Oracle® Key Manager 3

セキュリティーガイド

リリース 3.1

E52202-02

2016 年 4 月

ORACLE®

Oracle® Key Manager 3
セキュリティーガイド

E52202-02

目次

表の一覧

はじめに

このドキュメントでは、Oracle Key Manager 3 (OKM 3) のセキュリティー機能について説明します。

対象読者

このガイドは、OKM 3 のセキュリティー機能の使用およびセキュアなインストールと構成に関与するすべてのユーザーを対象にしています。

ドキュメントのアクセシビリティについて

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility Program の Web サイト (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc) を参照してください。

Oracle Support へのアクセス
サポートをご契約のお客様には、My Oracle Support を通して電子支援サービスを提供しています。詳細情報は (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info) か、聴覚に障害のあるお客様は (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs) を参照してください。

1

第1章 概要

このセクションでは、製品の概要を示し、アプリケーションセキュリティーの一般原則について説明します。

1.1. 製品の概要

Oracle Key Manager (OKM) は、暗号化鍵を作成、格納、および管理します。次のコンポーネントで構成されています。

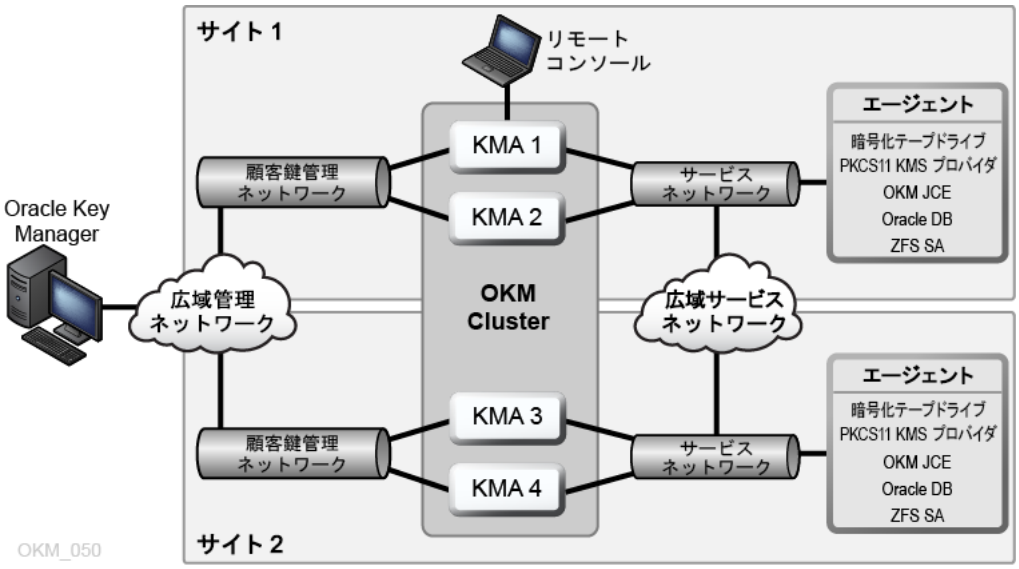
- Key Management Appliance (KMA) – ポリシーベースのライフサイクル鍵管理、認証、アクセス制御、および鍵プロビジョニングの各サービスを提供する、セキュリティーが強化されたボックスです。ストレージネットワークの信頼できる発行局として、KMA では、すべてのストレージデバイスが登録および認証されること、そしてすべての暗号化鍵が規定のポリシーに従って作成、プロビジョニング、および削除されることが保証されます。
- Oracle Key Manager GUI - ワークステーション上で実行されるグラフィカルユーザーインタフェースであり、IP ネットワーク経由で KMA と通信して OKM を構成および管理します。Oracle Key Manager GUI は、顧客が用意するワークステーションにインストールする必要があります。
- Oracle Key Manager CLI - ワークステーション上で実行される 2 つのコマンド行インタフェースであり、IP ネットワーク経由で KMA と通信して一般的に発行される管理操作を自動化します。Oracle Key Manager CLI は、顧客が用意したワークステーションにインストールする必要があります。
- OKM クラスタ – システム内の KMA の完全な集合。これらのすべての KMA は相互に認識し、情報を相互にレプリケートします。
- エージェント – OKM クラスタによって管理される鍵を使用して、暗号化を実行するデバイスまたはソフトウェア。StorageTek 暗号化テープドライブは、エージェントの例です。エージェントは、KMS Agent Protocol を使用して KMA と通信します。エージェント API は、エージェントハードウェアまたはソフトウェアに組み込まれている一連のソフトウェアインタフェースです。

OKM は、KMA、エージェント、および Oracle Key Manager GUI および CLI が実行されているワークステーションの間の接続のために TCP/IP ネットワークを使用します。ネットワーク接続を柔軟に行うために、各 KMA には、ネットワーク接続用の次の 3 つのインタフェースが用意されています。

- 管理接続 - 顧客ネットワークへの接続を目的にしています
- サービス接続 - エージェントへの接続を目的にしています
- ILOM/ELOM 接続 - KMA 上の ILOM または ELOM への接続を目的としています

次のイメージ内の例を参照してください。

図1.1



1.2. 一般的なセキュリティー原則

すべてのアプリケーションをセキュアに使うために、次の原則が重要になります。

1.2.1. ソフトウェアの最新状態の維持

優れたセキュリティー実践の原則の 1 つは、すべてのソフトウェアバージョンとパッチを最新に維持することです。最新の Oracle Key Manager アップグレードパッケージおよびインストーラは、My Oracle Support Web サイト `http://support.oracle.com` から入手できます。

1.2.2. クリティカルなサービスへのネットワークアクセスの制限

ビジネスアプリケーションは、ファイアウォールの背後に配置してください。ファイアウォールにより、これらのシステムへのアクセスが、既知のネットワークルートに確実に制限され、必要に応じてモニターおよび制限できることが保証されます。単一のファイアウォールルーターを複数の独立したファイアウォールの代わりに使用することもできます。

1.2.3. 最小特権の原則に従う

最小特権の原則は、ユーザーにはその業務を遂行するために必要な最小限の権限だけを与えるべきであるということを示しています。特に組織のライフサイクルの初期に、従業員が少数で作業を迅速に行う必要がある場合に、責任、役割、権限などを過剰に付与しすぎると、システムが大きく開放され不正使用を招くことがよくあります。ユーザー権限を定期的に見直して、現在の職務責任に対して妥当であるか見極めてください。

1.2.4. システムアクティビティーのモニター

システムのセキュリティーは、有効なセキュリティープロトコル、適切なシステム構成、システムモニタリングの 3 つの柱に支えられています。監査を行い、監査レコードを確認することで、この 3 番目の要件に対応します。システム内の各コンポーネントはどれも、ある程度のモニタリング機能を備えています。このドキュメントの監査アドバイスに従って、監査レコードを定期的にモニターしてください。

1.2.5. セキュリティー情報の最新状態の維持

Oracle では、ソフトウェアおよびドキュメントを絶えず改善しています。リビジョンについては年ごとに My Oracle Support Web サイトを確認してください。

2

第2章 セキュアなインストールおよび構成

このセクションでは、セキュアなインストールの計画プロセスについて説明し、システムの推奨される配備トポロジをいくつか紹介します。

2.1. 環境の理解

セキュリティーニーズをよく理解するため、次の質問を確認してください。

2.1.1. 保護しているのはどのリソースか。

本番環境の多くのリソースを保護できます。提供する必要があるセキュリティーレベルを決定する際には、保護対象のリソースを考慮してください。

保護対象のプライマリリソースは通常、データです。その他のリソースは、データの管理や保護に関連があるため、ここで概要を示しておきます。データの保護に関するさまざまな考慮事項には、データの損失 (つまり、使用できないデータ) および未承認の相手に対するデータの改ざんまたは開示などが含まれます。

暗号鍵は、未承認の開示からデータを保護するために使用されることがよくあります。つまり、これらも保護対象となる別のリソースです。高可用性のあるデータを維持するには、信頼性の高い鍵管理が不可欠です。保護対象となる別のリソースレイヤーには、Oracle Key Manager クラスタ自体の中にあるアセット (Key Management Appliance など) などが含まれます。

2.1.2. リソースをだれから保護しているか。

これらのリソースは、アクセスする権限を持たないすべてのユーザーから保護する必要があります。これらのリソースは物理的に保護されるべきです。どの従業員がこれらのリソースへのアクセスを持つべきかを検討してください。それから、各従業員が Oracle Key Manager 環境で発行できる操作のタイプを識別します。

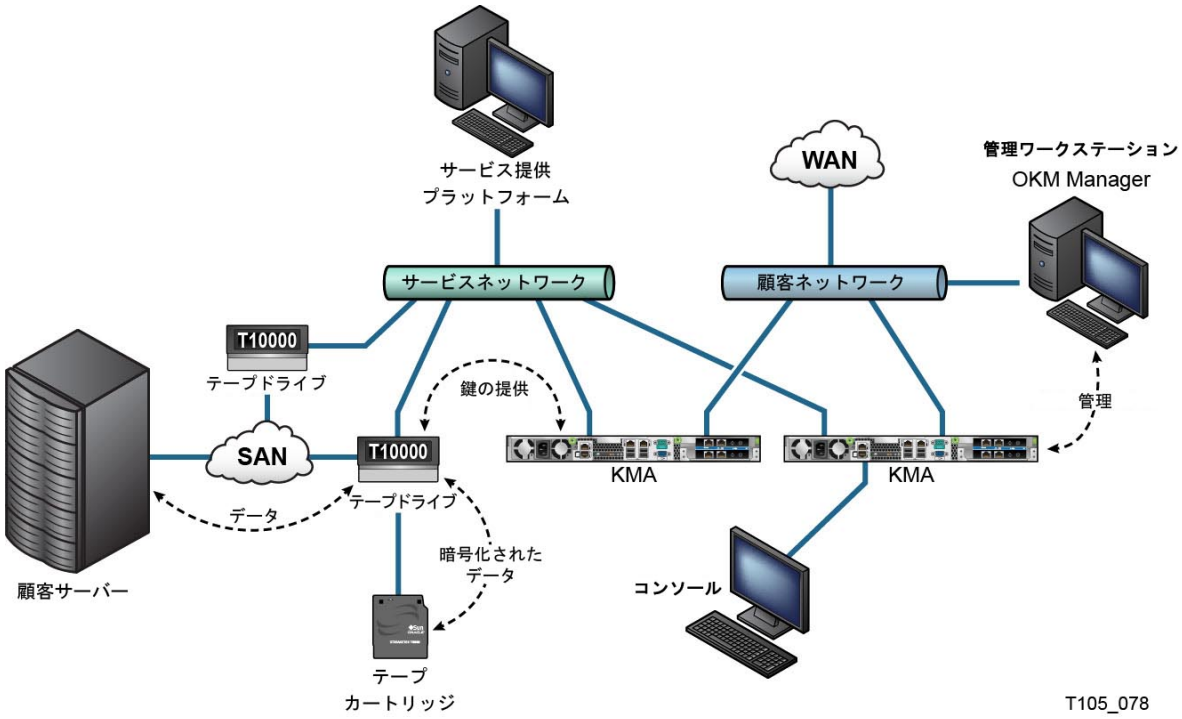
2.1.3. 戦略的リソースの保護に失敗した場合に何が起こるか。

ある場合には、簡単にセキュリティースキームの欠陥が検出され、面倒な事態になることが考えられます。その他の場合には、障害によって、リソースを使用する企業や個々のクライアントに多大な損害を与える可能性があります。各リソースのセキュリティーの影響を理解することで、適切に保護できます。

2.2. 推奨される配備トポロジ

次の図は、Oracle Key Manager ソリューションの標準的な配備を示しています。

図2.1 OKM ソリューションの標準的な配備



2.3. Key Management Appliance の設置

このセクションでは、OKM Key Management Appliance をセキュアに設置および構成する方法について説明します。

KMA は、Oracle Key Manager がすでに利用可能な状態になっている強化済みアプライアンスとして製造されています。

OKM クラスタでの KMA の設置および構成には、次の手順が含まれます。

1. 各 KMA は、ラック内に設置します。
2. 各 KMA は、ILOM をセキュリティー保護します。
3. OKM クラスタ内の最初の KMA を構成します。
4. 追加の KMA を OKM クラスタに追加します。

OKM クラスタの計画および配備の詳細については、『OKM 概要および計画ガイド』を参照してください。

2.3.1. ラックへの KMA 設置

Oracle カスタマサービスエンジニアが *Oracle Key Manager* インストールおよびサービスマニュアルに記載されている手順に従って KMA をラックに設置します。Oracle サービス担当者は、詳細についてこのマニュアルを参照できます。

2.3.2. KMA の ILOM のセキュリティー保護

Oracle Key Manager KMA は、最新の ILOM ファームウェアを使用して製造されています。KMA の ILOM は、Oracle カスタマサービスエンジニアまたは顧客によってセキュリティー保護されるようにしてください。また、ILOM ファームウェアのアップグレード後にも ILOM がセキュリティー保護されるようにしてください。

ILOM のセキュリティー保護は、セキュリティーを侵害する可能性のある変更が ILOM に加えられないように、特定の ILOM 設定で構成されます。説明については、『OKM 管理ガイド』の付録「サービスプロセッサ手順」にある「ILOM のセキュリティーの強化」を参照してください。

2.3.3. OKM クラスタ内の最初の KMA の構成

最初の KMA を構成する前に、この OKM クラスタで定義される鍵分割資格、ユーザー ID およびパスフレーズを識別します。これを行うには、OKM のインストールおよびサービスマニュアル (社内用) にあるようなワークシートを使用できます。Oracle サポート担当者に相談してください。

これらの鍵分割資格、ユーザー ID、およびパスワードについて適切な担当者に伝えます。詳細については、このドキュメントで後述する「定足数保護」を参照してください。

注記:

これらの鍵分割資格、ユーザー ID、およびパスフレーズは覚えておいて、保護してください!

Web ブラウザを開き、リモートコンソールを起動し、リモートコンソール内で OKM QuickStart ユーティリティーを起動します。この KMA の OKM クラスタを初期化するには、Oracle Key Manager ドキュメントライブラリに含まれている『*Oracle Key Manager* 管理ガイド』で説明されているクラスタの初期化手順に従います。

この手順中に鍵分割資格、およびセキュリティー責任者特権を持つユーザーが定義されます。QuickStart の手順が完了したら、セキュリティー責任者は KMA にログインして、追加の OKM ユーザーを定義する必要があります。

2.3.4. 鍵分割資格を定義するときの考慮事項

定義する鍵分割のユーザー ID およびパスフレーズを少なくし、しきい値を低くすると、簡便性は向上しますがセキュアではなくなります。定義する鍵分割のユーザー ID およびパスフレーズを多くし、しきい値を高くすると、簡便性は低下しますがセキュアになります。

2.3.5. 追加の OKM ユーザーを定義するときの考慮事項

定義する OKM ユーザーを少なくし、その一部に複数の役割を割り当てると、簡便性は向上しますがセキュアではなくなります。定義する OKM ユーザーを多くし、その大半に役割を 1 つのみ割り当てると、指定の OKM ユーザーによって実行される操作の追跡が容易になるため、簡便性は低下しますがセキュアになります。

2.3.6. OKM クラスタへのその他の KMA の追加

Web ブラウザを開き、リモートコンソールを起動し、リモートコンソール内で OKM QuickStart ユーティリティーを起動します。この KMA を OKM クラスタに追加するには、次にある『*Oracle Key Manager* 管理ガイド』で説明されているクラスタへの参加手順に従ってください。

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

2.3.7. その他の KMA を追加するときの考慮事項

Oracle Key Manager では、各 KMA の自律ロック解除を簡単に行うオプションを提供しています。このオプションは、クラスタにでの最初のおよび追加の KMA の QuickStart 手順中に定義され、あとからセキュリティー責任者が変更できます。

自律ロック解除が有効な場合、KMA は、起動時に自身を自動的にロック解除し、定足数の承認を必要とせずに鍵を提供する準備を整えます。自律ロック解除が無効な

場合、KMA は、起動時にロックされたままになり、セキュリティー責任者がロック解除の要求を発行して定足数がこの要求を承認するまで、鍵は提供されません。

セキュリティーを最大限に高めるため、自律ロック解除を有効にすることはお勧めしません。自律ロック解除オプションの詳細については、次にある *Oracle Key Manager* バージョン *2.x* のセキュリティーおよび認証に関するホワイトペーパーを参照してください。

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

2.3.8. 強化された KMA の特性

前述のとおり、KMA は、Oracle Key Manager がすでに利用可能な状態になっている強化済みアプライアンスとして製造されています。強化されたアプライアンスとして、次のような特性があります。

- 不要な Solaris パッケージは、Solaris イメージに含まれません。たとえば、ftp および telnet のサービスおよびユーティリティーは、Solaris イメージには現れません。
- KMA は、コアファイルを生成しません。
- 標準の Solaris login(1) ユーティリティーは、OKM コンソールに置き換えられました。そのため、ユーザーは Solaris コンソールにログインできません。
- ssh サービスはデフォルトで無効になっています。顧客サポートのために、限られた時間だけセキュリティー責任者が ssh サービスを有効にし、サポートアカウントを定義することはできます。このサポートアカウントは、唯一使用可能なアカウントであり、制限付きのアクセスおよびアクセス権を持ちます。Solaris の監査では、サポートアカウントが呼び出すコマンドを追跡します。
- root アカウントは無効になっていて、役割として構成されています。
- KMA には、DVD ドライブが装備されていません。
- USB ポートは実質的に無効です。
- 未使用のネットワークポートは閉じられます。
- 非実行可能スタックが有効になっています。
- アドレス空間検索ランダム化が構成されています。
- 非実行可能ヒープが有効になっています。
- セキュリティー上重要なファイルシステムに対して ZFS 暗号化が使用されます。

- SCAP PCI-DSS ベンチマークに準拠するように Solaris が構成されています。
- 不要な SMF サービスが無効になっています。
- システムブートプロセスのセキュリティーを保護するために、Oracle Solaris 検証済みブートを SPARC T7-1 ベースの KMA で構成可能で、カーネルモジュールの破損、ルートキットの挿入、またはその他の悪意のあるプログラムから保護します。
- SPARC T7-1 および Netra SPARC T4-1 サーバーをベースにした新しい KMA は、電源供給中にシャーシ扉にアクセス可能な場合に改ざん痕跡 (ILOM 障害) に対応します。
- ILOM 3.2 ファームウェアは、現在 FIPS 140-2 Level 1 認証済みで、FIPS モードで構成できます。
- フォレンジックを支援するために基本監査およびレポートツールが定期的に実行されます。これらのレポートは、OKM システムダンプに含まれています。
- ハードウェアセキュリティーモジュールの有無にかかわらず、(Solaris 11.1 用に文書化された) FIPS 140-2 Level 1 セキュリティーポリシーに従って、Solaris 暗号化セキュリティーフレームワークが構成されています。

2.4. TCP/IP 接続と KMA

各実体 (OKM Manager、エージェント、および同じクラスタ内のほかの KMA) と KMA の間にファイアウォールが存在する場合、そのファイアウォールでは、次のポート上での実体による KMA との TCP/IP 接続の確立が許可されている必要があります。

- OKM Manager から KMA への通信には、ポート 3331、3332、3333、3335 が必要です。
- エージェントから KMA への通信には、ポート 3331、3332、3334、3335 が必要です。
- KMA から KMA への通信には、ポート 3331、3332、3336 が必要です。

注記:

IPv6 アドレスを使用するように KMA を構成するユーザーの場合は、何らかの IPv6-over-IPv4 トンネル化トラフィックを使用したインターネットホストから内部ホストへのアクセスを防止するため、IPv4 ベースのエッジファイアウォールを、すべてのアウトバウンド IPv4 プロトコル 41 パケットと UDP ポート 3544 パケットをドロップするように構成します。

詳細については、ファイアウォール構成のドキュメントを参照してください。表2.1「KMA のポート接続」 に、KMA が明示的に使用するポート、または KMA がサービスを提供するポートの一覧を表示しています。

表2.1 KMA のポート接続

ポート番号	プロトコル	方向	説明
22	TCP	リスニング	SSH (テクニカルサポートが有効になっている場合のみ)
123	TCP/UDP	リスニング	NTP
3331	TCP	リスニング	OKM CA サービス
3332	TCP	リスニング	OKM 証明書サービス
3333	TCP	リスニング	OKM 管理サービス
3334	TCP	リスニング	OKM エージェントサービス
3335	TCP	リスニング	OKM 検出サービス
3336	TCP	リスニング	OKM レプリケーションサービス

表2.2「その他のサービス」 に、使用されていない可能性のあるポートで待機しているその他のサービスを示します。

表2.2 その他のサービス

ポート番号	プロトコル	方向	説明
53	TCP/UDP	接続	DNS (KMA が DNS を使用するように構成されている場合のみ)
68	UDP	接続	DHCP (KMA が DHCP を使用するように構成されている場合のみ)
111	TCP/UDP	リスニング	RPC (KMA が rpcinfo クエリーに応答します)。このポートは、KMS 2.1 以前でのみ外部要求に対して開かれます

ポート番号	プロトコル	方向	説明
161	UDP	接続	SNMP (SNMP マネージャーが定義されている場合のみ)
161	UDP	リスニング	SNMP (Hardware Management Pack が有効になっている場合のみ)
514	TCP	接続	リモート syslog (リモート syslog サーバーが暗号化されていない TCP を使用するように定義および構成されている場合のみ)
546	UDP	接続	DHCPv6 (KMA が DHCP と IPv6 を使用するように構成されている場合のみ)
4045	TCP/UDP	リスニング	NFS ロックデーモン (KMS 2.0 のみ)
6514	TLS over TCP	接続	リモート syslog (リモート syslog サーバーが TLS を使用するように定義および構成されている場合のみ)

注記:

ファイアウォール経由でサービスプロセッサ Web インタフェースおよび OKM コンソールにアクセスできるようにするには、ポート 443 を開けておく必要があります。ELOM および ILOM ポートについては、*Oracle Key Manager* インストールおよびサービスマニュアル (社内のみ) を参照してください。

表2.3「ELOM/ILOM ポート」 に KMA ELOM/ILOM ポートを示します。ファイアウォール外部から ELOM/ILOM へのアクセスが必要な場合はこれらのポートを有効にする必要がありますが、それ以外の場合はこれらを ELOM/ILOM IP アドレス用に有効にする必要はありません。

表2.3 ELOM/ILOM ポート

ポート番号	プロトコル	方向	説明
22	TCP	リスニング	SSH (ELOM/ILOM コマンド行インタフェース用)
53	TCP/UDP	接続	DNS (DNS が構成されている場合のみ必要)
68	UDP	接続	ELOM/ILOM 用に DHCP が必要な場合。 **注記**: DHCP および ELOM/ILOM 用のドキュメントはありませんが、サポートされています。

ポート番号	プロトコル	方向	説明
80	TCP	リスニング	HTTP (ELOM/ILOM Web インタフェース用) HTTP が必要な場合。それ以外の場合、ユーザーはリモートコンソールに接続する方法についての説明を次の場所で参照できます。 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	リスニング/接続	SNMPv3 (構成可能、これがデフォルトのポート)
443	TCP /TLS	リスニング	Embedded/Integrated Lights Out Manager Management Protocol (WS-Man) over Transport Layer Security (TLS) のための Desktop Management Task Force (DMTF) Web サービス
623	UDP	リスニング	Intelligent Platform Management Interface (IPMI)

3

第3章 セキュリティー機能

このセクションでは、製品に備えられている特定のセキュリティーメカニズムについて説明します。

3.1. 潜在的な脅威

暗号化が有効なエージェントを持つ顧客は、主に次の点に関心を持ちます。

- ポリシー違反の情報の開示
- データの損失または破棄
- 破局的故障時のデータ復元の許容できない遅延 (たとえばビジネス継続性サイトにおける)
- 検出されないデータ変更。

3.2. セキュリティー機能の目標

Oracle Key Manager のセキュリティー機能の目標は次のとおりです。

- 暗号化されたデータが開示されないようにする。
- 攻撃への暴露を最小限に抑える。
- 十分に高い信頼性と可用性を提供する。

3.3. セキュリティーモデル

セキュリティーガイドのこのセクションでは、システムが対抗するように設計された脅威、および個々のセキュリティー機能を組み合わせて攻撃を防ぐ方法についての概要を示します。

このような保護を提供するクリティカルなセキュリティー機能は次のとおりです。

- 認証 - 権限のある個人のみがシステムおよびデータにアクセスできるようにします

- 承認 - システム権限およびデータに対するアクセス制御。このアクセス制御は、個人が適切なアクセス権のみを取得するように、認証の上に構築されます
- 監査 - 管理者が認証メカニズムの侵害の試みや、アクセス制御の侵害または侵害の試みを検出できます。

Oracle Key Manager のセキュリティーおよび認証に関する詳細については、次の *Oracle Key Manager* バージョン *2.x* のセキュリティーおよび認証に関するホワイトペーパーを参照してください。

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

3.4. 認証

Oracle Key Manager アーキテクチャーは、システムのすべての要素間 (KMA 対 KMA、エージェント対 KMA、およびユーザー操作の場合の Oracle Key Manager GUI または CLI 対 KMA) の相互認証を提供します。

システムの各要素 (たとえば新しい暗号化エージェント) は、OKM で ID およびパスフレーズを作成し、追加する要素に入力することでシステムに登録されます。たとえば、テープドライブがシステムに追加される場合、エージェントおよび KMA は共有パスフレーズに基づいてチャレンジ応答プロトコルを自動的に実行し、エージェントはルート認証局 (CA) 証明書、およびエージェントの新しい鍵ペアと署名済み証明書を取得します。エージェントはルート CA 証明書、エージェント証明書、および鍵ペアを適所に使用して、その後の KMA とのすべての通信で Transport Layer Security (TLS) プロトコルを実行できます。すべての証明書は X.509 証明書です。

OKM はルート認証局として動作し、KMA が使用するルート証明書を生成して、エージェント、ユーザー、および新しい KMA で使用される証明書を導出 (自己署名) します。

3.5. アクセス制御

アクセス制御には次のタイプがあります。

- ユーザーと役割ベースのアクセス制御
- 定足数保護。

3.5.1. ユーザーと役割ベースのアクセス制御

Oracle Key Manager には、それぞれがユーザー ID とパスフレーズを持つ複数のユーザーを定義する機能があります。各ユーザーには、1 つ以上の事前定義済みの役割が付与されています。これらの役割は、Oracle Key Manager システムでユーザーが実行を許可される操作を決定します。これらの役割は、次のとおりです。

- セキュリティー責任者 - Oracle Key Manager の設定と管理を実行します
- オペレータ - エージェントの設定と日常業務を実行します
- コンプライアンス責任者 - 鍵グループを定義し、それらの鍵グループへのエージェントからのアクセスを制御します
- バックアップオペレータ - バックアップ操作を実行します
- 監査者 - システムの監査証跡を表示します
- 定足数メンバー - 保留中の定足数操作を表示して承認します

セキュリティー責任者は、OKM クラスタで KMA を設定する QuickStart 処理中に定義されます。その後、ユーザーは追加のユーザーを定義するために、Oracle Key Manager GUI を使用し、セキュリティー責任者としてクラスタにログインする必要があります。セキュリティー責任者は、特定のユーザーに複数の役割を割り当てたり、複数のユーザーに特定の役割を割り当てたりできます。

各役割で許可されている操作、およびセキュリティー責任者がユーザーを作成して役割を割り当てる方法の詳細については、次にある Oracle Key Manager ドキュメントライブラリに含まれている『*Oracle Key Manager* 管理ガイド』を参照してください。

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

この役割ベースのアクセス制御では、運用上の機能を分離するために、米国商務省国立標準技術研究所 (NIST) の Special Publication (SP) 800-60 にある運用上の役割をサポートしています。

3.5.2. 定足数保護

一部の操作では、追加のセキュリティーレベルが必要になるほど重要です。このような操作には、OKM クラスタへの KMA 追加、KMA のロック解除、ユーザーの

作成、ユーザーへの役割追加などがあります。このセキュリティーを実装するために、前述の役割ベースのアクセスだけでなく、一連の鍵分割資格が使用されます。

鍵分割資格は、ユーザー ID とパスフレーズの一連のペアとともに、システムで特定の操作を完了させるために必要なペアの最小数で構成されます。鍵分割資格は「定足数」とも呼ばれ、最小数は「定足数しきい値」とも呼ばれます。

Oracle Key Manager では、最大で 10 組の鍵分割ユーザー ID/パスフレーズのペアとしきい値とを定義できます。これらは QuickStart 処理中、OKM クラスタで最初の KMA が構成されるときに定義されます。鍵分割ユーザーの ID とパスフレーズは、システムにログインするために使用されるユーザー ID とパスフレーズとは異なります。ユーザーが定足数承認を必要とする操作を試みると、システムでこの操作が実行される前に、鍵分割ユーザーおよびパスフレーズの定義済みしきい値によってこの操作が承認される必要があります。

3.6. 監査

各 KMA は、OKM クラスタ内でエージェント、ユーザー、およびピア KMA によって発行される操作など、実行する操作の監査イベントを記録します。KMA では、エージェント、ユーザー、またはピア KMA が自分自身を認証できなかったときには必ず監査イベントを記録します。セキュリティー違反を示す監査イベントは記録されます。認証の失敗は、セキュリティー違反を示す監査イベントの例です。また、SNMP エージェントが OKM クラスタで識別されている場合、セキュリティー違反が発生すると、KMA は SNMP エージェントに SNMP INFORM を送信します。リモート syslog が構成されている場合、KMA はこれらの監査メッセージを構成済みのサーバーにも転送します。「リモート *Syslog* 」を参照してください。

ユーザーは、OKM クラスタに適切にログインする必要があり、監査イベントの表示を許可される前に、役割が割り当てられている必要があります。

KMA は、監査イベントを管理します。KMA は保持期間および制限 (件数) に基づいて古い監査イベントを削除します。セキュリティー責任者は、必要に応じて保持期間および制限を変更できます。

3.7. その他のセキュリティー機能

Oracle Key Manager には、その他のセキュリティー機能があります。そのような機能およびその他の OKM 機能の詳細については、次にある *Oracle Key Manager* の概要を参照してください。

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

3.7.1. セキュアな通信

KMA とエージェントの間、ユーザーと KMA の間、および KMA とピア KMA の間の通信プロトコルは同じです。いずれの場合も、システムはチャレンジ応答プロトコルを実行するために、通信を初期化するエンティティーのパスフレーズを使用します。成功した場合、エンティティーは証明書とそれに対応する秘密鍵とともに提供されます。この証明書および秘密鍵により、Transport Layer Security (TLS) (セキュアソケット) チャネルを確立できます。相互認証が実行されます。任意の接続の各端が他端を認証します。OKM 3.1+ KMA は常にピアツーピアレプリケーショントラフィックに TLS 1.2 を使用します。

3.7.2. ハードウェアセキュリティーモジュール

KMA では、別途販売されているハードウェアセキュリティーモジュールを使用できます。このハードウェアセキュリティーモジュール Sun Cryptographic Accelerator (SCA) 6000 カードは、FIPS 140-2 Level 3 で認証済みだったもので、Advanced Encryption Standard (AES) 256 ビット暗号化鍵を提供します (この証明書は 2015 年 12 月 31 日で期限が切れて更新されていません。後続のリリースでは代替の HSM が提供されます)。SCA 6000 カードは FIPS 140-2 Level 3 動作モードをサポートしており、OKM では常にこの方法でカードを使用します。OKM クラスタが FIPS 準拠モードで動作する場合、SCA 6000 カードの暗号境界は暗号化鍵によってラップ解除形式のままになりません。SCA 6000 カードは、FIPS 186-2 の SHA-1 を使用した DSA 乱数生成器で指定されている FIPS 承認の乱数生成器を使用して暗号化鍵を生成します。

KMA が SCA 6000 カードを使用するように構成されていない場合、暗号は Solaris Cryptographic Framework (SCF) PKCS#11 ソフトトークンを使用して実行されます。SCF は、最近発行された Solaris FIPS 140-2 セキュリティーポリシーに従って、FIPS 140 モードで構成されています。

3.7.3. AES 鍵のラッピング

Oracle Key Manager では 256 ビット鍵暗号化鍵による AES 鍵のラッピング (RFC 3994) を使用して、対称鍵が作成されるとき、KMA に格納されるとき、エージェントに伝送されるとき、または鍵転送ファイル内にあるときに、それらを保護します。

3.7.4. 鍵のレプリケーション

OKM クラスタで最初の KMA が初期化されるときに、KMA は大きい鍵プールを生成します。その他の KMA がクラスタに追加されると、鍵が新しい KMA にレプリケートされて、データを暗号化するために使用される準備が整います。クラスタに追加される KMA ごとに鍵プールを生成し、クラスタ内のピア KMA にレプリケートします。すべての KMA は、鍵プールサイズを維持するために必要に応じて新しい鍵を生成し、準備した鍵が常にエージェントで使用できるようにします。エージェントが新しい鍵を要求するときは、クラスタ内の KMA に接続して新しい鍵を要求します。KMA は準備された鍵を鍵プールから取り出し、この鍵をエージェントのデフォルト鍵グループおよびデータユニットに割り当てます。次に KMA はネットワークを介してこれらのデータベース更新をクラスタ内のほかの KMA にレプリケートします。その後、エージェントは鍵を取得するためにクラスタ内の別の KMA に接続できます。クリアテキストの鍵マテリアルがネットワーク上を伝送することはありません。

3.7.5. Solaris FIPS 140-2 セキュリティーポリシー

2013 年 12 月、米国商務省国立標準技術研究所 (NIST) は、Solaris 11 の Oracle Solaris カーネル暗号化フレームワークモジュール用の FIPS 140-2 Level 1 検証証明書 #2061 を授与しました。2014 年 1 月、NIST は SPARC T4 および SPARC T5 による Oracle Solaris ユーザーランド暗号化フレームワーク用の FIPS 140-2 Level 1 検証証明書 #2076 を授与しました。Oracle Key Manager 3.1.0 KMA は、FIPS 140-2 検証テストが現在行われている Solaris 11.3 に基づいています。Oracle Key Manager 3.1.0 KMA の Oracle Solaris カーネル暗号化フレームワークは、*Oracle* カーネル暗号化フレームワークセキュリティーポリシーに従って構成されています。同様に、KMA はまた *SPARC T4* および *SPARC T5* による *Oracle Solaris* ユーザーランド暗号化フレームワークのセキュリティーポリシーに従って構成されています。新しい Solaris セキュリティーポリシーが使用可能になるたびに、OKM はそのセキュリティーポリシーに更新されます。

3.7.6. ソフトウェアアップグレード

すべての KMA ソフトウェアアップグレードバンドルは、承認されていないソースから不正なソフトウェアをロードしないようデジタル署名されています。

4

第4章 エンドポイント

OKM は、さまざまな暗号化エンドポイントをサポートしています。サポートされているエンドポイントは次のとおりです。

- 暗号化対応のテープドライブ
- Oracle Transparent Database Encryption (TDE) 11g 以上
- Oracle ZFS Storage Appliance
- Oracle Solaris 11 ZFS ファイルシステム

さらに、アプリケーション開発者向けのエンドポイントツールや、PKCS#11 の場合は Oracle Database の Transparent Database Encryption (TDE) の使用のためのエンドポイントツールが利用できます。

4.1. Linux PKCS#11 KMS プロバイダ

Linux PKCS#11 KMS プロバイダは、PKCS#11 を使用して OKM と通信する顧客用に使用できます。管理者は、Linux PKCS#11 KMS プロバイダを My Oracle Support Web サイトからダウンロードし、Oracle Enterprise Linux サーバーにインストールできます。Linux PKCS#11 KMS プロバイダは、ほかのエージェントと同様に Oracle Key Manager アプライアンスのセキュリティー特性と認証を利用できます。Linux PKCS#11 KMS プロバイダは、ログファイルおよびプロファイル情報を `/var/opt/kms/username` ディレクトリに格納します。ユーザーや管理者は、このログファイルを手動で管理するか、logrotate のようなユーティリティーを使用して管理するようにしてください。`/var/opt/kms/username` ディレクトリに対するアクセス制御は、適切な権限を使用して制限するようにしてください。プロファイルディレクトリ内では、エージェントの認証資格は、PKCS#12 ファイル内に保持されます。PKCS#12 ファイルは、パスワードでセキュリティー保護されます。Linux PKCS#11 KMS プロバイダの詳細については、次にある Oracle Key Manager ドキュメントライブラリに含まれている『*Oracle Key Manager* 管理ガイド』を参照してください。

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

4.2. Solaris 用 PKCS#11 KMS プロバイダ

Solaris 10 および Solaris 11 についても、類似の PKCS#11 KMS プロバイダを利用できます。

4.3. JCE KMS プロバイダ

Java 暗号化環境プロバイダは、OKM から鍵を取得できる Java クライアントアプリケーションを実装する開発者用に使用できます。この製品はさまざまな Oracle 製品と統合されていて、Oracle Technology Network から入手できます。

4.4. Oracle Enterprise Manager の OKM プラグイン

Oracle Enterprise Manager (OEM) Cloud Control 用の Oracle Key Manager (OKM) アプライアンスプラグインは OKM クラスタのモニタリング機能を提供します。クラスタに属する各 KMA がプラグインによってモニターされます。このツール用のセキュリティーガイドが提供されています。

5

第5章 リモート Syslog

Oracle Key Manager は、リモート syslog をサポートしています。KMA は、暗号化されていない TCP または Transport Layer Security (TLS) を使用して、リモート syslog サーバーに RFC 3164 または RFC 5424 メッセージ形式でメッセージを送信するように構成できます。RFC 5424 メッセージ形式での syslog メッセージのトランスポートに使用するセキュアな接続を提供するための TLS の使用については、RFC 5425 に記載されています。

セキュリティー責任者は、暗号化されていない TCP または TLS を使用してメッセージを送信するために KMA を構成できます。TLS を使用して KMA とリモート syslog サーバーの間の通信を認証および暗号化する方が安全です。KMA は証明書と公開鍵をリクエストすることによってリモート syslog サーバーを認証します。オプションで、リモート syslog サーバーは相互認証を使用するように構成できます。相互認証により、リモート syslog サーバーは、承認されたクライアント (KMA など) からのメッセージのみ受け入れるようになります。相互認証を使用するように構成されている場合、リモート syslog サーバーは KMA の識別情報を確認するために、KMA の証明書をリクエストします。

6

第6章 Hardware Management Pack

Oracle Key Manager は、SPARC T7-1、Netra SPARC T4-1、および Sun Fire X4170 M2 KMA 上で Oracle Hardware Management Pack (HMP) をサポートします。HMP 製品は、ILOM とともに Oracle Single System Management のメンバーです。セキュリティー責任者は、KMA 上で HMP を有効にして Solaris 内で管理エージェントを使用することで、SNMP を介した KMA の帯域内モニタリングを有効にできます。HMP ソフトウェアはインストール済みですが、SNMP エージェント構成では無効になっています。したがって、SNMP エージェントのリスニングポートは HMP が有効になるまで開きません。HMP はデフォルトで無効になっています。

HMP を有効にすると、次の機能が提供されます。

- Oracle Key Manager 固有の SNMP 通知または KMA の停止として表示される前に、ハードウェアの問題のイベントを通知する機能。
- OKM クラスタ内のサポートされているいずれかあるいはすべての KMA 上で HMP を有効にする機能。
- MIB-II、SUN-HW-MONITORING-MIB、SUN-STORAGE-MIB などの KMA 上での SNMP MIBS への読み取り専用の SNMP Get 操作を使用する機能。
- SNMP Receivelet と SNMP Fetchlet を介した Oracle Enterprise Manager との Oracle Red Stack の統合。

KMA 上で HMP を有効にすることを選択した場合、次のセキュリティー上の考慮点に留意してください。有効にすると、HMP は次のように動作します。

- Oracle Key Manager クラスタ内で構成されている、任意の有効なプロトコル v2c SNMP マネージャーを利用します。SNMP v2c プロトコルには SNMP v3 プロトコルに見られるセキュリティー拡張機能はありません。
- KMA 上の SNMP 管理エージェントを有効化することで、この KMA 上で SNMP MIB 情報への読み取り専用ネットワークアクセスを可能にします。

- *Oracle Hardware Management Pack (HMP)* セキュリティーガイド (http://docs.oracle.com/cd/E20451_01/pdf/E27799.pdf) で特定されたセキュリティーリスクが次のことにより緩和されます。
  - 「システム管理製品を使用して、ブート可能な root 環境を構築できます」- KMA の強化によりシステムのユーザーへの root アクセスが無効化されます。SNMP は読み取り専用アクセス用に構成されています。したがって、SNMP Put 操作は拒否されます。
  - 「システム管理製品には、管理者および root 特権の実行に必要な強力なツールが含まれています」- KMA への root アクセスが無効化されます。したがって、システムユーザーはこれらのツールを実行できません。

付録A

付録A セキュアな導入のためのチェックリスト

次のセキュリティーチェックリストに、鍵管理システムのセキュリティー保護に役立つガイドラインを示します。

1. 物理的にセキュアな環境に各 KMA をインストールします。
2. 各 KMA 上の OpenBoot PROM または BIOS のセキュリティーを保護します。
3. 各 KMA 上の Lights Out Manager のセキュリティーを保護します。
4. この Oracle Key Manager クラスタの鍵分割構成を定義します。
5. 必要に応じて、各 KMA の自律ロック解除設定を設定します。
6. Oracle Key Manager ユーザーとそれに関連付けられた役割を定義します。
7. 最小権限の原則を順守します。
   a. 各 Oracle Key Manager ユーザーに必要な役割のみを付与します。
8. Oracle Key Manager クラスタのアクティビティーをモニターします。
   a. Oracle Key Manager 監査ログに記録されるエラー、特にセキュリティー違反を調査します。
9. 鍵分割構成が最初に定義されている場合、鍵分割構成が変更されるたびに、コアセキュリティーをバックアップします。
10. Oracle Key Manager のバックアップを定期的に実行します。
11. コアセキュリティーバックアップファイルおよび Oracle Key Manager バックアップファイルを、セキュアな場所に格納します。

付録B

付録B 参照情報

- Oracle Key Manager カスタマドキュメント

  http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto
- *Oracle Enterprise Manager System Monitoring Plug-in for Oracle Key Manager* セキュリティーガイド
- *Oracle Key Manager* のインストールおよびサービスマニュアル (社内のみ)
- *Oracle Key Manager* の概要

  http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf
- *Oracle Key Manager* バージョン *2.X* のセキュリティーおよび認証に関するホワイトペーパー

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

  http://docs.oracle.com/cd/E37444_01/
- SPARC T7-1 サーバーのドキュメント https://docs.oracle.com/cd/E54976_01/
- Netra SPARC T4-1 サーバーのドキュメント

  http://docs.oracle.com/cd/E23203_01/
- Oracle Hardware Management Pack のドキュメント
  - Oracle Hardware Management Pack ドキュメントライブラリ

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

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

- NIST のドキュメント:
  - 米国商務省国立標準技術研究所の *Special Publication 800-60 Volume I Revision 1*

    http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf
- Oracle 製品のセキュリティーポリシードキュメント:
  - *Oracle Solaris* カーネル暗号化フレームワークセキュリティーポリシー

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2061.pdf
  - *SPARC T4* および *T5* での *Oracle Solaris* カーネル暗号化フレームワークセキュリティーポリシー

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2060.pdf
  - *Sun Cryptographic Accelerator 6000 FIPS 140-2* のセキュリティーポリシー

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1050.pdf
  - *Oracle StorageTek T10000D* テープドライブセキュリティーポリシー

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2254.pdf
  - *Oracle StorageTek T10000C* テープドライブセキュリティーポリシー

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1561.pdf
  - *Oracle StorageTek T10000B* テープドライブセキュリティーポリシー

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1156.pdf
  - *Oracle StorageTek T10000A* テープドライブセキュリティーポリシー

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1157.pdf

- *Oracle StorageTek T9480D* テープドライブセキュリティーポリシー

  http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1288.pdf

- Oracle 製品用の FIPS 検証証明書:
  - Sun Crypto Accelerator 6000 - 証明書 #1026 (期限切れ)

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