ORACLE DATA SHEET

Oracle Key Vault

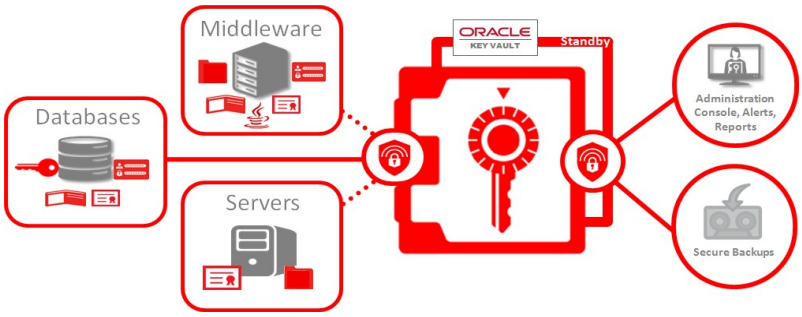
個人識別情報、クレジット・カード・データ、医療記録、およびその他の機密情報の規制強化やセキュリティ上の脅威から、データセンターでは暗号化の使用が増加しています。この増加に伴い、暗号化鍵、ウォレット、Java キーストア、およびその他のシークレットの管理は、データセンター・エコシステムにおいてセキュリティとビジネス継続性の両方に影響を及ぼす重要な要素になっています。Oracle Key Vault は、企業全体への暗号化の導入を促進する、一元的な鍵管理プラットフォームです。

おもな機能

- 最新の堅牢な鍵管理プラットフォームで鍵、Oracle ウォレット、Java キーストア、資格証明ファイルを管理
- 権限が付与されたすべての企業内エンドポイントで鍵をセキュアに共有
- 作成、ローテーション、有効期限など、鍵のライフ・サイクルのステージを管理
- 透過的データ暗号化（TDE）のマスター鍵用に最適化
- エンドポイントを容易に登録およびプロビジョニング
- 保護された RESTful インタフェースを使用してエンドポイントの登録を自動化
- プライマリとスタンバイのサポートにより高可用性とディザスタ・リカバリを実現
- エンドポイントのサーバーと永続キャッシュに対して読取り専用の制限モードをサポートすることにより、エンドポイントの可用性を強化
- 遠隔地への自動バックアップをスケジューリング
- データベースのパッチ適用なしに以前のデータベース・バージョンをサポート
- Linux、Windows、Solaris、AIX、および HP-UX（IA）の各エンドポイント・プラットフォームをサポート
- ハートウェア・セキュリティ・モジュール（HSM）統合をサポート
- OASIS KMIP 標準をサポート

Oracle Key Vault の概要

Oracle Key Vault は、暗号化鍵、Oracle ウォレット、Java キーストア、および資格証明ファイルを一元管理することで、暗号化およびその他のセキュリティ・ソリューションを迅速に導入できるようにします。また、Oracle Advanced Security の透過的データ暗号化（TDE）のマスター鍵を管理するために最適化されています。このセキュリティ強化されたフルスタックのソフトウェア・アプライアンスでは、セキュリティ、可用性、スケーラビリティを提供するために Oracle Linux および Oracle Database テクノロジーが使用されています。Oracle Key Vault は、業界標準の OASIS KMIP（Key Management Interoperability Protocol）をサポートしています。



図：Oracle Key Vaultの導入の概要

Oracle ウォレットと Java キーストアの一元管理

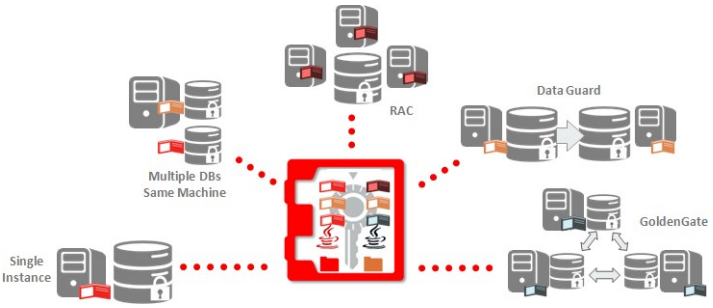
Oracle ウォレットと Java キーストアは多くの場合、サーバーおよびサーバー・クラスタ全体に手動で分散されています。Oracle Key Vault はこれらのファイルの内容をマスター・リポジトリに項目別に格納します。また、サーバーのエンドポイントが Oracle Key Vault と通信できない状態でも、ローカル・コピーを使用して処理を継続できます。ウォレットとキーストアをアーカイブした後は、ローカル・コピーを誤って削除したりパスワードを忘れたりということがあっても、サーバーにリカバリできます。

ORACLE KEY VAULT 関連製品

Oracle Key Vault は Oracle Database Security スイートの重要な制御手段です。Oracle Database Security の関連製品は次のとおりです。

- Oracle Advanced Security
- Oracle Database Vault
- Oracle Label Security
- Oracle Data Masking and Subsetting
- Oracle Audit Vault and Database Firewall

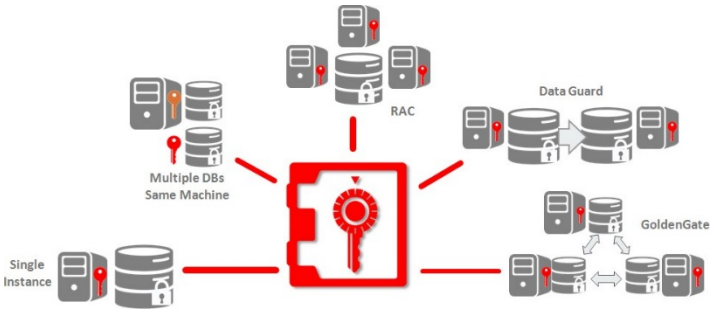
Oracle Key Vault は、Oracle Real Application Clusters（Oracle RAC）、Oracle Active Data Guard、Oracle GoldenGate などのデータベース・クラスタ全体でウォレットの共有を効率化します。ウォレットをセキュアに共有すると、Oracle Data Pump および Oracle トランスポータブル表領域を使用して暗号化データの移動も容易に行えます。Oracle Key Vault は、サポートされているすべての Oracle Middleware リリースおよび Oracle Database リリースの Oracle ウォレットで使用できます。



図：Oracle Key Vaultでのウォレット管理シナリオ

オンラインの透過的データ暗号化マスター鍵管理

Oracle Database で透過的データ暗号化（TDE）を使用している場合、Oracle Key Vault はローカル・ウォレット・ファイルを使用する代わりに、直接ネットワーク接続を介して TDE マスター鍵を一元管理します。そのため、定期的なパスワードのローテーション、ウォレット・ファイルのバックアップ、パスワードを忘れた状況からのリカバリなど、ウォレット・ファイルの管理に伴う操作上の課題がなくなります。また、暗号化鍵と暗号化データを物理的に分離できます。この分離は、規制遵守においてよく言及されていることです。Oracle Key Vault に格納されたマスター鍵を、エンドポイントのアクセス制御設定に応じて、データベース全体で表領域の鍵や表の鍵を復号するために使用できます。ローカルのウォレット・コピーなしに鍵を共有するこの方法は、Oracle RAC、Oracle Active Data Guard、Oracle GoldenGate などのデータベース・クラスタで TDE を実行する場合に役立ちます。Oracle データベース内の暗号化データに使用されている既存のマスター鍵を、初期設定の一部として Oracle ウォレットから Oracle Key Vault に容易に移行できます。TDE と Oracle Key Vault 間の直接ネットワーク接続は、Oracle Database 11gR2、Oracle Database 12c、および Oracle Database 18c でサポートされており、データベースのパッチ適用は不要です。



図：Oracle Key Vaultでのオンライン TDEマスター鍵シナリオ

資格証明ファイルの一元バックアップ

SSH 鍵を含む資格証明ファイル、Kerberos キータブ・ファイル、および同様な資格証明ファイルも、適切な保護メカニズムが適用されていない状態で広く分散されています。Oracle Key Vault では、資格証明ファイルを長期保存およびリカバリ目的でバックアップし、必要な時に簡単にリカバリします。また、これらのファイルへのアクセスを監査し、信頼できるエンドポイント全体でこれらのファイルを共有します。

Oracle Key Vault の管理

ブラウザベースの管理コンソールにより、Oracle Key Vault の管理、サーバー・エンドポイントのプロビジョニング、鍵グループのセキュアな管理、鍵へのアクセスについてのレポートを簡単に行えます。管理者ロールを鍵、システム、監査の各管理機能に分割できるため、職務分離を実現できます。サーバー・エンドポイントの操作責任を持つ他のユーザーに鍵およびウォレットへのアクセス権限を付与できるため、管理が容易になります。管理者は、近日中に発生するパスワードや鍵の有効期限切れなど、重要なステータス更新やシステム・アクティビティについて電子メール・アラートを受信します。

企業規模の導入では、セキュリティは重要な側面となります。Oracle Key Vault は、さまざまな Oracle データベース・セキュリティ・テクノロジーを使用して、Oracle Key Vault 内に格納されている鍵およびシークレットを保護しています。たとえば、Oracle Key Vault では、組込みの Oracle データベースに格納されている鍵を暗号化するために、透過的データ暗号化を使用しています。また、無許可の特権ユーザー・アクセスを制限し、鍵アクセスや鍵ライフ・サイクルの変更を含む重要なすべての操作を監査するために、Oracle Database Vault を使用しています。監査を統合するために、Oracle Database Vault の監査データを Oracle Audit Vault and Database Firewall（Oracle AVDF）または syslog サーバーに転送できます。Oracle Database Vault を SNMPv3 経由でリモートから監視できます。

Oracle Key Vault の導入

Oracle Key Vault は ISO イメージとしてパッケージ化され、構成済みのセキュアなソフトウェア・アプライアンスとして提供されています。このアプライアンスはインストールが容易で、導入規模に応じてユーザーが選択した x86-64 互換ハードウェアに導入することが可能です。

Oracle Key Vault は、Linux、Windows、Solaris、AIX、HP-UX（IA）を含む一般的なエンタープライズ・プラットフォーム上のエンドポイントをサポートしています。保護された RESTful インタフェースを使用してエンドポイントの登録とプロビジョニングを自動化できるため、オンプレミスとクラウドのいずれの場合でも大規模な導入が可能です。Oracle Key Vault は通常、可用性を高めるためにプライマリおよびスタンバイ構成で導入されています。

Oracle Key Vault により、企業の鍵とシークレットを保護しながら、鍵、Oracle ウォレット、Java キーストア、およびシークレットの管理を簡素化および一元化できます。

お問い合わせ

Oracle Key Vault について、詳しくは oracle.com を参照するか、+1.800.ORACLE1 でオラクルの担当者にお問い合わせください。

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Hardware and Software, Engineered to Work Together