Oracle® Key Manager 3

安全指南

3.1 版

E52207-02

2016 年 4 月

ORACLE®

Oracle® Key Manager 3
安全指南

E52207-02

內容

序言 7

對象 7
文件輔助功能 7

1. 簡介 9

1.1. 產品簡介 9
1.2. 一般安全原則 10
1.2.1. 將軟體保持在最新狀態 10
1.2.2. 限制對重要服務的網路存取 10
1.2.3. 遵循最低權限的原則 10
1.2.4. 監督系統活動 10
1.2.5. 將安全資訊保持在最新狀態 11

2. 安全安裝與組態 13

2.1. 瞭解您的環境 13
2.1.1. 我要保護哪些資源？ 13
2.1.2. 我要保護資源不受到哪些人存取？ 13
2.1.3. 策略性資源的保護萬一失敗將發生什麼情況？ 13
2.2. 建議的部署拓樸 13
2.3. 安裝金鑰管理設備 14
2.3.1. 在機架中安裝 KMA 14
2.3.2. 保護 KMA 的 ILOM 15
2.3.3. 設定 OKM 叢集中的第一個 KMA 15
2.3.4. 定義分割金鑰證明資料的考量 15
2.3.5. 定義其他 OKM 使用者的考量 15
2.3.6. 新增其他 KMA 至 OKM 叢集 15
2.3.7. 新增其他 KMA 的考量 16
2.3.8. 強化 KMA 的特性 16
2.4. TCP/IP 連線和 KMA 17

3. 安全功能 21

3.1. 潛在威脅 21
3.2. 安全功能的目標 21

3.3. 安全模型 21
3.4. 認證 22
3.5. 存取控制 22
3.5.1. 以使用者與角色為基礎的存取控制 22
3.5.2. 仲裁保護 23
3.6. 稽核 23
3.7. 其他安全功能 23
3.7.1. 安全通訊 23
3.7.2. 硬體安全模組 24
3.7.3. AES 金鑰包裝 24
3.7.4. 金鑰複製 24
3.7.5. Solaris FIPS 140-2 安全原則 24
3.7.6. 軟體升級 25

4. 端點 27

4.1. Linux PKCS#11 KMS 提供者 27
4.2. 適用於 Solaris 的 PKCS#11 KMS 提供者 27
4.3. JCE KMS 提供者 27
4.4. Oracle Enterprise Manager 適用的 OKM 外掛程式 28

5. 遠端系統日誌 29

6. 硬體管理套件 31

A. 安全部署檢查清單 33

B. 參考資料 35

附表目錄

2.1. KMA 連接埠連線 17
2.2. 其他服務 17
2.3. ELOM/ILOM 連接埠 18

前言

本文件說明 Oracle Key Manager 3 (OKM 3) 的安全功能。

對象

本指南適用於使用 OKM 3 安全功能、安全安裝及組態的相關人員。

文件輔助功能

如需 Oracle 對於輔助功能的承諾的相關資訊，請造訪 Oracle Accessibility Program 網站，網址為 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc。

取用 Oracle Support
已購買支援的 Oracle 客戶可以透過 My Oracle Support 使用電子支援。如需相關資訊，請造訪 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；或如果您在聽力上需要特殊服務，請造訪 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

1

第 1 章 簡介

本節提供產品的簡介並說明應用程式安全的一般原則。

1.1. 產品簡介

Oracle Key Manager (OKM) 可建立、儲存與管理加密金鑰。OKM 是由下列元件所組成：

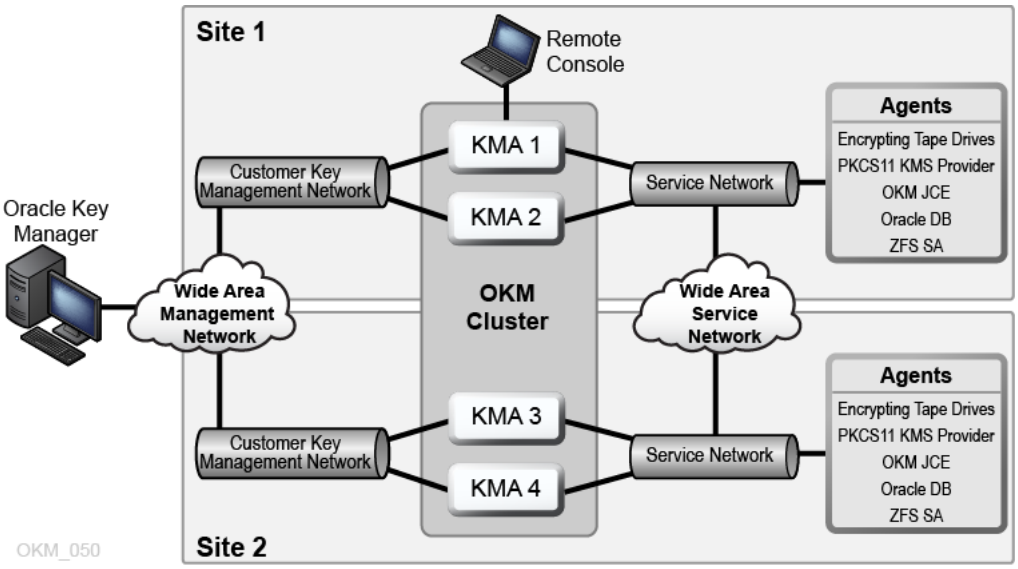
- 金鑰管理設備 (Key Management Appliance，KMA) – 此為強化安全的設備，提供可設定原則的週期金鑰管理、認證、存取控制與金鑰啟動設定服務。作為儲存網路的信任授權單位，KMA 可確保註冊並認證所有儲存裝置，且所有加密金鑰的建立、啟動設定及刪除均符合指定的原則。
- Oracle Key Manager GUI – 此為圖形使用者介面；這個圖形使用者介面會在工作站上執行，並可透過 IP 網路與 KMA 通訊，以設定與管理 OKM。Oracle Key Manager GUI 必須安裝在客戶提供的工作站上。
- Oracle Key Manager CLI – 此為兩個指令行介面；這兩個指令行介面會在工作站上執行，並可透過 IP 網路與 KMA 通訊，以自動化一般管理作業。Oracle Key Manager CLI 必須安裝在客戶提供的工作站上。
- OKM 叢集 – 系統中整組的 KMA。所有 KMA 均知悉彼此的存在，且會相互複製資訊。
- 代理程式 – 使用 OKM 叢集管理的金鑰執行加密的裝置或軟體。例如 StorageTek 加密磁帶機。代理程式使用 KMS 代理程式協定與 KMA 通訊。代理程式 API 是一組軟體介面，可整合至代理程式的硬體或軟體。

OKM 在 KMA、代理程式及執行 Oracle Key Manager GUI 與 CLI 所在工作站之間的連線使用 TCP/IP 網路。為了提供彈性的網路連線，每個 KMA 上的網路連線均有三個介面：

- 管理連線 – 用於客戶網路連線
- 服務連線 – 用於代理程式連線
- ILOM/ELOM 連線 – 用於 KMA 上的 ILOM 或 ELOM 連線

請看下列影像中的範例：

圖 1.1.



1.2. 一般安全原則

下列為安全使用任何應用程式的基本原則。

1.2.1. 將軟體保持在最新狀態

為了安全起見，建議您讓所有軟體版本與修補程式保持在最新的狀態。My Oracle Support 網站上提供最新的 Oracle Key Manager 升級套裝軟體和安裝程式，位置在：`http://support.oracle.com`。

1.2.2. 限制對重要服務的網路存取

請使用防火牆保護您的商業應用程式。防火牆可確保只有透過已知的網路路徑才能存取這些系統，並且能依照需求監督與限制這些網路路徑。另外，您也可以使用防火牆路由器取代多部獨立的防火牆。

1.2.3. 遵循最低權限的原則

最低權限的原則是指使用者應被授予最少的權限來執行他們的工作。過度授予職責、角色、授權等 (特別是在人員較少且必須迅速完成工作的組織早期階段)，可能會導致系統遭到濫用。請定期複查使用者權限，以判斷與現有工作責任的關聯。

1.2.4. 監督系統活動

系統安全取決於三個條件：良好的安全協定、正確的系統組態以及系統監督。稽核及複查稽核記錄可滿足第三項需求。系統內的每個元件都具備某種程度的監督功能。依循本文件中的稽核建議並定期監督稽核記錄。

1.2.5. 將安全資訊保持在最新狀態

Oracle 會持續改善其軟體和文件。請每年查看 My Oracle Support 網站是否有新的修訂版本。

2

第 2 章 安全安裝與組態

本節概述安全安裝的規劃程序，以及描述數種建議的系統部署拓樸。

2.1. 瞭解您的環境

為了更進一步瞭解您的安全需求，請思考下列問題：

2.1.1. 我要保護哪些資源？

在生產環境中有許多資源需要受到保護。決定您必須提供的安全等級時，請考慮需要保護的資源。

要保護的主要資源通常是您的資料。此處列出管理與保護資料相關的其他資源。保護資料的相關重點包括資料遺失 (亦即無法使用資料) 與資料被入侵或洩露給未取得授權的人員。

加密金鑰經常用來保護資料，防止未經授權的存取。因此，加密金鑰也是要保護的資源。必須要有十分可靠的金鑰管理，才能維持資料的高可用性。需要保護的另一層資源包括 Oracle Key Manager 叢集內的資產，其中包含金鑰管理設備。

2.1.2. 我要保護資源不受到哪些人存取？

上述資源必須受到保護，未經授權的任何人皆不得存取。這些資源也應受到實體保護。您應考量有哪些員工可存取這些資源。然後識別每位員工在 Oracle Key Manager 環境中可執行作業的類型。

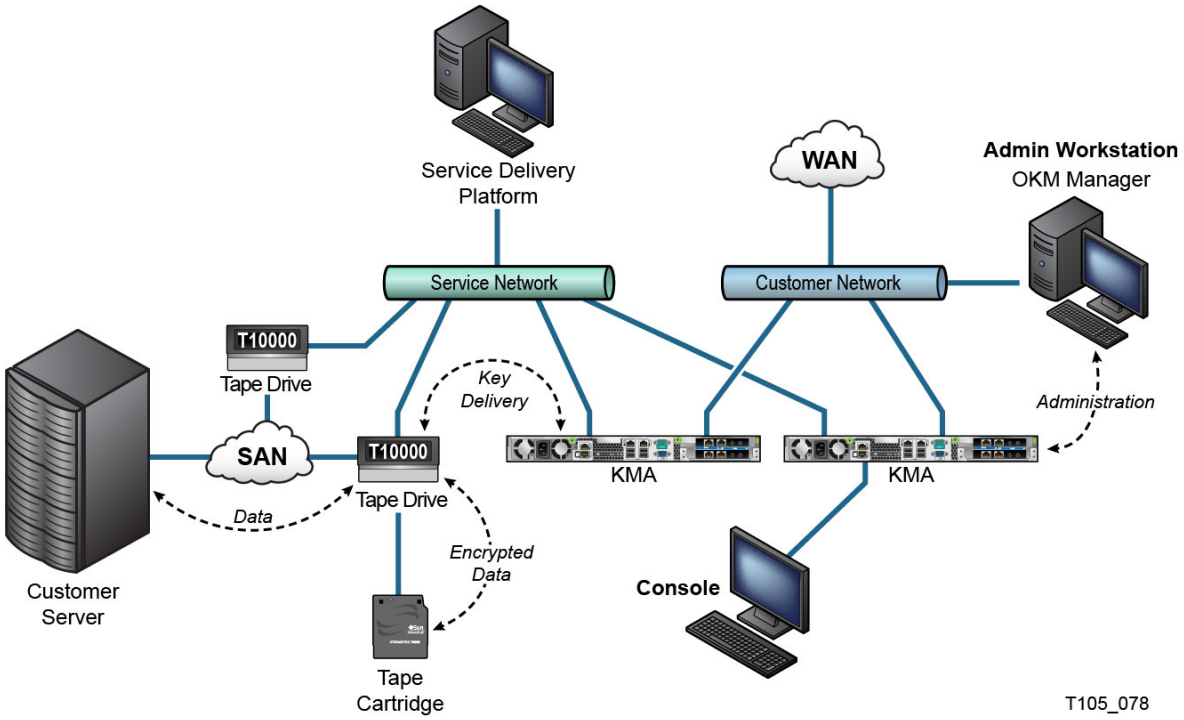
2.1.3. 策略性資源的保護萬一失敗將發生什麼情況？

在某些情況下，可以輕易偵測到安全方案中的錯誤，只會造成輕微困擾。在其他情況下，錯誤可能造成使用資源的公司或個人客戶重大損失。瞭解每種資源的安全相關問題將有助於妥善保護資源。

2.2. 建議的部署拓樸

下圖顯示 Oracle Key Manager 解決方案的一般部署。

圖 2.1. OKM 解決方案的一般部署



2.3. 安裝金鑰管理設備

本節說明如何安全地安裝與設定 OKM 金鑰管理設備。

KMA 為強化的設備，內建 Oracle Key Manager 功能。

在 OKM 叢集中安裝與設定 KMA 包含下列步驟：

1. 將每個 KMA 安裝在一個機架中。
2. 保護每個 KMA 的 ILOM。
3. 設定 OKM 叢集中的第一個 KMA。
4. 新增其他 KMA 至 OKM 叢集。

有關規劃 OKM 叢集部署的詳細資訊，請參閱 OKM 的「*Overview and Planning Guide*」。

2.3.1. 在機架中安裝 KMA

Oracle 客服工程師會根據「*Oracle Key Manager Installation and Service Manual*」中的程序，將 KMA 安裝在機架中。Oracle 服務人員可能會參閱此手冊以瞭解詳細資訊。

2.3.2. 保護 KMA 的 ILOM

Oracle Key Manager KMA 製造時會使用最新的 ILOM 韌體。KMA 的 ILOM 應由 Oracle 客服工程師或客戶加以保護。升級 ILOM 韌體之後，也應保護 ILOM。

保護 ILOM 包括設定特殊的 ILOM 設定值，以避免 ILOM 被變更而危及安全性。如需指示，請參閱「OKM *Administration Guide*」附錄「Service Processor Procedures」中的「ILOM Security Hardening」。

2.3.3. 設定 OKM 叢集中的第一個 KMA

設定第一個 KMA 之前，首先請識別此 OKM 叢集中定義的分割金鑰證明資料與使用者 ID 及密碼詞組。您可以就此目的使用工作表，例如在「OKM *Installation and Service Manual* (internal-only)」中找到的工作表 — 請洽詢您的 Oracle 客戶服務代表。

將這些分割金鑰證明資料與使用者 ID 及密碼詞組提供給適當的人員。請參閱本文件後面的「仲裁保護」，瞭解詳細資訊。

注意:

請保留並保護這些分割金鑰證明資料與使用者 ID 及密碼詞組！

開啟 Web 瀏覽器，啟動「遠端主控台」，並啟動「遠端主控台」中的 OKM 快速啟動公用程式。若要起始此 KMA 上的 OKM 叢集，請依照 Oracle Key Manager 文件庫中「*Oracle Key Manager Administration Guide*」所述的 "Initialize Cluster" 程序操作。

此程序會定義分割金鑰證明資料，以及具有一位「安全人員」權限的使用者。完成快速啟動程序之後，「安全人員」必須登入 KMA 並定義其他 OKM 使用者。

2.3.4. 定義分割金鑰證明資料的考量

定義較少的分割金鑰使用者 ID 與密碼詞組及較低的臨界值雖然較為方便，但是較不安全。定義較多的分割金鑰使用者 ID 與密碼詞組及較高的臨界值雖然較不方便，但是較為安全。

2.3.5. 定義其他 OKM 使用者的考量

定義較少的 OKM 使用者，並指派多個角色給其中部分使用者，雖然較為方便，但是較不安全。定義較多的 OKM 使用者，但僅指派單一角色給大部分使用者，雖然較不方便，但是較為安全，因為這樣做有助於追蹤特定 OKM 使用者執行的作業。

2.3.6. 新增其他 KMA 至 OKM 叢集

開啟 Web 瀏覽器，啟動「遠端主控台」，並啟動「遠端主控台」中的 OKM 快速啟動公用程式。若要新增此 KMA 至 OKM 叢集，請依照「*Oracle Key Manager Administration Guide*」所述的 "Join Cluster" 程序操作：

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

2.3.7. 新增其他 KMA 的考量

Oracle Key Manager 為每個 KMA 提供「自動解除鎖定」的方便選項。此選項是在叢集中第一個與其他 KMA 的快速啟動程序期間定義，之後可由「安全人員」修改。

如果啟用「自動解除鎖定」，則 KMA 將會在啟動時自行自動解除鎖定，且無須經由仲裁核准便可提供金鑰。若停用「自動解除鎖定」，則 KMA 將會在啟動時維持鎖定狀態，除非「安全人員」發出解除鎖定的要求，且仲裁核准此要求，才會提供金鑰。

為達最高的安全性，Oracle 不建議啟用自動解除鎖定。如需「自動解除鎖定」選項的詳細資訊，請參閱「*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

2.3.8. 強化 KMA 的特性

如上所述，KMA 為強化的設備，當中內建立即可用的 Oracle Key Manager 功能。KMA 作為強化設備，具有下列特性：

- 非必要的 Solaris 套裝軟體不會包含在 Solaris 影像中。例如，ftp 和 telnet 服務及公用程式不會出現在 Solaris 影像中。
- KMA 不會產生核心檔案。
- 標準 Solaris login(1) 公用程式已由 OKM 主控台所取代。因此，使用者無法登入 Solaris 主控台。
- 預設會停用 ssh 服務。為了客戶服務之故，「安全人員」可在有限的時間內啟用 ssh 服務並定義支援帳號。此支援帳號為唯一可用的帳號，具有有限的權限。Solaris 稽核會追蹤支援帳號呼叫的命令。
- 停用 root 帳號，並將其設定為一個角色。
- KMA 不會配備 DVD 光碟機。
- 會確實停用 USB 連接埠。
- 會關閉不使用的網路連接埠。
- 會啟用不可執行的堆疊。
- 會設定位址空間查詢隨機載入。
- 會啟用不可執行的堆集。
- 會使用 ZFS 加密安全機密檔案系統。
- Solaris 設定為符合 SCAP PCI-DSS 基準。
- 會停用不必要的 SMF 服務。
- 您可以在 SPARC T7-1 型的 KMA 上設定「Oracle Solaris 驗證式開機」，以保護系統開機程序，避免核心模組損毀、防止插入 root 套件或其他惡意程式。

- 使用 SPARC T7-1 和 Netra SPARC T4-1 伺服器的較新 KMA，通電時若機架門開啟，便會觸發篡改存跡 (ILOM 錯誤) 功能。
- ILOM 3.2 韌體現在已通過 FIPS 140-2 Level 1 認證，可以在 FIPS 模式中設定。
- 「基本稽核和報告工具」會定期執行以協助鑑識調查。這些報告會包括在 OKM 系統傾印中。
- 不論是否含有「硬體安全模組」，Solaris Cryptographic Security Framework 都會依據 FIPS 140-2 Level 1 安全原則 (針對 Solaris 11.1 所說明) 進行設定。

2.4. TCP/IP 連線和 KMA

若個體 (相同叢集中的 OKM 管理程式、代理程式以及其他 KMA) 與 KMA 之間有防火牆存在，則防火牆必須允許個體在下列連接埠建立與 KMA 的 TCP/IP 連線：

- OKM 管理程式與 KMA 的通訊需要使用連接埠 3331、3332、3333、3335。
- 代理程式與 KMA 的通訊需要使用連接埠 3331、3332、3334、3335。
- KMA 與 KMA 的通訊需要使用連接埠 3331、3332、3336。

注意:

對於將其 KMA 設定為使用 IPv6 位址的使用者而言，應該將以 IPv4 為基礎的邊緣防火牆 (Edge Firewall) 設定為刪除所有外送 IPv4 協定 41 的封包和 UDP 連接埠 3544 的封包，以防止網際網路主機使用任何 IPv6-over-IPv4 通道流量來連線內部主機。

請參閱您的防火牆組態文件瞭解詳細資訊。表格 2.1, 「KMA 連接埠連線 」 列出 KMA 明確使用的連接埠或 KMA 提供服務所在的連接埠。

表格 2.1. KMA 連接埠連線

連接埠號碼	協定	方向	描述
22	TCP	監聽	SSH (只有在啟用「技術支援」時才會提供此選項)
123	TCP/UDP	監聽	NTP
3331	TCP	監聽	OKM CA 服務
3332	TCP	監聽	OKM 憑證服務
3333	TCP	監聽	OKM 管理服務
3334	TCP	監聽	OKM 代理程式服務
3335	TCP	監聽	OKM 尋找服務
3336	TCP	監聽	OKM 複製服務

表格 2.2, 「其他服務 」 顯示在可能未使用之連接埠進行監聽的其他服務。

表格 2.2. 其他服務

連接埠號碼	協定	方向	描述
53	TCP/UDP	連線	DNS (只有當 KMA 設定為使用 DNS 時，才會提供此選項)

連接埠號碼	協定	方向	描述
68	UDP	連線	DHCP (只有當 KMA 設定為使用 DHCP 時，才會提供此選項)
111	TCP/UDP	監聽	RPC (KMA 回應 rpcinfo 查詢)。此連接埠只有在 KMS 2.1 和更舊版本才會開啟供外部要求使用
161	UDP	連線	SNMP (只有在已定義「SNMP 管理程式」時，才會提供此選項)
161	UDP	監聽	SNMP (只有在啟用「硬體管理套件」時，才會提供此選項)
514	TCP	連線	遠端系統日誌 (只有在已定義遠端系統日誌伺服器並將其設定為以未加密方式使用 TCP 時，才會提供此選項)
546	UDP	連線	DHCPv6 (只有當 KMA 設定為使用 DHCP 和 IPv6 時，才會提供此選項)
4045	TCP/UDP	監聽	NFS 鎖定常駐程式 (僅限 KMS 2.0)
6514	TLS over TCP	連線	遠端系統日誌 (只有在已定義遠端系統日誌伺服器並將其設定為使用 TLS 時，才會提供此選項)

注意:

必須開啟連接埠 443，客戶才能夠透過防火牆存取「服務處理器」Web 介面及「OKM 主控台」。請參閱「*Oracle Key Manager Installation and Service Manual* (internal only)」以查看 ELOM 與 ILOM 連接埠。

表格 2.3, 「ELOM/ILOM 連接埠 」 列出 KMA ELOM/ILOM 連接埠。如果來自防火牆外部的存取需要 ELOM/ILOM 的存取權，系統將會啟用這些連接埠，否則，ELOM/ILOM IP 位址就不需要啟用這些連接埠：

表格 2.3. ELOM/ILOM 連接埠

連接埠號碼	協定	方向	描述
22	TCP	監聽	SSH (適用於 ELOM/ILOM 指令行介面)
53	TCP/UDP	連線	DNS (只有在 DNS 已設定時才需要)
68	UDP	連線	當 ELOM/ILOM 需要 DHCP 時。 **注意**：雖然系統支援 DHCP 及 ELOM/ILOM，但並未提供相關文件。

80	TCP	監聽	HTTP (適用於 ELOM/ILOM Web 介面)
			
			需要使用 HTTP 時；否則，使用者可以查看如何連線至遠端主控台的指示，網址為：
			
			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	監聽/連線	SNMPv3 (可設定，此為預設連接埠)

連接埠號碼	協定	方向	描述
443	TCP/TLS	監聽	Embedded/Integrated Lights Out Manager 透過「傳輸層安全 (TLS)」之管理協定 (WS-Man) 的桌面管理工作小組 (DMTF) Web 服務
623	UDP	監聽	智慧平台管理介面 (IPMI)

3

第 3 章 安全功能

本節概述產品提供的特定安全機制。

3.1. 潛在威脅

使用加密代理程式的客戶主要關切的重點是：

- 違反原則的資訊揭露
- 資料遺失或損毀
- 發生嚴重失敗時 (例如，在持續營運的網站)，回復資料的延遲時間超過可接受範圍
- 未偵測到的資料修改。

3.2. 安全功能的目標

Oracle Key Manager 安全功能的目標為：

- 保護加密的資料以免外洩。
- 儘量降低遭受攻擊的風險。
- 提供足夠的高可靠性與可用性。

3.3. 安全模型

本節概要簡介系統所要抵禦的威脅，以及如何結合個別安全功能以避免攻擊。

提供這些保護的重要安全功能包括：

- 認證 – 確保只有經過授權的個人才能夠存取系統和資料
- 授權 – 系統權限與資料的存取控制；此存取控制以認證為基礎，可確保人員只能取得適當的權限
- 稽核 – 可讓管理員偵測到違反認證機制的嘗試，以及違反或成功的存取控制嘗試。

如需 Oracle Key Manager 安全與認證相關詳細資訊，請參閱「*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

3.4. 認證

Oracle Key Manager 架構提供所有系統元素之間的相互認證：KMA 與 KMA、代理程式與 KMA，以及使用者作業的 Oracle Key Manager GUI 或 CLI 與 KMA。

系統的每個元素 (例如，新的加密代理程式) 會在系統中註冊，方式是在 OKM 中建立 ID 與密碼詞組，然後輸入要新增的元素中。例如，當磁帶機新增至系統時，代理程式與 KMA 會根據共用密碼詞組自動執行查問/回應協定，而使得代理程式取得根憑證授權機構 (CA) 憑證與新金鑰組，以及簽署給代理程式的憑證。代理程式具有根 CA 憑證、代理程式憑證與金鑰組之後，便能執行「傳輸層安全 (TLS)」協定，用於與 KMA 的所有後續通訊。所有憑證皆為 X.509 憑證。

OKM 有如根憑證授權機構，可產生根憑證，供 KMA 用來衍生 (自我簽署) 代理程式、使用者與新 KMA 所用的憑證。

3.5. 存取控制

有下列類型的存取控制：

- 以使用者與角色為基礎的存取控制
- 仲裁保護

3.5.1. 以使用者與角色為基礎的存取控制

Oracle Key Manager 可以定義多位使用者，每位使用者具有使用者 ID 及密碼詞組。每位使用者會被授予一或多個預先定義的角色。這些角色決定了使用者在 Oracle Key Manager 系統上所能執行的作業。這些角色為：

- 安全人員 – 執行 Oracle Key Manager 安裝與管理
- 操作員 – 執行代理程式安裝與日常作業
- 相容性人員 – 定義金鑰群組並控制代理程式對於金鑰群組的存取
- 備份操作員 – 執行備份作業
- 稽核者 – 檢視系統稽核歷程檔
- 仲裁成員 – 檢視與核准擱置中的仲裁作業

在 OKM 叢集中設定 KMA 的快速啟動程序中會定義「安全人員」。之後，使用者必須使用 Oracle Key Manager GUI，以「安全人員」身分登入叢集，才能定義其他使用者。「安全人員」可選擇指派多個角色給特定單一使用者，也可選擇指派特定單一角色給多位使用者。

如需每個角色允許的作業與「安全人員」建立使用者與指派角色的詳細資訊，請參閱 Oracle Key Manager 文件庫中包含的「*Oracle Key Manager Administration Guide*」：

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

以角色為基礎的存取控制支援 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 作業角色，以分隔作業功能。

3.5.2. 仲裁保護

部分作業極為重要，需要額外的安全性。這些作業包括新增 KMA 至 OKM 叢集、解除鎖定 KMA、建立使用者與新增角色至使用者。為了實作此安全性，系統除了上述以角色為基礎的存取控制之外，也使用一組分割金鑰證明資料。

分割金鑰證明資料是由成對的使用者 ID 與密碼詞組所組成，以及系統完成特定作業所需最少數量的成對使用者 ID 與密碼詞組。分割金鑰證明資料亦稱為「仲裁」，最少數量稱為「仲裁臨界值」。

Oracle Key Manager 允許定義最多達 10 個成對的分割金鑰使用者 ID/密碼詞組，以及一個臨界值。它們是在 OKM 叢集中設定第一個 KMA 的快速啟動程序中定義的。分割金鑰使用者 ID 及密碼詞組不同於用來登入系統的使用者 ID 及密碼詞組。當使用者嘗試執行需要仲裁核准的作業時，必須有定義之臨界值數量的分割金鑰使用者與密碼詞組核准此作業，系統才會執行此作業。

3.6. 稽核

每個 KMA 會記錄執行之作業的稽核事件，包括 OKM 叢集中的代理程式、使用者及對等 KMA 發出的作業。KMA 也會在代理程式、使用者或對等 KMA 無法自身認證時記錄稽核事件。將會標示安全違規的稽核事件。認證失敗就是安全違規稽核事件的範例。若 SNMP 代理程式可在 OKM 叢集中識別，則 SNMP 代理程式發生安全違規時，KMA 也會傳送 SNMP INFORM 至這些 SNMP 代理程式。如果「遠端系統日誌」已設定，KMA 也會將這些稽核訊息轉送給已設定的伺服器。請參閱「遠端系統日誌」。

使用者必須正確登入 OKM 叢集，且必須被指派角色，才能檢視稽核事件。

KMA 會管理其稽核事件。KMA 會根據保留條件與限制 (計數) 移除較舊的稽核事件。「安全人員」可依需要修改這些保留條件與限制。

3.7. 其他安全功能

Oracle Key Manager 提供其他安全功能。如需這些功能與其他 OKM 功能的詳細資訊，請參閱「*Oracle Key Manager Overview*」：

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

3.7.1. 安全通訊

代理程式與 KMA 之間、使用者與 KMA 之間，以及 KMA 與對等 KMA 之間的通訊協定均相同。在每一種狀況中，系統都會在起始通訊的個體使用密碼詞組，以執行查問/

回應協定。若成功，將提供個體憑證及對應的私密金鑰。此憑證與私密金鑰可建立「傳輸層安全 (TLS)」(安全通訊端) 通道。系統會執行相互認證；連線的端點會彼此認證。OKM 3.1+ KMA 針對其對等複製流量一律會使用 TLS 1.2。

3.7.2. 硬體安全模組

KMA 提供可另行選購的「硬體安全模組」。此硬體安全模組 (Sun Cryptographic Accelerator (SCA) 6000 卡) 已通過 FIPS 140-2 Level 3 認證，並提供「進階加密標準 (AES)」256 位元加密金鑰 (此憑證已於 2015 年 12 月 31 日到期且未更新，後續版本將會提供替代的 HSM)。SCA 6000 卡支援 FIPS 140-2 Level 3 模式的作業，且 OKM 一律會以此模式來使用此卡。當 OKM 叢集以 FIPS 相容模式作業時，加密金鑰不會以未包裝的形式離開 SCA 6000 卡的密碼邊界。SCA 6000 卡使用 FIPS 核准的亂數產生器，如同 FIPS 186-2 DSA Random Number Generator 所指定的一般，使用 SHA-1 來產生加密金鑰。

如果 KMA 未設為使用 SCA 6000 卡，則會使用 Solaris Cryptographic Framework (SCF) PKCS#11 軟體記號來執行加密。SCF 是在 FIPS 140 模式中依據最新發行的 Solaris FIPS 140-2 安全原則所設定。

3.7.3. AES 金鑰包裝

Oracle Key Manager 使用具有 256 位元加密金鑰的 AES 金鑰包裝 (RFC 3994) 來保護對稱式金鑰的時機如下：建立對稱式金鑰時、將對稱式金鑰儲存在 KMA 時、將對稱式金鑰傳輸至代理程式時，或在金鑰傳輸檔案中傳輸對稱式金鑰時。

3.7.4. 金鑰複製

起始 OKM 叢集中的第一個 KMA 時，KMA 會產生一個大型金鑰集區。當其他 KMA 新增至叢集時，金鑰便會被複製到新的 KMA，並可用來加密資料。新增至叢集的每個 KMA 都會產生一個金鑰集區，並複製到叢集中對等的 KMA。所有 KMA 將會依需求產生新的金鑰，以維持金鑰集區的大小，並隨時供代理程式使用。當代理程式需要新的金鑰時，代理程式便會聯絡叢集中的 KMA 並要求新的金鑰。KMA 會從它的金鑰集區中取出可用的金鑰，並將此金鑰指派給代理程式的預設金鑰群組和資料單位。KMA 接著會將這些資料庫更新經由網路複製到叢集中的其他 KMA。之後，代理程式便可聯絡叢集中其他 KMA 以擷取金鑰。任何金鑰資料絕不會以文字方式在網路上傳輸。

3.7.5. Solaris FIPS 140-2 安全原則

National Institute of Standards and Technology (NIST) 於 2013 年 12 月頒發 FIPS 140-2 Level 1 驗證憑證 (編號 2061) 給 Oracle Solaris Kernel Cryptographic Framework 模組 (Solaris 11)。於 2014 年 1 月，NIST 頒發 FIPS 140-2 Level 1 驗證憑證 (編號 2076) 給 Oracle Solaris Userland Cryptographic Framework (SPARC T4 及 SPARC T5)。Oracle Key Manager 3.1.0 KMA 現在是以仍在進行 FIPS 140-2 驗證測試的 Solaris 11.3 為基礎。Oracle Key Manager 3.1.0 KMA 中的 Oracle Solaris Kernel Cryptographic Framework 是根據「*Oracle Kernel Cryptographic Framework Security Policy*」所設定。同樣地，KMA 也是根據「*Oracle Solaris Userland*

Cryptographic Framework with SPARC T4 and SPARC T5 Security Policy」所設定。當 OKM 可供使用時，將會更新為較新的 Solaris 安全原則。

3.7.6. 軟體升級

所有 KMA 軟體升級組合會經過數位簽署，以防止從未經核准的來源載入有問題的軟體。

4

第 4 章 端點

OKM 支援多種加密端點。下列為支援的端點：

- 具備加密功能的磁帶機
- Oracle Transparent Database Encryption (TDE) 11g 和更新版本
- Oracle ZFS Storage Appliance
- Oracle Solaris 11 ZFS 檔案系統

此外，端點工具可供應用程式開發人員使用，或者若使用 PKCS#11，則可以與 Oracle 資料庫的 Transparent Database Encryption (TDE) 搭配使用。

4.1. Linux PKCS#11 KMS 提供者

Linux PKCS#11 KMS 提供者適合想利用 PKCS#11 與 OKM 進行通訊的客戶使用。管理員可從 My Oracle Support 網站下載 Linux PKCS#11 KMS 提供者，並安裝在 Oracle Enterprise Linux 伺服器上。Linux PKCS#11 KMS 提供者與其他代理程式相同，具有相同的安全特性並使用 Oracle Key Manager 設備認證。Linux PKCS#11 KMS 提供者會在 */var/opt/kms/username* 目錄下儲存日誌檔與設定檔資訊。使用者和 (或) 管理員應手動或使用 logrotate 之類的公用程式管理此日誌檔。請使用適當的權限來限制 */var/opt/kms/username* 目錄的存取控制。在設定檔目錄中，代理程式的認證證明資料保留在 PKCS#12 檔案內。PKCS#12 檔案受到密碼保護。如需 Linux PKCS#11 KMS 提供者的詳細資訊，請參閱 Oracle Key Manager 文件庫中包含的「*Oracle Key Manager Administration Guide*」：

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

4.2. 適用於 Solaris 的 PKCS#11 KMS 提供者

與 PKCS#11 KMS 提供者類似的產品可搭配 Solaris 10 和 Solaris 11 使用。

4.3. JCE KMS 提供者

Java Cryptographic Environment 提供者適合想要實作 Java 用戶端應用程式 (可從 OKM 取得金鑰) 的開發人員使用。此產品已經與多項 Oracle 產品整合，您可以從「甲骨文全球開發者技術網路 (OTN)」取得本產品。

4.4. Oracle Enterprise Manager 適用的 OKM 外掛程式

Oracle Enterprise Manager (OEM) Cloud Control 適用的 Oracle Key Manager (OKM) 設備外掛程式會對 OKM 叢集進行監督。叢集所屬的每個 KMA 都會受此外掛程式監督。我們提供了此工具的安全指南。

5

第 5 章 遠端系統日誌

Oracle Key Manager 支援遠端系統日誌。您可以將 KMA 設定成使用 RFC 3164 或 RFC 5424 訊息格式，透過 TCP 以未加密的方式或透過「傳輸層安全 (TLS)」將訊息傳送至遠端系統日誌伺服器。請注意，RFC 5425 描述使用 TLS 透過 RFC 5424 訊息格式以提供安全連線來傳輸系統日誌訊息。

「安全人員」可將 KMA 設為透過 TCP 以未加密方式或透過 TLS 來傳送訊息。使用 TLS 來認證及加密 KMA 與遠端系統日誌伺服器之間的通訊會更安全。KMA 會藉由要求遠端系統日誌伺服器的憑證與公用金鑰來對其進行認證。您也可以選擇將遠端系統日誌伺服器設定為使用相互認證。相互認證可確保遠端系統日誌伺服器只接受來自已授權用戶端 (例如 KMA) 的訊息。若設定為使用相互認證，遠端系統日誌伺服器會要求 KMA 提供憑證，以驗證 KMA 的身分。

6

第 6 章 硬體管理套件

Oracle Key Manager 支援 SPARC T7-1、Netra SPARC T4-1 以及 Sun Fire X4170 M2 KMA 上的 Oracle Hardware Management Pack (HMP)。HMP 產品是 Oracle Single System Management 以及 ILOM 的成員。「安全人員」可以讓 KMA 上的 HMP 使用 Solaris 中的管理代理程式，來透過 SNMP 對 KMA 進行頻內監督。HMP 軟體為預先安裝的軟體，但會使用 SNMP 代理程式組態來加以停用。因此，啟用 HMP 之後，才會開啟 SNMP 代理程式監聽連接埠。預設會停用 HMP。

啟用 HMP 會提供下列各項功能：

- 硬體的事件通知會在以 Oracle Key Manager 特定 SNMP 通知或以 KMA 停機方式顯示之前發出。
- 可以啟用 OKM 叢集中任何或所有支援之 KMA 上的 HMP。
- 可以對 KMA 上的 SNMP MIBS (包括 MIB-II、SUN-HW-MONITORING-MIB 以及 SUN-STORAGE-MIB) 使用唯讀的 SNMP Get 作業。
- 透過 SNMP Receivelet 及 SNMP Fetchlet 進行 Oracle Red Stack 與 Oracle Enterprise Manager 的整合。

當您選擇在 KMA 上啟用 HMP 時，您應記住下列安全考量。啟用後，HMP 會執行下列動作：

- 利用 Oracle Key Manager 叢集中設定之所有已啟用的「v2c SNMP 管理程式」協定。SNMP v2c 協定沒有 SNMP v3 協定所具備的安全性增強功能。
- 在 KMA 上啟用 SNMP 管理代理程式，讓唯讀網路可以存取此 KMA 的 SNMP MIB 資訊。
- 您可以使用下列方法來降低「*Oracle Hardware Management Pack (HMP)* 安全指南」(http://docs.oracle.com/cd/E20451_01/pdf/E27799.pdf) 中指出的安全風險：
  - 「系統管理產品可用來取得一個可開機的 root 環境」- 強化 KMA 會停用系統使用者的 root 存取權。SNMP 已設定為唯讀存取權。因此，SNMP Put 作業將被拒絕。
  - 「系統管理產品包括許多功能強大的工具，需要管理員或 root 權限才能執行」- 已停用 KMA 的 root 存取權。因此，系統使用者無法執行這些工具。

附錄 A. 安全部署檢查清單

下列安全檢查清單包含協助保護金鑰管理系統的指示：

1. 在安全的實體環境中安裝每個 KMA。
2. 保護每個 KMA 上的 OpenBoot PROM 或 BIOS。
3. 保護每個 KMA 上的 Lights Out Manager。
4. 定義此 Oracle Key Manager 叢集的分割金鑰組態。
5. 適當設定每個 KMA 的自動解除鎖定設定。
6. 定義 Oracle Key Manager 使用者及其相關角色。
7. 執行最低權限的原則。
   a. 僅授予每位 Oracle Key Manager 使用者需要的角色。
8. 監督 Oracle Key Manager 叢集上的活動。
   a. 調查 Oracle Key Manager 稽核日誌中記錄的任何錯誤 (尤其是「安全違規」)。
9. 一開始定義分割金鑰組態及修改分割金鑰組態時，即備份核心安全。
10. 定期執行 Oracle Key Manager 備份。
11. 將核心安全備份檔案與 Oracle Key Manager 備份檔案存放在安全的位置。

附錄 B

附錄 B. 參考資料

- Oracle Key Manager 客戶文件

  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* (internal only)
- *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) 文件

  http://docs.oracle.com/cd/E37444_01/
- SPARC T7-1 伺服器文件 https://docs.oracle.com/cd/E54976_01/
- Netra SPARC T4-1 伺服器文件

  http://docs.oracle.com/cd/E23203_01/
- Oracle Hardware Management Pack 文件
  - Oracle Hardware Management Pack 文件庫

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

    http://www.oracle.com/technetwork/server-storage/servermgmt/overview/index.html
- NIST 文件：
  - *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 產品的安全原則文件：
  - *Oracle Solaris Kernel Cryptographic Framework Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2061.pdf
  - *Oracle Solaris Kernel Cryptographic Framework with SPARC T4 and T5 Security Policy*

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

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1050.pdf
  - *Oracle StorageTek T10000D Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2254.pdf
  - *Oracle StorageTek T10000C Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1561.pdf
  - *Oracle StorageTek T10000B Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1156.pdf
  - *Oracle StorageTek T10000A Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1157.pdf
  - *Oracle StorageTek T9480D Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1288.pdf
- Oracle 產品的 FIPS 驗證憑證：
  - Sun Crypto Accelerator 6000 - 憑證編號 1026 (已過期)

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