Oracle® Key Manager 3

安全指南

发行版 3.1

E52204-02

2016 年 4 月

ORACLE®

Oracle® Key Manager 3
安全指南

E52204-02

版权所有 © 2007, 2016, 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。

目录

表格清单

前言

本文档介绍了 Oracle Key Manager 3 (OKM 3) 的安全功能。

目标读者

本指南的目标读者是要使用 OKM 3 的安全功能以及要安全可靠地安装和配置 OKM 3 的所有人。

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。

1

第 1 章 概述

本部分对产品进行了概述，并说明了应用程序安全的一般原则。

1.1. 产品概述

Oracle Key Manager (OKM) 可以创建、存储和管理加密密钥。它由以下组件构成：

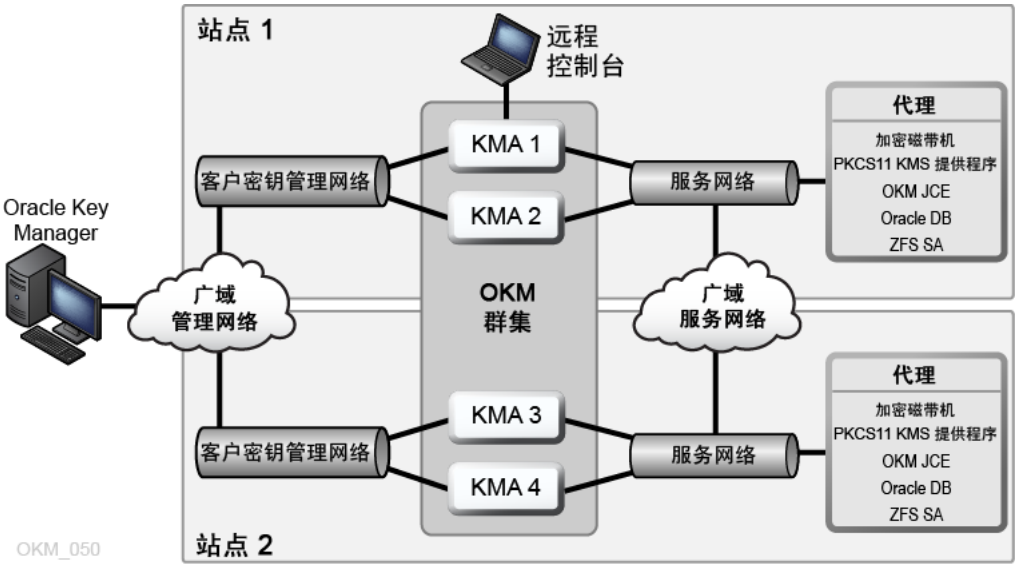
- 密钥管理设备 (Key Management Appliance, KMA)－一个强化了安全性的单元，可以提供基于策略的生命周期密钥管理、验证、访问控制和密钥置备服务。作为存储网络的可信机构，KMA 可确保所有存储设备都进行注册和验证，并且所有加密密钥的创建、置备和删除都遵守规定的策略。
- Oracle Key Manager GUI－一种图形用户界面，可在工作站上执行，并可通过 IP 网络与 KMA 通信来配置和管理 OKM。Oracle Key Manager GUI 必须安装在客户提供的工作站上。
- Oracle Key Manager CLI－两个命令行界面，可在工作站上执行，并可通过 IP 网络与 KMA 通信以实现常用管理操作的自动化。Oracle Key Manager CLI 必须安装在客户提供的工作站上。
- OKM 群集－系统中的全套 KMA。所有这些 KMA 都知道彼此的存在，并可互相复制信息。
- 代理－一个设备或软件，使用 OKM 群集管理的密钥执行加密。例如，StorageTek 加密磁带机就是一种代理。代理使用 KMS 代理协议与 KMA 进行通信。代理 API 是一组整合到代理硬件或软件中的软件接口。

OKM 使用 TCP/IP 网络实现 KMA、代理以及运行 Oracle Key Manager GUI 和 CLI 的工作站之间的连接。为了提供灵活的网络连接，每个 KMA 上提供了三个网络连接接口：

- 管理连接－用于连接到客户网络
- 服务连接－用于连接到代理
- ILOM/ELOM 连接－用于连接到 KMA 上的 ILOM 或 ELOM

请参见下图中的示例：

图 1.1.



1.2. 一般性安全原则

以下原则是安全地使用任何应用程序的基本原则。

1.2.1. 使软件保持最新

良好的安全做法包括许多原则，其中一条就是使所有软件版本和修补程序保持最新。可在 My Oracle Support 网站上找到最新的 Oracle Key Manager 升级包和安装程序：http://support.oracle.com。

1.2.2. 限制对关键服务的网络访问

将您的业务应用程序置于防火墙之后。防火墙可确保对这些系统的访问限定在已知的网络路由范围内，如有必要，可对其进行监视和限制。此外，防火墙路由器可代替多个独立的防火墙。

1.2.3. 遵循最小特权原则

最小特权原则是指应当向用户授予履行其职责所需的最小特权。过于宽松地授予职责、角色、权限等，尤其是在组织发展的早期，在人手少又需要迅速完成工作的情况下，常常会给系统留下很大的滥用漏洞。应定期查看用户特权，以确保仅授予与当前工作职责相关的特权。

1.2.4. 监视系统活动

系统安全依靠以下三方面：良好的安全协议、合适的系统配置以及系统监视。审计和检查审计记录可满足上面的第三项要求。系统中的每个组件都具有一定程度的监视能力。请遵循本文档中的审计建议，定期监视审计记录。

1.2.5. 密切关注最新安全信息

Oracle 会持续不断地改进其软件和文档。请每年在 My Oracle Support 网站检查是否存在修订版。

2

第 2 章 安全安装和配置

本部分概述了安全安装的规划过程，并介绍了几种推荐的系统部署拓扑。

2.1. 了解您的环境

为了更好地了解您的安全需求，可以问自己以下几个问题：

2.1.1. 我要保护的资源是什么？

可以保护生产环境中的许多资源。确定必须提供的安全级别时，请考虑需要保护的资源。

要保护的主要资源通常是您的数据。此处也列出了其他资源，这是因为它们与您的数据管理和保护有关联。对于保护数据的各种顾虑包括数据丢失（即，数据不可用）以及数据被破坏或者向未经授权的各方泄漏。

加密密钥经常用于保护数据免遭未经授权的泄漏。因此，它们是要保护的另一种资源。维护数据的高可用性必须要有高度可靠的密钥管理。要保护的另一层资源包括 Oracle Key Manager 群集自身中的资产，其中包含密钥管理设备。

2.1.2. 要阻止谁访问资源？

必须阻止无权访问这些资源的任何人访问它们。应当采用物理方式保护这些资源。应当考虑哪些员工应该具有这些资源的访问权限。然后，确定每个员工应该能够在 Oracle Key Manager 环境中执行哪些类型的操作。

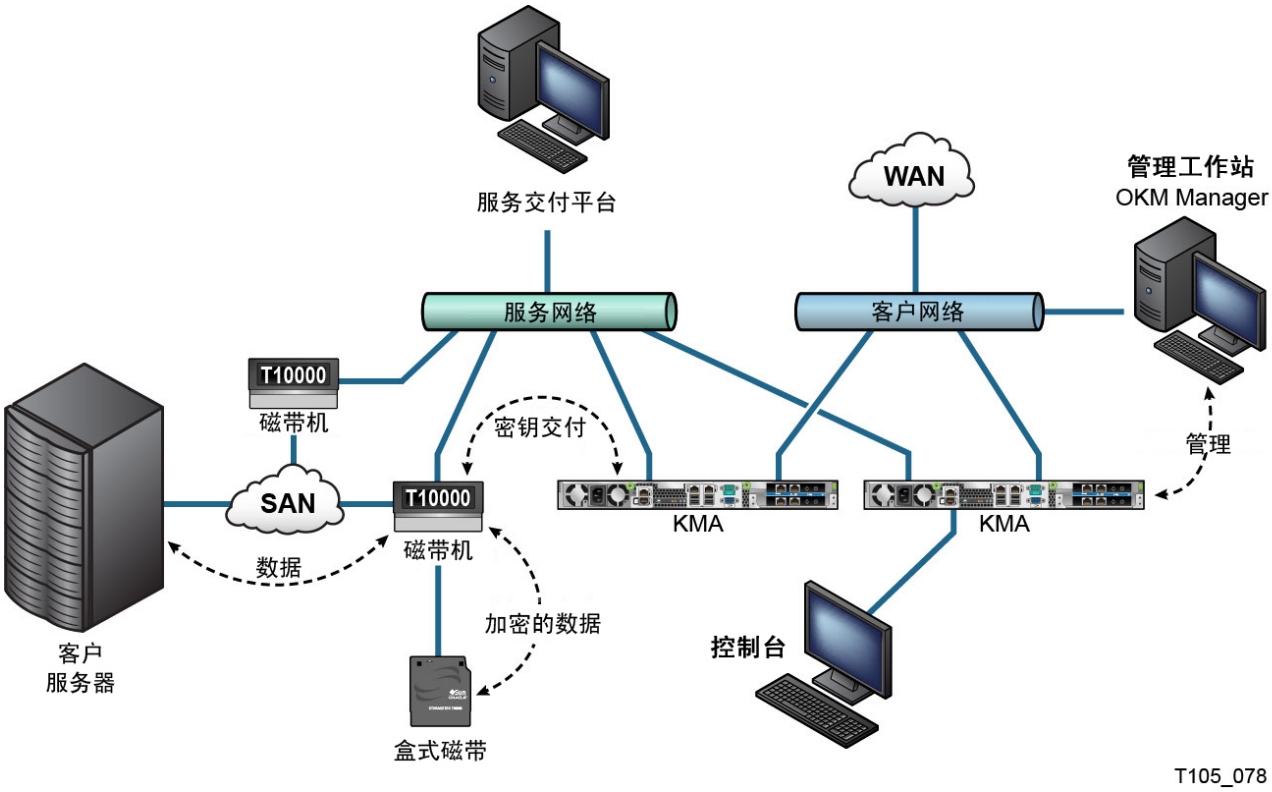
2.1.3. 如果对战略性资源的保护失败，将会产生什么后果？

在某些情况下，安全架构中出现的故障很容易被检测到，并且这种故障仅仅被视为操作不便。在另一些情况下，故障可能会对使用您的资源的公司或个人客户造成巨大损害。了解每个资源的安全后果有助于对其进行正确的保护。

2.2. 建议的部署拓扑结构

下图显示了 Oracle Key Manager 解决方案的典型部署。

图 2.1. OKM 解决方案的典型部署



2.3. 安装密钥管理设备

本部分介绍了如何安全地安装和配置 OKM 密钥管理设备。

KMA 是作为强化设备制造的，其中已包含了 Oracle Key Manager 功能。

在 OKM 群集中安装和配置 KMA 包括以下步骤：

1. 对于每个 KMA，将其安装在机架中。
2. 对于每个 KMA，确保其 ILOM 的安全。
3. 在 OKM 群集中配置第一个 KMA。
4. 向 OKM 群集中添加其他 KMA。

有关规划 OKM 群集部署的更多信息，请参阅 OKM 概述和规划指南。

2.3.1. 在机架中安装 KMA

Oracle 客户服务工程师根据 *Oracle Key Manager* 安装和服务手册中列出的步骤在机架中安装 KMA。Oracle 服务人员可以参阅此手册来获取更多详细信息。

2.3.2. 确保 KMA 的 ILOM 的安全

Oracle Key Manager KMA 采用了最新的 ILOM 固件。KMA 的 ILOM 应由 Oracle 客户服务工程师或客户进行保护。在升级 ILOM 固件之后也应该对 ILOM 进行保护。

要保护 ILOM 的安全，需要设置特定的 ILOM 设置来阻止对 ILOM 执行可能会危害安全的更改。有关说明，请参见 OKM 管理指南的“服务处理器过程”附录中的“ILOM 安全强化”。

2.3.3. 在 OKM 群集中配置第一个 KMA

在配置第一个 KMA 之前，请先确定密钥拆分凭证以及要在此 OKM 群集中定义的用户 ID 和密码短语。可以使用工作表（例如 OKM 安装和服务手册中的工作表（仅限内部使用））来实现此目的－请咨询 Oracle 支持代表。

将这些密钥拆分凭证以及用户 ID 和密码短语提供给相应的人员。有关更多信息，请参阅本文档下文中的"法定保护"。

注:

请保留并保护这些密钥拆分凭证以及用户 ID 和密码短语!

打开 Web 浏览器，启动远程控制台，然后在远程控制台中启动 OKM 快速启动实用程序。要在此 KMA 上初始化 OKM 群集，请按 Oracle Key Manager 文档库中的 *Oracle Key Manager* 管理指南中介绍的“初始化群集”过程操作。

在此过程中可定义密钥拆分凭证和具有安全官特权的用户。在快速启动过程完成后，安全官必须登录到 KMA 并定义其他 OKM 用户。

2.3.4. 定义密钥拆分凭证时的注意事项

定义较少的密钥拆分用户 ID 和密码短语和较低的阈值时，便利性较好，但安全性较低。定义较多的密钥拆分用户 ID 和密码短语和较高的阈值时，便利性较差，但安全性较高。

2.3.5. 定义其他 OKM 用户时的注意事项

定义较少的 OKM 用户数量，并且其中的某些用户分配有多个角色时，便利性较好，但安全性较差。定义较多的 OKM 用户并且其中大多数用户只分配有一个角色时，便利性较差，但安全性较高，因为便于跟踪由给定 OKM 用户执行的操作。

2.3.6. 向 OKM 群集中添加其他 KMA

打开 Web 浏览器，启动远程控制台，然后在远程控制台中启动 OKM 快速启动实用程序。要将此 KMA 添加到 OKM 群集，请按 *Oracle Key Manager* 管理指南中介绍的“加入群集”过程操作。

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto

2.3.7. 添加其他 KMA 时的注意事项

Oracle Key Manager 为每个 KMA 提供了方便的自主解锁选项。此选项是在群集中第一个及其他 KMA 的快速启动过程中定义的，并可由安全官在以后修改。

如果启用了自主解锁，则 KMA 将在启动时自动解锁，并准备好来提供密钥，不再要求法定审批。如果禁用自主解锁，则 KMA 将在启动时保持锁定状态，并且在安全官发出解锁请求并且对此请求进行法定批准之前，不会提供密钥。

为了获得最大的安全性，Oracle 建议不要启用自主解锁。有关自主解锁选项的更多信息，请参阅 *Oracle Key Manager Version 3.0 Security and Authentication White Paper*，网址为：

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf

2.3.8. 强化 KMA 的特征

如前所述，KMA 是作为强化设备制造的，其中已包含了 Oracle Key Manager 功能。强化设备具有以下特征：

- Solaris 映像中没有不需要的 Solaris 软件包。例如，Solaris 映像中没有 ftp 和 telnet 服务及实用程序。
- KMA 不生成核心文件。
- 标准 Solaris login(1) 实用程序已被 OKM 控制台取代。因此，用户无法登录到 Solaris 控制台。
- 默认情况下，ssh 服务处于禁用状态。为了提供客户支持，安全官可以将 ssh 服务启用一段有限的时间并定义一个支持帐户。此支持帐户是唯一可用帐户，具有有限的访问权限。Solaris 审计会跟踪该支持帐户调用的命令。
- Root 帐户处于禁用状态而且配置为一个角色。
- KMA 未配备 DVD 驱动器。
- 有效地禁用了 USB 端口。
- 关闭了不使用的网络端口。
- 启用了不可执行的堆。
- 配置了地址空间查找随机化。
- 启用了不可执行的堆。
- 针对安全敏感型文件系统使用了 ZFS 加密。
- 将 Solaris 配置为遵循 SCAP PCI-DSS 基准。
- 禁用了不必要的 SMF 服务。
- Oracle Solaris Verified Boot 在基于 SPARC T7-1 的 KMA 上是可配置的，这可确保系统引导进程的安全，防止损坏内核模块和插入 root 包或其他恶意程序。

- 在通电期间操作机箱门时，基于 SPARC T7-1 和 Netra SPARC T4-1 服务器的较新的 KMA 可防破坏（ILOM 故障）。
- ILOM 3.2 固件现在已通过 FIPS 140-2 Level 1 认证而且可以在 FIPS 模式下配置。
- 基本审计和报告工具会定期运行来帮助进行取证。这些报告包括在 OKM 系统转储中。
- Solaris 加密安全框架是在有或没有硬件安全模块的情况下，按照 FIPS 140-2 Level 1 安全策略（针对 Solaris 11.1 编写的）配置的。

2.4. TCP/IP 连接和 KMA

如果实体（OKM Manager、代理及同一群集中的其他 KMA）与 KMA 之间存在防火墙，该防火墙必须允许该实体在以下端口上与 KMA 建立 TCP/IP 连接：

- OKM Manager 到 KMA 通信需要端口 3331、3332、3333、3335。
- 代理到 KMA 通信需要端口 3331、3332、3334、3335。
- KMA 到 KMA 通信需要端口 3331、3332、3336。

注:

如果用户将其 KMA 配置为使用 IPv6 地址，请配置基于 IPv4 的边界防火墙来丢失所有出站 IPv4 协议 41 数据包和 UDP 端口 3544 数据包，以防止 Internet 主机使用任何 IPv6-over-IPv4 隧道通信访问内部主机。

有关详细信息，请参阅防火墙配置文档。表 2.1 “KMA 端口连接 ” 列出了 KMA 显式使用的端口或者 KMA 用来提供服务的端口。

表 2.1. KMA 端口连接

端口号	协议	方向	描述
22	TCP	侦听	SSH（仅当启用了技术支持时）
123	TCP/UDP	侦听	NTP
3331	TCP	侦听	OKM CA 服务
3332	TCP	侦听	OKM 证书服务
3333	TCP	侦听	OKM 管理服务
3334	TCP	侦听	OKM 代理服务
3335	TCP	侦听	OKM 搜索服务
3336	TCP	侦听	OKM 复制服务

表 2.2 “其他服务 ” 显示了在可能未使用的端口上侦听的其他服务。

表 2.2. 其他服务

端口号	协议	方向	描述
53	TCP/UDP	连接	DNS（仅当 KMA 配置为使用 DNS 时）
68	UDP	连接	DHCP（仅当 KMA 配置为使用 DHCP 时）

端口号	协议	方向	描述
111	TCP/UDP	侦听	RPC（KMA 对 rpcinfo 查询进行响应）。此端口仅在 KMS 2.1 和更早版本中才向外部请求开放
161	UDP	连接	SNMP（仅当定义了 SNMP 管理器时）
161	UDP	侦听	SNMP（仅当启用了 Hardware Management Pack 时）
514	TCP	连接	远程 syslog（仅当定义了远程 syslog 服务器而且将其配置为使用未加密的 TCP 时）
546	UDP	连接	DHCPv6（仅当 KMA 配置为使用 DHCP 和 IPv6 时）
4045	TCP/UDP	侦听	NFS 锁守护进程（仅限 KMS 2.0）
6514	基于 TCP 的 TLS	连接	远程 syslog（仅当定义了远程 syslog 服务器而且将其配置为使用未加密的 TLS 时）

注:

端口 443 必须开放，以便客户可以通过防火墙访问服务处理器 Web 界面和 OKM 控制台。请参阅《Oracle Key Manager Installation and Service Manual》（仅限内部使用）来查看 ELOM 和 ILOM 端口。

表 2.3 “ELOM/ILOM 端口 ” 列出了 KMA ELOM/ILOM 端口。如果需要从防火墙外部访问 ELOM/ILOM，则应启用这些端口；否则，不需要针对 ELOM/ILOM IP 地址启用这些端口：

表 2.3. ELOM/ILOM 端口

端口号	协议	方向	描述
22	TCP	侦听	SSH（对于 ELOM/ILOM 命令行界面）
53	TCP/UDP	连接	DNS（仅当配置了 DNS 时需要）
68	UDP	连接	如果 ELOM/ILOM 需要 DHCP。 注：虽然受支持，但未提供 DHCP 和 ELOM/ILOM 的文档。
80	TCP	侦听	HTTP（对于 ELOM/ILOM Web 界面） 如果需要 HTTP；否则，用户可以在以下位置查看有关如何连接到远程控制器的说明： ELOM： http://docs.oracle.com/cd/E19121-01/sf.x2100m2/819-6588-14/819-6588-14.pdf ILOM： http://docs.oracle.com/cd/E19860-01/index.html
161	UDP	侦听/连接	SNMPv3（可配置，这是默认端口）
443	TCP/TLS	侦听	Embedded/Integrated Lights Out Manager 基于传输层安全 (Transport Layer Security, TLS) 的管理协议 (WS-Man) 的 Desktop Management Task Force (DMTF) Web 服务

端口号	协议	方向	描述
623	UDP	侦听	智能平台管理接口 (Intelligent Platform Management Interface, IPMI)

3

第 3 章 安全功能

本部分概述了本产品提供的具体安全机制。

3.1. 潜在威胁

具有启用了加密功能的代理的客户主要担心：

- 违规泄漏信息
- 数据丢失或破坏
- 在发生灾难性故障（例如，在业务连续性站点中）时，不可接受的数据恢复延迟
- 未检测到的数据修改。

3.2. 安全功能的目标

Oracle Key Manager 的安全功能的目标是：

- 保护加密的数据以避免泄露。
- 最大程度地降低受攻击风险。
- 提供足够高的可靠性和可用性。

3.3. 安全模型

本安全指南的本部分内容将概括介绍系统设计用来应对的威胁，以及各项安全功能如何合作来阻止攻击。

提供这些保护的关键安全功能包括：

- 验证－确保只有经过授权才能访问系统和数据。
- 授权－对系统特权和数据的访问控制；这种访问控制建立在验证的基础上，可确保个体仅获得合适的访问权限
- 审计－使管理员可以检测到试图违反验证机制的违规行为以及试图或成功进行的访问控制违规行为。

有关 Oracle Key Manager 的安全性和验证方面的更多信息，请参阅《Oracle Key Manager Version 2.x Security and Authentication White Paper》，网址为：

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf

3.4. 验证

Oracle Key Manager 体系结构可以针对用户操作在系统的所有元素之间进行相互验证：KMA 对 KMA、代理对 KMA 以及 Oracle Key Manager GUI 或 CLI 对 KMA。

系统的每个元素（例如，新的加密代理）都通过以下方式在系统中进行注册：在 OKM 中创建 ID 和密码短语，然后将其输入到要添加的元素中。例如，将磁带机添加到系统中时，代理和 KMA 会根据共享的密码短语自动运行质询/响应协议，从而使代理获得根证书颁发机构 (Certificate Authority, CA) 证书以及一个新的密钥对和经过签署的代理证书。通过实施根 CA 证书、代理证书和密钥对，代理可以针对与 KMA 的所有后续通信运行传输层安全 (Transport Layer Security, TLS) 协议。所有证书都是 X.509 证书。

OKM 充当根证书颁发机构来生成一个根证书，然后，KMA 使用该证书来派生（自签署）代理、用户和新 KMA 使用的证书。

3.5. 访问控制

访问控制有以下类型：

- 基于用户和角色的访问控制
- 法定保护。

3.5.1. 基于用户和角色的访问控制

Oracle Key Manager 允许定义多个用户，每个用户都有一个用户 ID 和密码短语。可为每个用户提供一个或多个预定义角色。这些角色决定了允许用户对 Oracle Key Manager 系统执行的操作。这些角色包括：

- 安全官－执行 Oracle Key Manager 设置和管理
- 操作员－执行代理设置和日常操作
- 合规官－定义密钥组并控制代理对密钥组的访问权限
- 备份操作员－执行备份操作
- 审计员－查看系统审计迹
- 法定成员－查看和批准待定的法定操作

安全官是在快速启动过程中定义的，该过程在 OKM 群集中设置 KMA。以后，用户必须以安全官的身份使用 Oracle Key Manager GUI 登录到群集才能定义其他用户。安全官可以选择向特定用户分配多个角色，也可以选择将特定角色分配给多个用户。

有关每个角色允许的操作以及安全官如何创建用户并向其分配角色的更多信息，请参阅 Oracle Key Manager 文档库中的《Oracle Key Manager 管理指南》，网址为：

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto

这种基于角色的访问控制支持采用美国国家标准与技术研究院 (National Institute of Standards and Technology, NIST) 特殊出版物 (Special Publication, SP) 800-60 操作角色来分隔操作职能。

3.5.2. 法定保护

有些操作足够重要，需要增加安全级别。这些操作包括将 KMA 添加到 OKM 群集、KMA 解锁、创建用户以及为用户添加角色。为实施此安全性，系统除了使用前述基于角色的访问权限外，还使用一组密钥拆分凭证。

密钥拆分凭证包含一组用户 ID 和密码短语对，以及系统为支持完成特定操作所必需的这些对的最少数量。密钥拆分凭证也称为“法定”，最少数量也称为“法定阈值”。

Oracle Key Manager 最多允许定义 10 个密钥拆分用户 ID/密码短语对和一个阈值。它们是在快速启动过程中在 OKM 群集中配置第一个 KMA 时定义的。密钥拆分用户 ID 和密码短语不同于用来登录到系统的用户 ID 和密码短语。当用户尝试需要法定审批的操作时，所定义的密钥拆分用户阈值和密码短语必须在系统执行此操作之前批准此操作。

3.6. 审计

每个 KMA 都会针对其执行的操作记录审计事件，包括由代理、用户以及 OKM 群集中的对等 KMA 发出的事件。代理、用户或对等 KMA 自身每次验证失败时，MKA 也会记录审计事件。将记录指示安全违规的审计事件。例如，验证失败就是指示安全违规的一个审计事件。如果在 OKM 群集中标识了 SNMP 代理，则在遇到安全违规时，KMA 还会将 SNMP INFORM 发送到这些 SNMP 代理。如果配置了远程 Syslog，则 KMA 还会将这些审计消息转发给所配置的服务器。请参见"远程 *Syslog* "。

用户必须正确地登录到 OKM 群集，并且必须分配有某个角色才能查看审计事件。

KMA 管理其审计事件。KMA 会根据保留期限和限制（计数）删除较旧的审计事件。安全官可根据需要修改这些保留期限和限制。

3.7. 其他安全功能

Oracle Key Manager 还提供了其他安全功能。有关这些功能以及其他 OKM 功能的更多信息，请参阅《Oracle Key Manager Overview》，网址为：

`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf`

3.7.1. 安全通信

代理与 KMA 之间、用户与 KMA 之间以及 KMA 与对等 KMA 之间的通信协议是一样的。在每种情况下，系统都将使用发起通信的实体的密码短语来执行质询/响应协议。

如果成功，将向实体提供证书及其对应的私钥。这个证书和私钥可以建立传输层安全 (Transport Layer Security, TLS)（安全套接字）通道。执行相互验证；任何连接的每一端都会对另一方进行验证。OKM 3.1+ KMA 将始终使用 TLS 1.2 执行其对等方复制通信。

3.7.2. 硬件安全模块

KMA 有一个可用的硬件安全模块，该模块需要单独订购。此硬件安全模块是一个 Sun Cryptographic Accelerator (SCA) 6000 卡，通过了 FIPS 140-2 Level 3 认证，可提供高级加密标准 (Advanced Encryption Standard, AES) 256 位加密密钥（此证书已在 2015 年 12 月 31 日过期且没有续订，在后续版本中将提供替代 HSM）。该 SCA 6000 卡支持 FIPS 140-2 Level 3 操作模式，并且 OKM 始终以此方式使用该卡。当 OKM 群集以符合 FIPS 标准的模式运行时，加密密钥不会将 SCA 6000 卡的加密边界保留为未封装的形式。该 SCA 6000 卡使用经过 FIPS 认可的随机数生成器，按 FIPS 186-2 DSA 随机数生成器中指定的方式，使用 SHA-1 来生成加密密钥。

如果 KMA 未配置为使用 SCA 6000 卡，则会使用 Solaris 加密框架 (Solaris Cryptographic Framework, SCF) PKCS#11 软令牌执行加密。SCF 是在 FIPS 140 模式下按照最近发布的 Solaris FIPS 140-2 安全策略配置的。

3.7.3. AES 密钥包装

在创建密钥、在 KMA 上存储密钥、将密钥传输到代理或者在密钥传输文件中时，Oracle Key Manager 使用 AES 密钥包装 (RFC 3994)；该包装采用 256 位密钥加密密钥来保护对称密钥。

3.7.4. 密钥复制

初始化 OKM 群集的第一个 KMA 时，该 KMA 会生成一个很大的密钥池。当向群集添加其他 KMA 时，会将密钥复制到新 KMA，准备好用于加密数据。添加到群集中的每个 KMA 都会生成一个密钥池，并将它们复制到群集中的对等 KMA。所有 KMA 都将根据需要生成新的密钥来保持密钥池的大小，以便始终有准备好的密钥供代理使用。当某个代理需要新密钥时，该代理会与群集中的某个 KMA 通信，请求新密钥。该 KMA 会从其密钥池中提取一个准备好的密钥，并将该密钥分配到代理的默认密钥组以及数据单元。然后，该 KMA 会通过网络将这些数据库更新复制到群集中的其他 KMA。以后，代理可以与群集中的其他 KMA 通信来检索密钥。在任何时候都不会有任何明文材料通过网络传输。

3.7.5. Solaris FIPS 140-2 安全策略

2013 年 12 月，美国国家标准与技术研究院 (National Institute of Standards and Technology, NIST) 为 Solaris 11 中的 Oracle Solaris 内核加密框架模块颁发了编号为 2061 的 FIPS 140-2 Level 1 验证证书。2014 年 1 月，NIST 为 SPARC T4 和 SPARC T5 中的 Oracle Solaris Userland 加密框架颁发了编号为 2076 的 FIPS 140-2 Level 1 验证证书。Oracle Key Manager 3.1.0 KMA 现在基于仍在进行 FIPS 140-2 验证测试的 Solaris 11.3。 Oracle Key Manager 3.1.0 KMA 中的 Oracle Solaris 内核加

密框架是按照 *Oracle* 内核加密框架安全策略配置的。同样，KMA 也是按照 *SPARC T4* 和 *SPARC T5* 中的 *Oracle Solaris Userland* 加密框架安全策略配置的。一旦推出较新的 Solaris 安全策略，OKM 就将更新到较新的安全策略。

3.7.6. 软件升级

所有的 KMA 软件升级包都经过数字签名，以防止从未经批准的来源加载恶意软件。

4

第 4 章 端点

OKM 支持多种加密端点。下面是支持的端点：

- 能够加密的磁带机
- Oracle 透明数据库加密 (Transparent Database Encryption, TDE) 11g 和更高版本
- Oracle ZFS Storage Appliance
- Oracle Solaris 11 ZFS 文件系统

另外，还提供了可供应用程序开发人员使用的端点工具，对于 PKCS#11，提供了可以和 Oracle 数据库的透明数据库加密 (Transparent Database Encryption, TDE) 一起使用的端点工具。

4.1. Linux PKCS#11 KMS 提供程序

对于希望使用 PKCS#11 与 OKM 进行通信的客户，提供了一个 Linux PKCS#11 KMS 提供程序。管理员可以从 My Oracle Support 网站下载该 Linux PKCS#11 KMS 提供程序，并将其安装在 Oracle Enterprise Linux 服务器上。与其他代理一样，该 Linux PKCS#11 KMS 提供程序具有相同的安全特征，并使用 Oracle Key Manager 设备进行验证。该 Linux PKCS#11 KMS 提供程序将日志文件和配置文件信息存储在 *`/var/opt/kms/username`* 目录下。用户和/或管理员应手动或者使用 logrotate 之类的实用程序管理此日志文件。应通过相应的权限来限制对 *`/var/opt/kms/username`* 目录的访问控制。在配置文件目录中，代理的验证凭证保留在一个 PKCS#12 文件中。该 PKCS#12 文件由一个密码予以保护。有关该 Linux PKCS#11 KMS 提供程序的更多信息，请参阅 Oracle Key Manager 文档库中的 Oracle Key Manager 管理指南，网址为：

`http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#mainframeswncs`

4.2. Solaris PKCS#11 KMS 提供程序

随 Solaris 10 和 Solaris 11 提供了类似的 PKCS#11 KMS 提供程序。

4.3. JCE KMS 提供程序

对于希望实施可从 OKM 获取密钥的 Java 客户端应用程序的开发人员，提供了一个 Java Cryptographic Environment 提供程序。此产品已经与各种 Oracle 产品集成而且可以从 Oracle 技术网获得。

4.4. Oracle Enterprise Manager 的 OKM 插件。

Oracle Enterprise Manager (OEM) Cloud Control 的 Oracle Key Manager (OKM) 设备插件用来监视 OKM 群集。属于群集的每个 KMA 都由该插件进行监视。为该工具提供了安全指南。

5

第 5 章 远程 Syslog

Oracle Key Manager 支持远程 syslog。可以将 KMA 配置为通过未加密 TCP 或通过传输层安全 (Transport Layer Security, TLS) 协议向远程 syslog 服务器发送采用 RFC 3164 或 RFC 5424 消息格式的消息。注意，RFC 5425 描述了如何使用 TLS 为采用 RFC 5424 消息格式的 syslog 消息的传输提供安全连接。

安全官可以将 KMA 配置为通过未加密 TCP 或通过 TLS 发送消息。更加安全的方法是使用 TLS 进行验证并对 KMA 和远程 syslog 服务器之间的通信进行加密。KMA 通过请求远程 syslog 服务器的证书和公钥来对该服务器进行验证。（可选）可以将远程 syslog 服务器配置为使用相互验证。相互验证确保远程 syslog 服务器仅接受来自经授权的客户机（如 KMA）的消息。如果远程 syslog 服务器配置为使用相互验证，则该服务器将从 KMA 请求证书来对 KMA 的身份进行验证。

6

第 6 章 Hardware Management Pack

Oracle Key Manager 支持 SPARC T7-1、Netra SPARC T4-1 和 Sun Fire X4170 M2 KMA 上的 Oracle Hardware Management Pack (HMP)。与 ILOM 一起，HMP 产品是 Oracle Single System Management 的成员之一。安全官可以使 KMA 上的 HMP 使用 Solaris 中的管理代理通过 SNMP 实现对 KMA 的带内监视。HMP 软件随 SNMP 代理配置一起预先安装，但是处于禁用状态。因此，只有在启用 HMP 之后，SNMP 代理侦听端口才会打开。默认情况下，HMP 处于禁用状态。

启用 HMP 可以：

- 在硬件问题表现为特定于 Oracle Key Manager 的 SNMP 通知或 KMA 故障之前，提供硬件问题的事件通知。
- 使您能够在 OKM 群集中的任何或所有受支持的 KMA 上启用 HMP。
- 使您能够针对 KMA 上的 SNMP MIB（包括 MIB-II、SUN-HW-MONITORING-MIB 和 SUN-STORAGE-MIB）执行只读的 SNMP Get 操作。
- 允许 Oracle Red Stack 通过 SNMP Receivelet 和 SNMP Fetchlet 与 Oracle Enterprise Manager 进行集成。

选择在 KMA 上启用 HMP 时，应当牢记以下安全注意事项。在启用后，HMP 会执行以下操作：

- 利用 Oracle Key Manager 群集中配置的任何已启用的协议 v2c SNMP 管理器。SNMP v2c 协议没有 SNMP v3 协议中提供的安全增强功能。
- 在 KMA 上启用 SNMP 管理代理，允许对该 KMA 上的 SNMP MIB 信息进行只读网络访问。
- 通过以下方法降低了 *Oracle Hardware Management Pack (HMP)* 安全指南 (http://docs.oracle.com/cd/E20451_01/pdf/E27799.pdf) 中标识的安全风险：
  - “系统管理产品可以用于获取可引导的根环境”－强化的 KMA 禁用了用户对系统的 root 访问。SNMP 被配置为进行只读访问。因此，SNMP Put 操作会被拒绝。
  - “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”－禁用了对 KMA 的 root 访问。因此，系统用户无法运行这些工具。

附录 A

附录 A. 安全部署核对表

以下安全核对表包括有助于确保密钥管理系统安全的准则：

1. 在物理安全的环境中安装每个 KMA。
2. 确保每个 KMA 上 OpenBoot PROM 或 BIOS 的安全。
3. 确保每个 KMA 上 Lights Out Manager 的安全。
4. 为此 Oracle Key Manager 群集定义密钥拆分配置。
5. 根据情况为每个 KMA 设置相应的自主解锁设置。
6. 定义 Oracle Key Manager 用户及与其关联的角色。
7. 遵循最小特权原则。
    a. 仅向每个 Oracle Key Manager 用户授予必需的那些角色。
8. 监视 Oracle Key Manager 群集上的活动。
    a. 调查在 Oracle Key Manager 审计日志中记录的任何错误，尤其是安全违规。
9. 在初次定义密钥拆分配置时以及在修改密钥拆分配置时，备份核心安全设置。
10. 定期执行 Oracle Key Manager 备份。
11. 将核心安全备份文件和 Oracle Key Manager 备份文件存储在安全位置。

附录 B

附录 B. 参考

- Oracle Key Manager 客户文档

  http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto
- *Oracle Enterprise Manager System Monitoring Plug-in for Oracle Key Manager Security Guide*
- *Oracle Key Manager Installation and Service Manual*（仅限内部使用）
- *Oracle Key Manager Overview*

  http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf
- *Oracle Key Manager Version 2.X Security and Authentication White Paper*

  http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf
- Oracle Integrated Lights Out Manager (ILOM) 文档

  http://docs.oracle.com/cd/E37444_01/
- SPARC T7-1 服务器文档 https://docs.oracle.com/cd/E54976_01/
- Netra SPARC T4-1 服务器文档

  http://docs.oracle.com/cd/E23203_01/
- Oracle Hardware Management Pack 文档
  - Oracle Hardware Management Pack 文档库

    http://docs.oracle.com/cd/E20451_01/
  - Oracle Single System Management

    http://www.oracle.com/technetwork/server-storage/servermgmt/overview/index.html
- NIST 文档：
  - *National Institute of Standards and Technology Special Publication 800-60 Volume I Revision 1*

    http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

- Oracle 产品的安全策略文档：
  - *Oracle Solaris* 内核加密框架安全策略

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2061.pdf
  - *SPARC T4* 和 *T5* 中的 *Oracle Solaris* 内核加密框架安全策略

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2060.pdf
  - *Sun Cryptographic Accelerator 6000 FIPS 140-2* 安全策略

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1050.pdf
  - *Oracle StorageTek T10000D* 磁带机安全策略

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2254.pdf
  - *Oracle StorageTek T10000C* 磁带机安全策略

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1561.pdf
  - *Oracle StorageTek T10000B* 磁带机安全策略

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1156.pdf
  - *Oracle StorageTek T10000A* 磁带机安全策略

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1157.pdf
  - *Oracle StorageTek T9480D* 磁带机安全策略

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1288.pdf
- Oracle 产品的 FIPS 验证证书：
  - Sun Crypto Accelerator 6000 - 证书编号 1026（已过期）

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1026.pdf