Oracle® Key Manager 3

Sicherheitshandbuch

Release 3.1

E52205-02

April 2016

ORACLE®

Oracle® Key Manager 3
Sicherheitshandbuch

E52205-02

Inhalt

Tabellen

Vorwort

In diesem Dokument werden die Sicherheitsfunktionen von Oracle Key Manager 3 (OKM 3) beschrieben.

Zielgruppe

Dieses Handbuch richtet sich an Personen, die an der Verwendung von Sicherheitsfunktionen und der sicheren Installation und Konfiguration von OKM 3 beteiligt sind.

Barrierefreie Dokumentation

Informationen über Eingabehilfen für die Dokumentation finden Sie auf der Oracle Accessibility Program-Webseite unter http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Zugang zum Oracle-Support
Oracle-Kunden mit einem gültigen Oracle-Supportvertrag haben Zugriff auf elektronischem Support über My Oracle Support. Weitere Informationen erhalten Sie unter http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info oder unter http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs, falls Sie eine Hörbehinderung haben.

1

Kapitel 1. Überblick

Dieser Abschnitt enthält einen Überblick über das Produkt und erläutert die allgemeinen Grundsätze der Appliance-Sicherheit.

1.1. Produktüberblick

Oracle Key Manager (OKM) erstellt, speichert und verwaltet Verschlüsselungsschlüssel. Er besteht aus folgenden Komponenten:

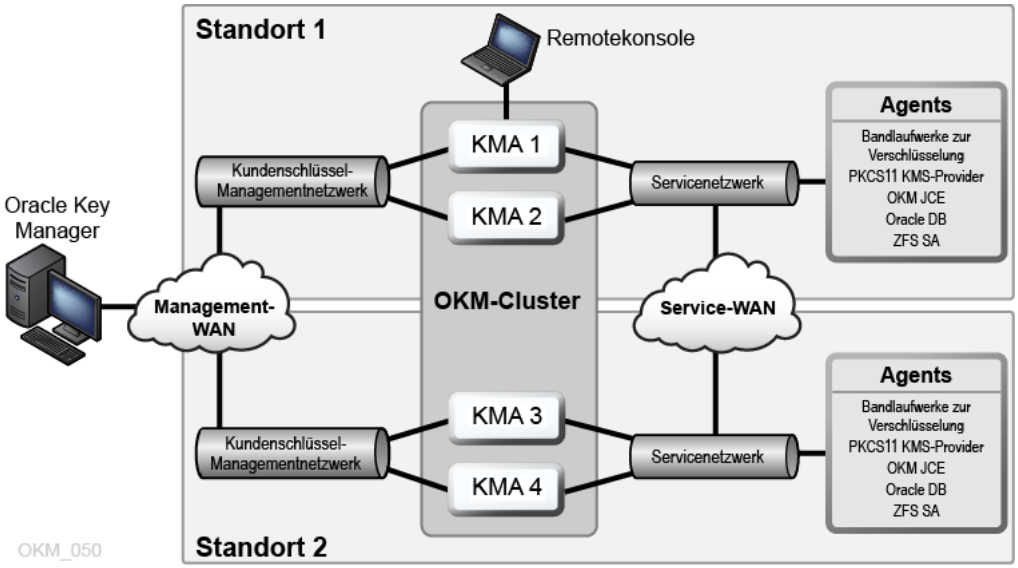
- Key Management Appliance (KMA) - Ein gehärtetes Gehäuse, das grundsatzbasiertes Lifecycle Key Management, Authentifizierung, Zugangskontrolle und Schlüsselbereitstellungsdienste bietet. Als vertrauenswürdige Authority für Speichernetzwerke stellt die KMA sicher, dass alle Speichergeräte registriert und authentifiziert sind und dass alle Verschlüsselungsschlüssel in Übereinstimmung mit vorgegebenen Richtlinien erstellt, bereitgestellt und gelöscht werden.
- Oracle Key Manager-GUI - Eine grafische Benutzeroberfläche, die auf einer Workstation ausgeführt wird und mit der KMA über ein IP-Netzwerk kommuniziert, um den OKM zu konfigurieren und zu verwalten. Die Oracle Key Manager GUI muss auf einer vom Kunden bereitgestellten Workstation installiert werden.
- Oracle Key Manager-CLIs - Zwei Befehlszeilenschnittstellen, die auf einer Workstation ausgeführt werden und mit der KMA über ein IP-Netzwerk kommunizieren, um gemeinsam herausgegebene Administrationsvorgänge zu automatisieren. Die Oracle Key Manager-CLIs müssen auf einer vom Kunden bereitgestellten Workstation installiert werden.
- OKM-Cluster - Die gesamte Gruppe von KMAs im System. Die KMAs sind miteinander verbunden und replizieren Informationen untereinander.
- Agent - Ein Gerät oder eine Software, das oder die mithilfe von vom OKM-Cluster verwalteten Schlüsseln die Verschlüsselung durchführt. Ein StorageTek-Bandlaufwerk zur Verschlüsselung ist ein Beispiel für einen Agent. Agents kommunizieren mit KMAs mithilfe des KMS Agent-Protokolls. Die Agent-API ist eine Gruppe von Softwareschnittstellen, die in die Agent-Hardware oder -Software integriert ist.

Der OKM verwendet ein TCP/IP-Netzwerk für die Verbindungen zwischen KMAs, Agents und Workstations, auf denen die Oracle Key Manager GUI und CLIs ausgeführt werden. Um flexible Netzwerkverbindungen bereitzustellen, gibt es auf jeder KMA drei Schnittstellen für Netzwerkverbindungen:

- Die Managementverbindung - Für die Verbindung zum Kundennetzwerk vorgesehen
- Die Serviceverbindung - Für die Verbindung zu den Agents vorgesehen
- Die ILOM/ELOM-Verbindung - Für die Verbindung zum ILOM oder ELOM auf der KMA vorgesehen

Siehe das Beispiel in der folgenden Abbildung:

Abbildung 1.1.



1.2. Allgemeine Sicherheitsgrundsätze

Die folgenden Grundsätze sind für die sichere Verwendung jeder Anwendung von wesentlicher Bedeutung.

1.2.1. Software immer auf dem neuesten Stand halten

Einer der Grundsätze für einen sicheren Betrieb besteht darin, alle Softwareversionen und Patches auf dem neuesten Stand zu halten. Die aktuellen Oracle Key Manager-Upgradepakete und -Installationsprogramme stehen auf der My Oracle Support-Website zur Verfügung: `http://support.oracle.com`.

1.2.2. Begrenzen des Netzwerkzugriffs auf kritische Services

Schützen Sie Ihre Geschäftsanwendungen mit einer Firewall. Die Firewall bietet die Gewähr, dass der Zugriff auf diese Systeme auf eine bekannte Netzwerkroute beschränkt ist, die gegebenenfalls überwacht und eingeschränkt werden kann. Als Alternative kann ein Firewallrouter anstelle von mehreren, unabhängigen Firewalls verwendet werden.

1.2.3. Prinzip der geringsten Rechte

Das Prinzip der geringsten Rechte bedeutet, dass Benutzern so wenige Berechtigungen wie möglich zur Ausführung ihrer Aufgaben erteilt werden. Zu ambitioniertes Zuweisen von Verantwortlichkeiten, Rollen, Zugriffsrechten und so weiter (insbesondere in den frühen Stadien einer Organisation), wenn der Personalbestand klein ist und Arbeiten schnell erledigt werden sollen, kann oftmals dazu führen, dass ein System für Missbrauch offen steht. Benutzerrechte müssen in regelmäßigen Abständen geprüft werden, um ihre Relevanz in Bezug auf berufliche Verantwortungsbereiche zu bestimmen.

1.2.4. Überwachen der Systemaktivität

Systemsicherheit steht auf drei Beinen: gute Sicherheitsprotokolle, richtige Systemkonfiguration und Systemüberwachung. Diese dritte Anforderung wird durch Auditing und Prüfung von Auditdatensätzen erfüllt. Jede Komponente innerhalb eines Systems verfügt zu einem gewissen Grad über Überwachungsmöglichkeiten. Befolgen der Audithinweise in diesem Dokument und regelmäßiges Überwachen von Auditdatensätzen.

1.2.5. Sicherheitsinformationen immer auf dem neuesten Stand halten

Oracle nimmt fortwährend Verbesserungen an Software und Dokumentation vor. Prüfen Sie jährlich die My Oracle Support-Website auf Revisionen.

2

Kapitel 2. Sichere Installation und Konfiguration

In diesem Abschnitt werden die Schritte bei der Planung einer sicheren Installation aufgeführt. Außerdem werden verschiedene empfohlene Deployment-Topologien für die Systeme beschrieben.

2.1. Analysieren der Umgebung

Die folgenden Punkte helfen Ihnen, ein besseres Verständnis Ihrer Sicherheitsanforderungen zu erlangen:

2.1.1. Welche Ressourcen werden geschützt?

Viele Ressourcen in der Production-Umgebung können geschützt werden. Bei der Entscheidung über die erforderliche Sicherheitsstufe berücksichtigen Sie die Ressourcen, die geschützt werden müssen.

Die primären zu sichernden Ressourcen sind in der Regel Ihre Daten. Im Folgenden werden weitere Ressourcen aufgeführt, da sie mit der Verwaltung und dem Schutz Ihrer Daten verknüpft sind. Beim Datenschutz geht es darum, vor Datenverlust (also der Nichtverfügbarkeit von Daten) und vor Verletzung von Daten oder vor Offenbarung von Daten gegenüber Unbefugten zu schützen.

Zum Schutz von Daten vor der Offenbarung gegenüber Unbefugten werden oft kryptographische Schlüssel verwendet. Deshalb sind sie eine weitere Ressource, die geschützt werden muss. Hochzuverlässiges Schlüsselmanagement ist bei der Verwaltung von hochverfügbaren Daten äußerst wichtig. Eine weitere Gruppe von zu schützenden Ressourcen sind Assets innerhalb des Oracle Key Manager-Clusters selbst, einschließlich der Key Management Appliances.

2.1.2. Vor wem werden die Ressourcen geschützt?

Diese Ressourcen müssen vor jeder Person geschützt werden, die über keine Zugriffsberechtigung verfügt. Diese Ressourcen müssen physisch geschützt werden. Überlegen Sie, welche Ihrer Mitarbeiter Zugang zu diesen Ressourcen haben sollen. Geben Sie dann an, welche Art Vorgänge jeder Mitarbeiter in der Oracle Key Manager-Umgebung herausgeben kann.

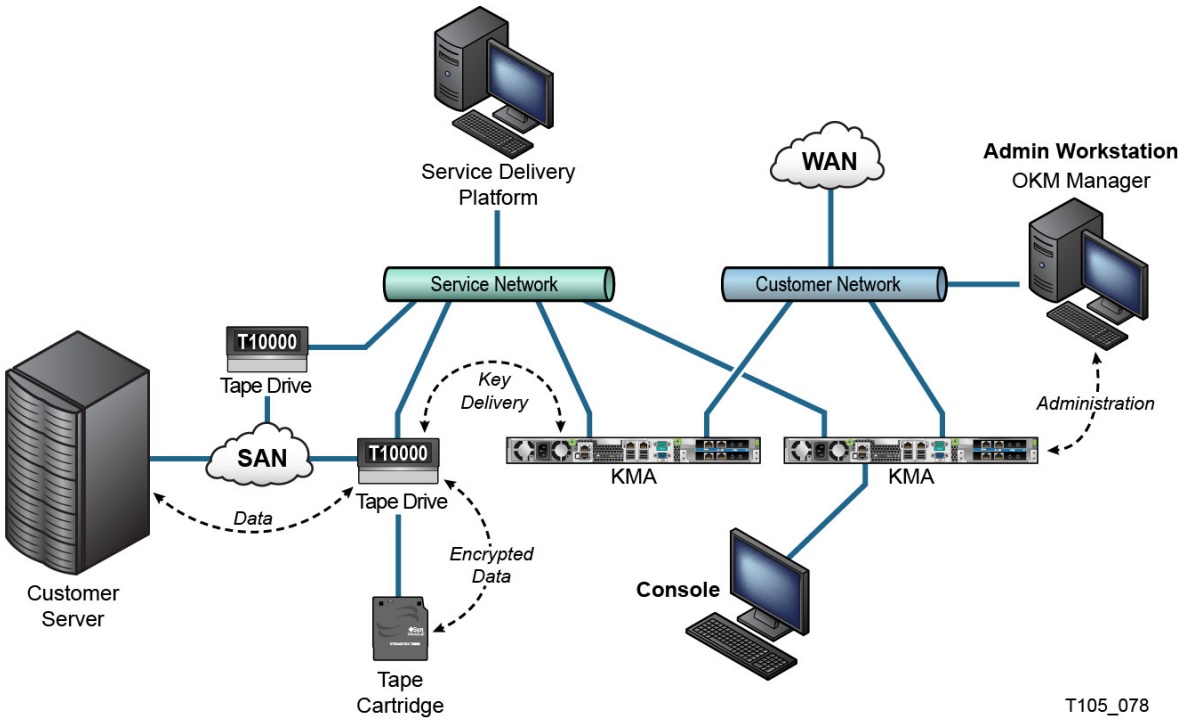
2.1.3. Was geschieht, wenn der Schutz bei strategischen Ressourcen versagt?

In einigen Fällen kann ein Fehler in Ihrem Sicherheitsschema einfach entdeckt und nur als eine Unannehmlichkeit eingestuft werden. In anderen Fällen kann ein Fehler großen Schaden für Unternehmen oder einzelne Kunden anrichten, die Ihre Ressourcen verwenden. Wenn Sie die Sicherheitsauswirkungen jeder Ressource kennen, können Sie diese richtig schützen.

2.2. Empfohlene Deployment-Topologien

Die folgende Abbildung zeigt eine typische Bereitstellung einer Oracle Key Manager-Lösung.

Abbildung 2.1. Typische Bereitstellung einer OKM-Lösung



2.3. Installieren einer Key Management Appliance (KMA)

In diesem Abschnitt wird die sichere Installation und Konfiguration einer OKM Key Management Appliance beschrieben.

KMAs werden als gehärtete Appliances mit verfügbarer Oracle Key Manager-Funktionalität hergestellt.

Die Installation und Konfiguration von KMAs in einem OKM-Cluster umfasst folgende Schritte:

1. Installieren Sie jede KMA in einem Rack.
2. Sichern Sie den ILOM jeder KMA.
3. Konfigurieren Sie die erste KMA im OKM-Cluster.
4. Fügen Sie weitere KMAs zum OKM-Cluster hinzu.

Weitere Informationen zur Planung des Deployments eines OKM-Clusters finden Sie in *Oracle Key Manager - Übersichts- und Planungshandbuch*.

2.3.1. Installieren einer KMA in einem Rack

Eine KMA wird von einem Oracle Customer Service Engineer in einem Rack installiert, wie in *Oracle Key Manager - Installations- und Servicehandbuch* beschrieben. Dieses Handbuch bietet Oracle-Kundendienstmitarbeitern ausführlichere Informationen.

2.3.2. Sichern des ILOM einer KMA

Oracle Key Manager-KMAs werden mit aktueller ILOM-Firmware hergestellt. Der ILOM einer KMA muss entweder von einem Oracle Customer Service Engineer oder vom Kunden gesichert werden. Der ILOM muss außerdem nach einem Upgrade der ELOM- oder ILOM-Firmware gesichert werden.

Für das Sichern des ILOM müssen bestimmte ILOM-Einstellungen festgelegt werden, um Änderungen am ILOM zu verhindern, die die Sicherheit beeinträchtigen können. Weitere Anweisungen finden Sie im Abschnitt über die ILOM-Sicherheitshärtung im Anhang "Serviceprozessorprozeduren" des *Oracle Key Manager - Administrationshandbuchs*.

2.3.3. Konfigurieren der ersten KMA in einem OKM-Cluster

Stellen Sie vor dem Konfigurieren der ersten KMA zunächst die Schlüsselaufteilungszugangsdaten und in diesem OKM-Cluster zu definierende Benutzer-IDs und Passphrases heraus. Dazu können Sie ein Arbeitsblatt verwenden, wie das Arbeitsblatt in *Oracle Key Manager - Installations- und Servicehandbuch* (nur intern). Wenden Sie sich dazu an den zuständigen Oracle Support-Ansprechpartner.

Geben Sie dem entsprechenden Personal diese Schlüsselaufteilungszugangsdaten, Benutzer-IDs und Passphrases. Weitere Informationen finden Sie unter "Quorumschutz" im weiteren Verlauf des Dokuments.

Hinweis:

Bewahren Sie diese Schlüsselaufteilungszugangsdaten, Benutzer-IDs und Passphrases an einem sicheren Ort auf.

Öffnen Sie einen Webbrowser, starten Sie die Remotekonsole, und starten Sie dann das OKM QuickStart-Dienstprogramm in der Remotekonsole. Um das OKM-Cluster in dieser KMA zu initialisieren, folgen Sie den unter "Initialisieren des Clusters" beschriebenen Anweisungen im *Oracle Key Manager - Administrationshandbuch* in den Oracle Key Manager-Dokumentationsbibliotheken.

Die Schlüsselaufteilungszugangsdaten und ein Benutzer mit Berechtigungen für Sicherheitsbeauftragte werden in diesem Verfahren definiert. Nach Abschluss des QuickStart-Vorgangs muss der Sicherheitsbeauftragte sich bei der KMA anmelden und weitere OKM-Benutzer definieren.

2.3.4. Aspekte beim Definieren von Schlüsselaufteilungszugangsdaten

Das Definieren von weniger Benutzer-IDs und Passphrases für die Schlüsselaufteilung und ein niedrigerer Schwellenwert sind praktischer, aber weniger sicher. Das Definieren von mehr Benutzer-IDs und Passphrases für die Schlüsselaufteilung und ein höherer Schwellenwert sind weniger praktisch, aber sicherer.

2.3.5. Aspekte beim Definieren von zusätzlichen OKM-Benutzern

Das Definieren von weniger OKM-Benutzern, von denen einigen mehrere Rollen zugewiesen wurden, ist praktischer, aber weniger sicher. Das Definieren von mehr OKM-Benutzern, von denen den meisten nur eine Rolle zugewiesen wurde, ist weniger praktisch, aber sicherer, da so die von bestimmten OKM-Benutzern durchgeführten Vorgänge besser verfolgt werden können.

2.3.6. Hinzufügen von weiteren KMAs zum OKM-Cluster

Öffnen Sie einen Webbrowser, starten Sie die Remotekonsole, und starten Sie dann das OKM QuickStart-Dienstprogramm in der Remotekonsole. Um diese KMA zu dem OKM-Cluster hinzuzufügen, befolgen Sie die entsprechende Prozedur in *Oracle Key Manager - Administrationshandbuch* unter:

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

2.3.7. Aspekte beim Hinzufügen von zusätzlichen KMAs

Oracle Key Manager bietet als praktische Option das autonome Entsperren der einzelnen KMAs. Diese Option wird während des QuickStart-Vorgangs für die erste und weitere KMAs in einem Cluster definiert und kann später von einem Sicherheitsbeauftragten geändert werden.

Wenn die Option zum autonomen Entsperren aktiviert ist, hebt die KMA beim Starten automatisch ihre Sperre auf und kann umgehend Schlüssel bereitstellen, ohne dass die Quorumgenehmigung erforderlich ist. Wenn das autonome Entsperren deaktiviert ist, bleibt die KMA beim Starten gesperrt und stellt erst dann Schlüssel bereit, wenn der Sicherheitsbeauftragte die Entsperrung anfordert und ein Quorum diese Anforderung genehmigt.

Um maximale Sicherheit zu gewährleisten, rät Oracle davon ab, das autonome Entsperren zu aktivieren. Weitere Informationen zur Option für autonomes Entsperren finden Sie in *Oracle Key Manager Version 2.x - Whitepaper zu Sicherheit und Authentifizierung* unter:

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

2.3.8. Eigenschaften von gehärteten KMAs

Wie oben angegeben, werden KMAs als gehärtete Appliances mit verfügbarer Oracle Key Manager-Funktionalität hergestellt. Sie haben wie gehärtete Appliances folgende Eigenschaften:

- Nicht erforderliche Solaris-Pakete sind nicht im Solaris-Image vorhanden. Beispiel: FTP- und Telnet-Dienste sowie Dienstprogramme werden nicht im Solaris-Image angezeigt.
- KMAs erstellen keine Core-Dateien.
- Das standardmäßige Solaris Login(1)-Dienstprogramm wurde durch die OKM-Konsole ersetzt. Deshalb können sich Benutzer nicht bei der Solaris-Konsole anmelden.
- Der SSH-Service ist standardmäßig deaktiviert. Zu Kundendienstzwecken kann der Sicherheitsbeauftragte den SSH-Service aktivieren und ein Supportkonto für einen begrenzten Zeitraum definieren. Dieses Supportkonto ist das einzige verfügbare Konto und verfügt über begrenzten Zugang und eingeschränkte Berechtigungen. Beim Solaris-Auditing werden Befehle verfolgt, die vom Supportkonto aufgerufen werden.
- Das Root-Konto ist deaktiviert und als Rolle konfiguriert.
- KMAs sind nicht mit einem DVD-Laufwerk ausgestattet.
- USB-Anschlüsse werden wirksam deaktiviert.
- Nicht verwendete Netzwerkanschlüsse werden geschlossen.
- Nicht-ausführbare Stacks werden aktiviert.
- Zufällige Adressbereichssuche ist konfiguriert.
- Nicht-ausführbare Heaps sind aktiviert.
- ZFS-Verschlüsselung wird für sicherheitsrelevante Dateisysteme verwendet.
- Solaris ist gemäß der SCAP PCI-DSS-Benchmark konfiguriert.
- Nicht erforderliche SMF-Services sind deaktiviert.
- Oracle Solaris Verified Boot kann auf SPARC T7-1-basierten KMAs konfiguriert werden, um den Boot-Prozess des Systems zu sichern und vor Beschädigung der Kernel-Module, Einfügen von Root-Kits oder anderen böswilligen Programmen zu schützen.

- Die neueren KMAs, die auf SPARC T7-1- und Netra SPARC T4-1-Servern basieren, sind originalgesichert (ILOM-Fehler), wodurch der Zugriff auf die Gehäusetür bei vorhandener Stromzufuhr offensichtlich wird.
- Die ILOM 3.2-Firmware ist jetzt für FIPS 140-2 Level 1 zertifiziert und kann im FIPS-Modus konfiguriert werden.
- Das Basis-Audit- und -Report-Tool wird in regelmäßigen Abständen im Hinblick auf forensische Verfahren ausgeführt. Diese Berichte sind in den OKM-Systemdumps enthalten.
- Das Solaris Cryptographic Security Framework ist gemäß FIPS 140-2 Level 1-Sicherheitsrichtlinien (die für Solaris 11.1 dokumentiert sind) mit oder ohne Vorhandensein eines Hardware Security Modules konfiguriert.

2.4. TCP/IP-Verbindungen und die KMA

Wenn zwischen den Entitys (OKM-Manager, Agents und anderen KMAs in demselben Cluster) und der KMA eine Firewall vorhanden ist, muss die Firewall zulassen, dass die Entity TCP/IP-Verbindungen zu den folgenden Ports innerhalb der KMA herstellt:

- OKM-Manager-zu-KMA-Kommunikation erfordert die Ports 3331, 3332, 3333, 3335.
- Agent-zu-KMA-Kommunikation erfordert die Ports 3331, 3332, 3334, 3335.
- KMA-zu-KMA-Kommunikation erfordert die Ports 3331, 3332, 3336.

Hinweis:

Für Benutzer, die ihre KMAs zur Verwendung von IPv6-Adressen konfigurieren, konfigurieren Sie IPv4-basierte Edgefirewalls, um alle ausgehenden IPv4-Protokoll-41-Pakete und UDP-Port-3544-Pakete zu löschen und so zu verhindern, dass IPv6-über-IPv4-Tunneldatenverkehr interne Hosts erreicht.

Weitere Einzelheiten finden Sie in der Dokumentation zur Firewallkonfiguration. Tabelle 2.1, „KMA-Portverbindungen“ führt Ports auf, die KMAs explizit verwenden oder Ports, an denen KMAs Services bereitstellen.

Tabelle 2.1. KMA-Portverbindungen

Portnummer	Protokoll	Richtung	Beschreibung
22	TCP	Listening	SSH (nur wenn Technischer Support aktiviert ist)
123	TCP/UDP	Listening	NTP
3331	TCP	Listening	OKM-CA-Service
3332	TCP	Listening	OKM-Zertifikatsservice
3333	TCP	Listening	OKM-Managementservice
3334	TCP	Listening	OKM-Agent-Service
3335	TCP	Listening	OKM-Discovery-Service
3336	TCP	Listening	OKM-Replikationsservice

Tabelle 2.2, „Andere Services“ zeigt andere Services, die auf Ports hören, die möglicherweise nicht verwendet werden.

Tabelle 2.2. Andere Services

Portnummer	Protokoll	Richtung	Beschreibung
53	TCP/UDP	Verbindung wird hergestellt	DNS (nur wenn KMA zur Verwendung von DNS konfiguriert ist)
68	UDP	Verbindung wird hergestellt	DHCP (nur wenn KMA zur Verwendung von DHCP konfiguriert ist)
111	TCP/UDP	Listening	RPC (KMAs antworten auf rpcinfo-Abfragen). Dieser Port ist nur bei KMS 2.1 und früher für externe Anforderungen geöffnet.
161	UDP	Verbindung wird hergestellt	SNMP (nur wenn SNMP-Manager definiert sind)
161	UDP	Listening	SNMP (nur wenn Hardware Management Pack aktiviert ist)
514	TCP	Verbindung wird hergestellt	Remote-Syslog (nur wenn Remote-Syslog-Server definiert und zur Verwendung von TCP unverschlüsselt konfiguriert sind)
546	UDP	Verbindung wird hergestellt	DHCPv6 (nur wenn KMA zur Verwendung von DHCP und IPv6 konfiguriert ist)
4045	TCP/UDP	Listening	NFS Lock Daemon (nur KMS 2.0)
6514	TLS über TCP	Verbindung wird hergestellt	Remote-Syslog (nur wenn Remote-Syslog-Server definiert und zur Verwendung von TLS konfiguriert sind)

Hinweis:

Port 443 muss geöffnet sein, damit Kunden auf die Serviceprozessor-Weboberfläche und die OKM-Konsole über die Firewall zugreifen können. Im *Oracle Key Manager - Installations- und Servicehandbuch* (nur intern) werden die ELOM- und ILOM-Ports aufgeführt.

In Tabelle 2.3, „ELOM-/ILOM-Ports“ werden die ELOM-/ILOM-Ports von KMA aufgeführt. Diese Ports würden aktiviert, wenn von außerhalb der Firewall auf ELOM/ILOM zugegriffen werden muss; sonst müssen sie für die ELOM-/ILOM-IP-Adresse nicht aktiviert werden:

Tabelle 2.3. ELOM-/ILOM-Ports

Portnummer	Protokoll	Richtung	Beschreibung
22	TCP	Listening	SSH (für ELOM-/ILOM-Befehlszeilenoberfläche)
53	TCP/UDP	Verbindung wird hergestellt	DNS (nur erforderlich, wenn DNS konfiguriert ist)
68	UDP	Verbindung wird hergestellt	Wenn DHCP für ELOM/ILOM benötigt wird. **Hinweis**: Dokumentation für DHCP und ELOM/ILOM ist nicht verfügbar, auch wenn diese unterstützt werden.
80	TCP	Listening	HTTP (für die ELOM-/ILOM-Weboberfläche) Wenn HTTP erforderlich ist; sonst können Benutzer die Anweisungen zur Verbindung zu der Remotekonsole aufrufen unter: ELOM:

Portnummer	Protokoll	Richtung	Beschreibung
			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	Listening/ Verbindung wird hergestellt	SNMPv3 (konfigurierbar, dies ist der Standardport)
443	TCP /TLS	Listening	Embedded/Integrated Lights Out Manager Desktop Management Task Force-(DMTF-)Webservices für Management Protocol (WS-Man) über Transport Layer Security (TLS)
623	UDP	Listening	Intelligent Platform Management Interface (IPMI)

3

Kapitel 3. Sicherheitsfunktionen

In diesem Abschnitt werden die spezifischen Sicherheitsverfahren beschrieben, die das Produkt bietet.

3.1. Potenzielle Bedrohungen

Kunden mit verschlüsselungsfähigen Agents sorgen sich hauptsächlich um:

- Richtlinienverletzende Offenbarung von Informationen
- Verlust oder Zerstörung von Daten
- Inakzeptable Verzögerungen bei der Wiederherstellung von Daten bei fatalem Ausfall (Beispiel: bei einem Notfallsystem)
- Nicht erkannte Änderung von Daten

3.2. Ziele der Sicherheitsfunktionen

Die Ziele der Sicherheitsfunktionen von Oracle Key Manager sind:

- Schutz verschlüsselter Daten vor der Offenbarung.
- Minimierung des Angriffsrisikos.
- Ausreichend hohe Zuverlässigkeit und Verfügbarkeit.

3.3. Das Sicherheitsmodell

Dieser Abschnitt des Sicherheitshandbuchs soll einen umfassenden Überblick über die Bedrohungen geben, für die das System konzipiert wurde, und darüber, wie die einzelnen Sicherheitsfunktionen zusammen Angriffe abwehren.

Folgende kritische Sicherheitsfunktionen bieten diesen Schutz:

- Authentifizierung - Stellt sicher, dass nur autorisierte Personen auf das System und die Daten zugreifen können.
- Autorisierung - Zugangskontrolle auf Systemberechtigungen und Daten. Diese Zugangskontrolle baut auf der Authentifizierung auf, um sicherzustellen, dass Einzelpersonen ausschließlich den für sie angemessenen Zugang erhalten.
- Audit - Beim Audit können Administratoren versuchte Verletzungen des Authentifizierungsverfahrens und versuchte oder erfolgreiche Verletzungen der Zugriffskontrolle erkennen.

Weitere Informationen zum Sicherheits- und Authentifizierungsaspekt von Oracle Key Manager finden Sie in *Oracle Key Manager Version 2.x - Whitepaper zu Sicherheit und Authentifizierung* unter:

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

3.4. Authentifizierung

Die Oracle Key Manager-Architektur sorgt für die gegenseitige Authentifizierung zwischen allen Elementen des Systems: KMA zu KMA, Agent zu KMA und Oracle Key Manager GUI zu CLI zu KMA für Benutzervorgänge.

Jedes Element des Systems (zum Beispiel ein neuer Verschlüsselungs-Agent) wird beim System registriert, indem eine ID und eine Passphrase in OKM erstellt werden, die dann im hinzuzufügenden Element eingegeben werden. Beispiel: Wenn dem System ein Bandlaufwerk hinzugefügt wird, führen der Agent und die KMA automatisch ein Challenge-/Antwortprotokoll basierend auf der gemeinsamen Passphrase aus, durch das der Agent das Root Certificate Authority (CA)-Zertifikat, ein neues Schlüsselpaar und ein signiertes Zertifikat für den Agent erhält. Nach dem Erstellen von Root CA-Zertifikat, Agent-Zertifikat und Schlüsselpaar kann der Agent das Transport Layer Security (TLS)-Protokoll für alle nachfolgenden Kommunikationen mit der KMA ausführen. Alle Zertifikate sind X.509-Zertifikate.

Der OKM dient als Root-Zertifizierungsstelle, die ein Root-Zertifikat erstellt, das KMAs wiederum zur Ableitung (selbstsigniert) von Zertifikaten verwenden, die von anderen Agents, Benutzern und neuen KMAs genutzt werden.

3.5. Zugriffskontrolle

Es gibt folgende Arten von Zugriffskontrolle:

- Benutzer- und rollenbasierte Zugriffskontrolle
- Quorumschutz

3.5.1. Benutzer- und rollenbasierte Zugriffskontrolle

Oracle Key Manager bietet die Möglichkeit, mehrere Benutzer mit je einer ID und Passphrase zu definieren. Jedem Benutzer wird mindestens eine vordefinierte Rolle zugewiesen. Diese Rollen bestimmen, welche Vorgänge ein Benutzer auf einem Oracle Key Manager-System durchführen darf. Diese Rollen sind:

- Sicherheitsbeauftragter - Richtet Oracle Key Manager ein und verwaltet es
- Bediener - Richtet den Agent ein und führt alltägliche Vorgänge durch

- Compliance-Mitarbeiter - Definiert Schlüsselgruppen und kontrolliert den Agent-Zugriff auf Schlüsselgruppen
- Backupoperator - Führt Backupvorgänge durch
- Auditor - Überprüft Audittrails des Systems
- Quorummitglied - Überprüft und genehmigt ausstehende Quorumvorgänge

Ein Sicherheitsbeauftragter wird während des QuickStart-Prozesses definiert, bei dem eine KMA in einem OKM-Cluster eingerichtet wird. Später muss sich ein Benutzer über die Oracle Key Manager-GUI als Sicherheitsbeauftragter beim Cluster anmelden, um weitere Benutzer zu definieren. Der Sicherheitsbeauftragte kann wahlweise einem bestimmten Benutzer mehrere Rollen oder eine bestimmte Rolle mehreren Benutzern zuweisen.

Weitere Informationen über die zulässigen Vorgänge der einzelnen Rollen und darüber, wie ein Sicherheitsbeauftragter Benutzer erstellt und ihnen Rollen zuweist, finden Sie im *Oracle Key Manager - Administrationshandbuch* in den Oracle Key Manager-Dokumentationsbibliotheken unter:

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

Diese rollenbasierte Zugriffskontrolle unterstützt die betrieblichen Rollen der National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 zur Abgrenzung von betrieblichen Funktionen.

3.5.2. Quorumschutz

Für einige Vorgänge ist wegen ihrer kritischen Natur eine zusätzliche Sicherheitsebene erforderlich. Zu diesen Vorgängen gehören das Hinzufügen einer KMA zu einem OKM-Cluster, das Entsperren einer KMA, das Erstellen von Benutzern und das Hinzufügen von Rollen zu Benutzern. Zur Implementierung dieser Sicherheitsebene wird vom System neben dem oben beschriebenen rollenbasierten Zugriff eine Gruppe von Schlüsselaufteilungszugangsdaten verwendet.

Schlüsselaufteilungszugangsdaten bestehen aus einer Gruppe von Benutzer-ID- und Passphrase-Paaren und der Mindestanzahl an Paaren, die erforderlich sind, damit das System bestimmte Vorgänge abschließen kann. Die Schlüsselaufteilungszugangsdaten werden auch als "Quorum" bezeichnet, und die Mindestanzahl wird "Quorumschwellenwert" genannt.

In Oracle Key Manager können bis zu 10 Benutzer-ID-/Passphrase-Paare zur Schlüsselaufteilung und ein Schwellenwert festgelegt werden. Sie werden während des QuickStart-Prozesses bei der ersten Konfiguration der KMA in einem OKM-Cluster definiert. Die Benutzer-IDs und Passphrases für die Schlüsselaufteilung unterscheiden sich von denen zur Anmeldung beim System. Wenn ein Benutzer einen Vorgang durchführen möchte, für den eine Quorumgenehmigung erforderlich ist, muss dieser Vorgang vom definierten Schwellenwert der Benutzer-IDs und Passphrases für die Schlüsselaufteilung genehmigt werden, bevor das System diesen Vorgang durchführt.

3.6. Audits

Jede KMA protokolliert Auditereignisse für von ihr durchgeführte Vorgänge, einschließlich der Ereignisse, die von Agents, Benutzern und anderen KMAs im OKM-Cluster ausgegeben wurden. KMAs protokollieren auch Auditereignisse, wenn ein Agent, Benutzer oder eine andere KMA sich nicht selbst authentifiziert. Auditereignisse, die auf eine Sicherheitsverletzung hinweisen, werden festgehalten. Die Nichtauthentifizierung ist ein Beispiel eines Auditereignisses, das auf eine Sicherheitsverletzung hinweist. Wenn SNMP-Agents im OKM-Cluster identifiziert werden, senden KMAs außerdem SNMP INFORMs an diese SNMP-Agents, sobald sie eine Sicherheitsverletzung erkennen. Wenn "Remote-Syslog" konfiguriert ist, leitet eine KMA auch diese Auditnachrichten an konfigurierte Server weiter. Siehe "*Remote-Syslog*".

Ein Benutzer muss sich ordnungsgemäß beim OKM-Cluster anmelden, und ihm muss eine Rolle zugewiesen sein, damit er in der Lage ist, Auditereignisse anzuzeigen.

KMAs verwalten ihre Auditereignisse. KMAs entfernen ältere Auditereignisse basierend auf Aufbewahrungsbedingungen und -begrenzungen (Anzahl). Diese Aufbewahrungsbedingungen und -begrenzungen können vom Sicherheitsbeauftragten nach Bedarf geändert werden.

3.7. Sonstige Sicherheitsfunktionen

Oracle Key Manager bietet noch weitere Sicherheitsfunktionen. Weitere Informationen darüber und über sonstige OKM-Funktionen finden Sie in *Oracle Key Manager - Überblick* unter:

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

3.7.1. Sichere Kommunikation

Das Kommunikationsprotokoll zwischen einem Agent und einer KMA, einem Benutzer und einer KMA ist dasselbe wie zwischen einer KMA und einer Peer-KMA. In beiden Fällen verwendet das System die Passphrase für die Entity, die die Kommunikation initiiert, um ein Challenge-/Antwortprotokoll durchzuführen. Verläuft dieser Vorgang erfolgreich, erhält die Entity ein Zertifikat und den dazugehörigen privaten Schlüssel. Dieses Zertifikat und der zugehörige private Schlüssel können einen Transport Layer Security (TLS) 1.0 (Secure Sockets) Kanal einrichten. Die gegenseitige Authentifizierung wird durchgeführt, sodass jedes Verbindungsende die jeweils andere Partei authentifiziert. OKM 3.1+ KMAs verwenden immer TLS 1.2 für den Peer-zu-Peer-Replikationsdatenverkehr.

3.7.2. Hardware Security Module

Für KMAs steht ein Hardware Security Module zur Verfügung, dass separat bestellt werden kann. Dieses Hardware Security Module - eine Sun Cryptographic Accelerator (SCA)

6000-Karte - war für FIPS 140-2 Level 3 zertifiziert und stellt Advanced Encryption Standard (AES) 256-Bit-Verschlüsselungschlüssel bereit (dieses Zertifikat ist am 31 .12.2015 abgelaufen und wird nicht erneuert. Ein alternatives HSM wird in einem nachfolgenden Release bereitgestellt). Die SCA 6000-Karte unterstützt einen FIPS 140-2 Level 3-Betriebsmodus, und die Karte wird von OKM stets auf diese Weise verwendet. Wenn das OKM-Cluster im FIPS-konformen Modus betrieben wird, verlassen keine Verschlüsselungsschlüssel unverpackt den kryptographischen Grenzbereich der SCA 6000-Karte. Die SCA 6000-Karte verwendet für das Generieren der Verschlüsselungsschlüssel einen von FIPS genehmigten Zufallszahlengenerator (wie in FIPS 186-2 DSA Random Number Generator angegeben) unter Verwendung von SHA-1.

Wenn eine KMA nicht mit einer SCA 6000-Karte konfiguriert ist, erfolgt die Kryptographie mittels des Solaris Cryptographic Framework (SCF) PKCS#11 Soft Token. Das SCF wird im FIPS 140-Modus gemäß den zuletzt veröffentlichten Solaris FIPS 140-2-Sicherheitsrichtlinien konfiguriert.

3.7.3. AES-Schlüssel-Wrap

Oracle Key Manager verwendet den AES-Schlüssel-Wrap-Algorithmus (RFC 3994) mit 256-Bit Schlüssel-Verschlüsselungsschlüssel zum Schutz von symmetrischen Schlüsseln, während sie erstellt, auf der KMA gespeichert und an Agents übertragen werden, oder innerhalb von Schlüsselübertragungsdateien.

3.7.4. Schlüsselreplikation

Wenn die erste KMA eines OKM-Clusters initialisiert wird, generiert die KMA einen großen Pool von Schlüsseln. Wenn weitere KMAs hinzugefügt werden, werden die Schlüssel für die neuen KMAs repliziert, wodurch diese umgehend zur Verschlüsselung von Daten bereit sind. Jede KMA, die dem Cluster hinzugefügt wird, generiert einen Pool von Schlüsseln und repliziert diese für andere KMAs im Cluster. Alle KMAs generieren je nach Bedarf neue Schlüssel, um die Schlüsselpoolgröße zu erhalten. So stehen den Agents stets Schlüssel zur Verfügung. Wenn ein Agent einen neuen Schlüssel benötigt, kann er eine KMA im Cluster kontaktieren und einen neuen Schlüssel anfordern. Die KMA bezieht einen verfügbaren Schlüssel aus ihrem Pool von Schlüsseln und weist ihn der Standardschlüsselgruppe des Agent und der Dateneinheit zu. Anschließend repliziert die KMA diese Datenbankupdates im ganzen Netzwerk für die anderen KMAs im Cluster. Später kann der Agent eine andere KMA im Cluster kontaktieren, um den Schlüssel abzurufen. Dabei wird zu keiner Zeit irgendwelches Textschlüsselmaterial im Netzwerk übertragen.

3.7.5. Solaris FIPS 140-2-Sicherheitsrichtlinien

Im Dezember 2013 hat das National Institute of Standards and Technology (NIST) das FIPS 140-2 Level 1-Validierungszertifikat #2061 für das Oracle Solaris Kernel Cryptographic Framework-Modul in Solaris 11 genehmigt. Im Januar 2014 hat NIST das FIPS 140-2 Level 1-Validierungszertifikat #2076 für das Oracle Solaris Userland Cryptographic Framework mit SPARC T4 und SPARC T5 genehmigt. Die Oracle Key Manager 3.1.0 KMA basiert

jetzt auf Solaris 11.3, das immer noch in der FIPS 140-2-Validierungstestphase ist. Oracle Solaris Kernel Cryptographic Framework in einer Oracle Key Manager 3.1.0 KMA ist gemäß den *Oracle Kernel Cryptographic Framework - Sicherheitsrichtlinien* konfiguriert. Gleichermaßen ist die KMA ebenfalls gemäß den *Oracle Solaris Userland Cryptographic Framework with SPARC T4- and SPARC T5 - Sicherheitsrichtlinien* konfiguriert. OKM wird auf neuere Solaris-Sicherheitsrichtlinien upgedatet sobald diese verfügbar sind.

3.7.6. Softwareupgrades

Alle KMA-Softwareupgrade-Bundles sind digital signiert, um zu verhindern, dass nicht autorisierte Software aus nicht genehmigten Quellen geladen wird.

4

Kapitel 4. Endpunkte

OKM unterstützt eine Vielzahl von Verschlüsselungsendpunkten. Im Folgenden werden die unterstützten Endpunkte aufgeführt:

- Verschlüsselungsfähige Bandlaufwerke
- Oracle Transparent Database Encryption (TDE) 11g und höher
- Oracle ZFS Storage Appliance
- Oracle Solaris 11 ZFS-Dateisysteme

Darüber hinaus sind Endpunkttools für Anwendungsentwickler oder, bei PKCS#11, zur Verwendung mit der TDE (transparenten Datenverschlüsselung) der Oracle Database verfügbar.

4.1. Linux PKCS#11 KMS-Provider

Ein Linux PKCS#11 KMS-Provider ist für Kunden verfügbar, die mit OKM über PKCS#11 kommunizieren möchten. Der Linux PKCS#11 KMS-Provider kann von einem Administrator von der My Oracle Support-Website heruntergeladen und auf einem Oracle Enterprise Linux-Server installiert werden. Der Linux PKCS#11 KMS-Provider hat dieselben Sicherheitseigenschaften und authentifiziert wie andere Agents mit Oracle Key Manager Appliances. Der Linux PKCS#11 KMS-Provider speichert eine Logdatei und Profilinformationen in folgendem Verzeichnis: `/var/opt/kms/username`. Diese Logdatei ist vom Benutzer und/oder Administrator manuell oder mithilfe eines Dienstprogramms, wie logrotate, zu verwalten. Der Zugriff auf das Verzeichnis `/var/opt/kms/username` muss durch entsprechende Berechtigungen beschränkt sein. Die Zugangsdaten zur Authentifizierung des Agent werden in einer PKCS#12-Datei im Profilverzeichnis aufbewahrt. Die PKCS#12-Datei ist passwortgeschützt. Informationen zum Linux PKCS#11 KMS-Provider finden Sie im *Oracle Key Manager - Administrationshandbuch* in den Dokumentationsbibliotheken von Oracle Key Manager unter:

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

4.2. PKCS#11 KMS-Provider für Solaris

Ein analoger PKCS#11 KMS-Provider ist mit Solaris 10 und Solaris 11 verfügbar.

4.3. JCE KMS-Provider

Ein Java Cryptographic Environment-Provider ist für Entwickler verfügbar, die Java-Clientanwendungen implementieren möchten, die Schlüssel aus OKM abrufen können. Dieses Produkt wurde in verschiedenen Oracle-Produkten integriert und ist im Oracle Technology Network verfügbar.

4.4. OKM-Plug-in für Oracle Enterprise Manager

Das Oracle Key Manager (OKM-)Appliance-Plug-in für Oracle Enterprise Manager (OEM) Cloud Control ermöglicht die Überwachung von OKM-Clustern. Jede KMA, die zu einem Cluster gehört, wird vom Plug-in überwacht. Für dieses Tool wird ein Sicherheitshandbuch bereitgestellt.

5

Kapitel 5. Remote-Syslog

Oracle Key Manager unterstützt Remote-Syslog. KMAs können so konfiguriert werden, dass Nachrichten im RFC 3164- oder RFC 5424-Nachrichtenformat an einen Remote-Syslog-Server über TCP unverschlüsselt oder Transport Layer Security (TLS) gesendet werden. RFC 5425 beschreibt die Verwendung von TLS zur Bereitstellung einer sicheren Verbindung für den Transport von Syslog-Nachrichten im RFC 5424-Nachrichtenformat.

Ein Sicherheitsbeauftragter kann eine KMA so konfigurieren, dass Nachrichten über TCP unverschlüsselt oder TLS gesendet werden. Die Verwendung von TLS zur Authentifizierung und Verschlüsselung der Kommunikation zwischen der KMA und einem Remote-Syslog-Server ist sicherer. Die KMA authentifiziert den Remote-Syslog-Server, indem dessen Zertifikat und öffentlicher Schlüssel angefordert werden. Optional kann der Remote-Syslog-Server zur Verwendung der gegenseitigen Authentifizierung verwendet werden. Durch die gegenseitige Authentifizierung wird sichergestellt, dass der Remote-Syslog-Server Nachrichten nur von autorisierten Clients (wie KMAs) akzeptiert. Wenn die Verwendung der gegenseitigen Authentifizierung konfiguriert ist, fordert der Remote-Syslog-Server ein Zertifikat von der KMA an, um die Identität der KMA zu prüfen.

6

Kapitel 6. Hardware Management Pack

Oracle Key Manager unterstützt das Oracle Hardware Management Pack (HMP) auf SPARC T7-1, Netra SPARC T4-1 und Sun Fire X4170 M2 KMAs. Das HMP-Produkt ist Teil von Oracle Single System Management zusammen mit ILOM. Ein Sicherheitsbeauftragter kann veranlassen, dass das HMP in einer KMA einen Management-Agent in Solaris verwendet, um die In-Band-Überwachung der KMA über SNMP zu aktivieren. Die HMP-Software ist vorinstalliert, ist jedoch bei der SNMP-Agent-Konfiguration deaktiviert. Somit ist der Listener-Port des SNMP-Agent erst geöffnet, wenn das HMP aktiviert ist. Das HMP ist standardmäßig deaktiviert.

Die Aktivierung von HMP bietet folgende Möglichkeiten:

- Ereignisbenachrichtigung bei Hardwareproblemen, bevor sie als Oracle Key Manager-spezifische SNMP-Benachrichtigungen oder als KMA-Ausfall angezeigt werden.
- Aktivierung von HMP auf einigen, oder allen, unterstützten KMAs in einem OKM-Cluster.
- Verwendung von schreibgeschützten SNMP-Get-Vorgängen für SNMP-MIBS in der KMA, einschließlich MIB-II, SUN-HW-MONITORING-MIB und SUN-STORAGE-MIB.
- Oracle Red Stack-Integration mit Oracle Enterprise Manager über SNMP-Receivelets und SNMP-Fetchlets.

Wenn Sie HMP in einer KMA aktivieren, sollten Sie folgende Sicherheitsaspekte berücksichtigen. Wenn HMP aktiviert ist, beachten Sie Folgendes:

- HPM nutzt aktivierte SNMP-Manager mit v2c-Protokoll, die im Oracle Key Manager-Cluster konfiguriert sind. Das SNMP v2c-Protokoll verfügt nicht über die Sicherheitserweiterungen des SNMP v3-Protokolls.
- Es aktiviert einen SNMP-Management-Agent in der KMA, sodass schreibgeschützter Netzwerkzugriff auf SNMP-MIB-Informationen in dieser KMA möglich ist.
- Sicherheitsrisiken, die in *Oracle Hardware Management Pack (HMP) - Sicherheitshandbuch* (`http://docs.oracle.com/cd/E20451_01/pdf/E27799.pdf`) aufgeführt werden, werden gemindert durch:
  - "Systemmanagementprodukte können verwendet werden, um eine bootfähige Root-Umgebung anzufordern" - Die Härtung der KMAs deaktiviert den Root-Zugriff auf Benutzer des Systems. SNMP ist für den schreibgeschützten Zugriff konfiguriert. Deshalb werden SNMP-Put-Vorgänge abgelehnt.

- "Systemmanagementprodukte umfassen leistungsfähige Tools, für deren Ausführung Administrator- oder Root-Berechtigungen erforderlich sind" - Root-Zugriff auf KMAs ist deaktiviert. Deshalb können Systembenutzer diese Tools nicht ausführen.

Anhang A

Anhang A. Prüfliste für sicheres Deployment

Die folgende Sicherheitsprüfliste enthält Richtlinien, mit denen Sie Ihr Key Management System (KMS) besser sichern können:

1. Installieren Sie jede KMA in einer physisch sicheren Umgebung.
2. Sichern Sie den OpenBoot-PROM oder das BIOS in jeder KMA.
3. Sichern Sie den Lights Out Manager in jeder KMA.
4. Definieren Sie die Schlüsselaufteilungskonfiguration für dieses Oracle Key Manager-Cluster.
5. Legen Sie die autonome Entsperreinstellung für jede KMA entsprechend fest.
6. Definieren Sie Oracle Key Manager-Benutzer und ihre entsprechenden Rollen.
7. Wenden Sie das Prinzip der geringsten Rechte an.
   a. Erteilen Sie Oracle Key Manager-Benutzern nur die jeweils erforderlichen Rollen.
8. Überwachen Sie die Aktivität im Oracle Key Manager-Cluster.
   a. Untersuchen Sie alle Fehler, insbesondere Sicherheitsverletzungen, die im Oracle Key Manager-Auditprotokoll protokolliert wurden.
9. Führen Sie beim ersten Definieren und bei jeder Änderung der Schlüsselaufteilungskonfiguration ein Backup der Core-Sicherheit durch.
10. Führen Sie regelmäßige Oracle Key Manager-Backups durch.
11. Speichern Sie die Backupdateien der Core-Sicherheit und des Oracle Key Managers an einem sicheren Ort.

Anhang B

Anhang B. Referenzen

- Oracle Key Manager - Kundendokumentation

  http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto
- *Oracle Enterprise Manager - Systemüberwachungs-Plug-in für Oracle Key Manager - Sicherheitshandbuch*
- *Oracle Key Manager - Installations- und Servicehandbuch* (nur intern)
- *Oracle Key Manager - Überblick*

  http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf
- *Oracle Key Manager Version 2.X - Whitepaper zu Sicherheit und Authentifizierung*

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

  http://docs.oracle.com/cd/E37444_01/
- SPARC T7-1-Serverdokumentation https://docs.oracle.com/cd/E54976_01/
- Netra SPARC T4-1-Serverdokumentation

  http://docs.oracle.com/cd/E23203_01/
- Oracle Hardware Management Pack - Dokumentation
  - Oracle Hardware Management Pack - Dokumentationsbibliothek

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

    http://www.oracle.com/technetwork/server-storage/servermgmt/overview/index.html
- NIST-Dokumentation:
  - *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

- Dokumentation der Sicherheitsrichtlinien für Oracle-Produkte:
  - *Oracle Solaris Kernel Cryptographic Framework - Sicherheitsrichtlinien*

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

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

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1050.pdf
  - *Oracle StorageTek T10000D-Bandlaufwerk - Sicherheitsrichtlinien*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2254.pdf
  - *Oracle StorageTek T10000C-Bandlaufwerk - Sicherheitsrichtlinien*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1561.pdf
  - *Oracle StorageTek T10000B-Bandlaufwerk - Sicherheitsrichtlinien*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1156.pdf
  - *Oracle StorageTek T10000A-Bandlaufwerk - Sicherheitsrichtlinien*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1157.pdf
  - *Oracle StorageTek T9480D-Bandlaufwerk - Sicherheitsrichtlinien*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1288.pdf
- FIPS-Validierungszertifikate für Oracle-Produkte:
  - Sun Crypto Accelerator 6000 - Zertifikat #1026 (abgelaufen)

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