信息，请参见以下文档库：

- Oracle Hardware Management Pack 文档库 (<http://www.oracle.com/goto/ohmp/docs>)
- Oracle ILOM 文档库 (<http://www.oracle.com/goto/ilom/docs>)

基于代理的 SNMP Plugin 安全性设置

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 Linux，将模块添加到 net-snmp 代理（之前必须安装该代理）。对于 Solaris，将模块添加到 Solaris Management Agent。对于 Windows，插件扩展本机 SNMP 服务。

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。有关如何安全地配置 SNMP 的说明，请参见 net-snmp 或 Windows SNMP 服务的文档。另请参见以下链接中《Oracle Server Management Agents 用户指南》中的说明：

- Oracle Hardware Management Pack 文档库 (<http://www.oracle.com/goto/ohmp/docs>)

选择 SNMP 代理的 SNMP 协议版本

SNMP 是用于监视或管理系统的标准协议。SNMPv1/v2c 不提供加密，并且使用团体字符串作为验证形式。团体字符串通过网络以明文形式发送，并且通常在的一组用户之间共享，而不是供单个用户专用。与之相反，SNMPv3 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）。有关如何配置 SNMPv3 的说明，请参见 net-snmp（Oracle Solaris 和 Linux）或 Windows SNMP 服务的文档。

Oracle Hardware Management Pack 安装

其中包括以下主题：

- “运行 Oracle Hardware Management Pack 安装程序” [13]
- “选择启用主机到 ILOM 互连” [13]
- “选择在文件中保存凭证” [14]

运行 Oracle Hardware Management Pack 安装程序

Oracle Hardware Management Pack 包含一组本机安装软件包，可以使用操作系统的本机安装工具（例如 RPM）来安装这些软件包。此外，基于向导的安装程序可用于协助进行安装。除了添加本机软件包，安装程序还可帮助配置 Oracle Hardware Management Pack 以供使用。

由于 Oracle Hardware Management Pack 安装程序必须安装本机软件包，因此必须以 root 或管理员身份运行。有关更多信息，请参见以下链接中的《Oracle Hardware Management Pack 安装指南》：

- Oracle Hardware Management Pack 文档库 (<http://www.oracle.com/goto/ohmp/docs>)

选择启用主机到 ILOM 互连

作为 KCS 接口的速度更快的替代连接，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。Oracle Hardware Management Pack 将此功能称为“主机到 ILOM 互连”。Oracle ILOM 界面将此功能称为“本地主机互连”。此互连通过内部 Ethernet-over-USB 连接实施，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。

通过主机到 ILOM 互连（本地主机互连）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。主机可通过主机到 ILOM 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主机到 ILOM 互连。

Oracle Hardware Management Pack 安装程序提供了启用主机到 ILOM 互连的选项。Oracle 建议，仅当联网指令支持 RFC 3927 并能够使用链路本地 IPv4 地址时才启用主机到 ILOM 互连。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 之间的管理通信保持私密。有关更多信息，请参见以下链接中的《Oracle Hardware Management Pack 安装指南》：

- Oracle Hardware Management Pack 文档库 (<http://www.oracle.com/goto/ohmp/docs>)

选择在文件中保存凭证

自 *Oracle Hardware Management Pack 2.3.3* 起，已禁用此功能。

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，从而无法在其他 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，请参见以下链接中的《Oracle CLI Tools for Oracle Solaris 用户指南》。

- Oracle Hardware Management Pack 文档库 (<http://www.oracle.com/goto/ohmp/docs>)

Oracle Hardware Management Pack 安装后

其中包括以下主题：

- “[卸载 Oracle Hardware Management Pack](#)” [15]

卸载 Oracle Hardware Management Pack

可以使用本机软件包工具（例如 RPM）或使用 Oracle Hardware Management Pack 附带的基于向导的卸载程序来卸载 Oracle Hardware Management Pack 软件包。使用本机软件包方法删除软件包时，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 保存了主机凭证高速缓存文件，将不删除该文件。这种情况下，在卸载 Oracle Hardware Management Pack 软件包之前，请先运行 `ilomconfig delete credential` 命令删除此文件。

基于向导的卸载程序会删除凭证文件。因此，Oracle 建议使用基于向导的安装程序卸载 Oracle Hardware Management Pack。有关更多信息，请参见以下链接中的《*Oracle Hardware Management Pack 安装指南*》：

- [Oracle Hardware Management Pack 文档库 \(http://www.oracle.com/goto/ohmp/docs\)](http://www.oracle.com/goto/ohmp/docs)

