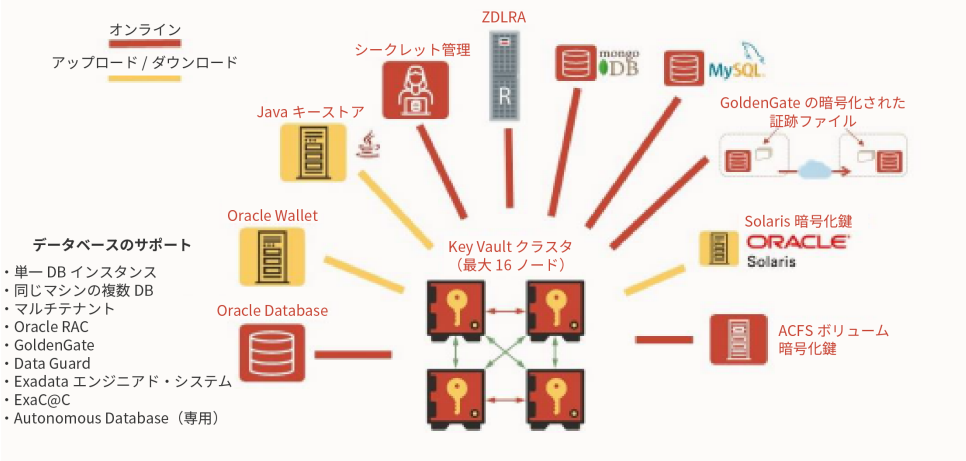
ORACLE

Oracle Key Vault

セキュリティ上の脅威や機密情報の取扱いに対する規制強化を理由に、データセンターでオラクルの透過的データ暗号化（TDE）などの暗号化テクノロジー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、データセンター業務の重要な要素になっています。Oracle Key Vaultを使用すると、企業はスケーラブルで可用性の高い鍵およびシークレット管理により、TDEやその他の暗号化テクノロジーを企業全体でシンプルに導入できます。

はじめに

Oracle Key Vaultでは、透過的データ暗号化（TDE）データベース暗号化鍵、Oracle Wallet、Javaキーストア、資格証明ファイル、およびその他のシークレットを一元管理することで、暗号化をはじめとするセキュリティ・ソリューションを展開できます。高可用性クラスタ・デプロイ・アーキテクチャがサポートされるため、継続的な可用性と地理的な局所性が確保されます。



Oracle Key Vaultは、企業全体でミッション・クリティカルなシステムのセキュアな鍵管理を実現します。

TDEマスター鍵の管理

多くの規制やセキュリティのベスト・プラクティスでは、暗号化鍵を暗号化データと別に保管することが要求されます。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、鍵をサービスでセキュアに管理することによって、Oracle TDEユーザーのこの要件に対処しています。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。

Oracle Key Vaultのユースケース

- TDEを使用したOracle Databaseの鍵管理
- GoldenGateやZDLRAなど、統合されたオラクル製品およびソリューションの鍵管理
- Oracle Databaseおよびアプリケーションのウォレット、キーストア、資格証明ファイルの管理
- 自動化スクリプトを保護するためのシークレット管理
- 機密情報を処理するアプリケーションの鍵およびシークレットの一元管理
- サードパーティ製鍵管理をサポートする、KMIPとの互換性

ORACLE

マスター鍵の共有では、オンプレミス、Exadata Cloud@Customer、Autonomous Database（専用）で実行されるOracle Databaseのほか、Oracle Real Application Clusters（Oracle RAC）、Oracle Data Guard、Oracle GoldenGateなどの選択肢がサポートされます。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、Oracle WalletからOracle Key Vaultに容易に移行できます。

Oracle Wallet、Javaキーストア、その他のシークレットの保護

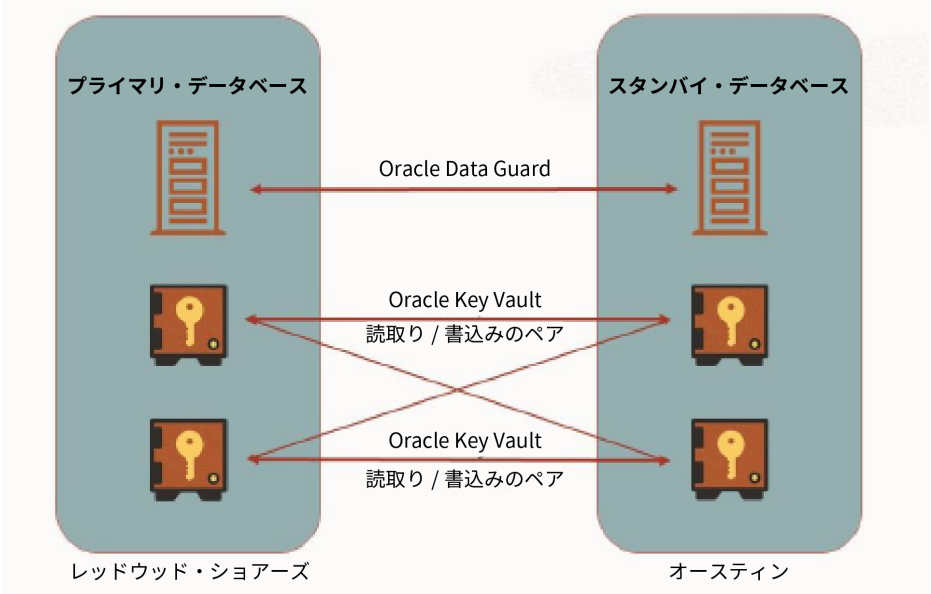
Oracle WalletとJavaキーストアは多くの場合、管理者によってサーバーおよびサーバー・クラスタ全体に手動でコピーされています。Oracle Key Vaultは、Oracle RAC、Oracle Data Guard、Oracle GoldenGateなどのデータベース・クラスタ全体でウォレットの共有を効率化します。ウォレットをセキュアに共有すると、Oracle Data PumpおよびOracle Recovery Manager（Oracle RMAN）を使用して暗号化データの移動も容易に行えます。Oracle Key Vaultはこうしたファイルを安全にアーカイブし、誤って削除したり、パスワードを忘れてしまったりした場合でも、ウォレットとキーストアをリカバリできます。

多くの企業では、SSH鍵を含むエンタープライズ・ファイル、Kerberosキータブ・ファイル、およびシステム・パスワードは、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はこうしたファイルをセキュアに保管し、ファイルへのアクセスを監査し、ファイルを信頼できるエンドポイント全体で共有し、長期的な保存やリカバリに備えてバックアップします。

継続的な可用性とスケーラビリティを実現するクラスタ・アーキテクチャ

Oracle Key Vaultノードは、クラスタの一部として展開され、継続的な可用性と地理的な対応範囲が確保されます。Oracle Key Vaultは1つのクラスタで最大16ノードをサポートし、1つのノードで発生した変更を、クラスタ全体に自動で同期します。

データベースの各エンドポイントは、使用可能なノードの独自リストを透過的に管理し、クラスタへの変更を常に認識しています。現在のノードが使用できなくなった場合、エンドポイントは付近のノードに透過的にフェイルオーバーします。ネットワークの不具合が発生した場合のレジリエンスをさらに高めるために、Oracle Key Vaultにはデータベース・サーバーにキャッシュを作成するオプションがあります。キャッシュを作成することで、全ノードへのネットワーク接続が切断された場合でも、データベースはフル稼働し続けることができます。



デフォルト・ノードが使用できなくなった場合、データベース・エンドポイントは付近のノードに透過的にフェイルオーバーします。

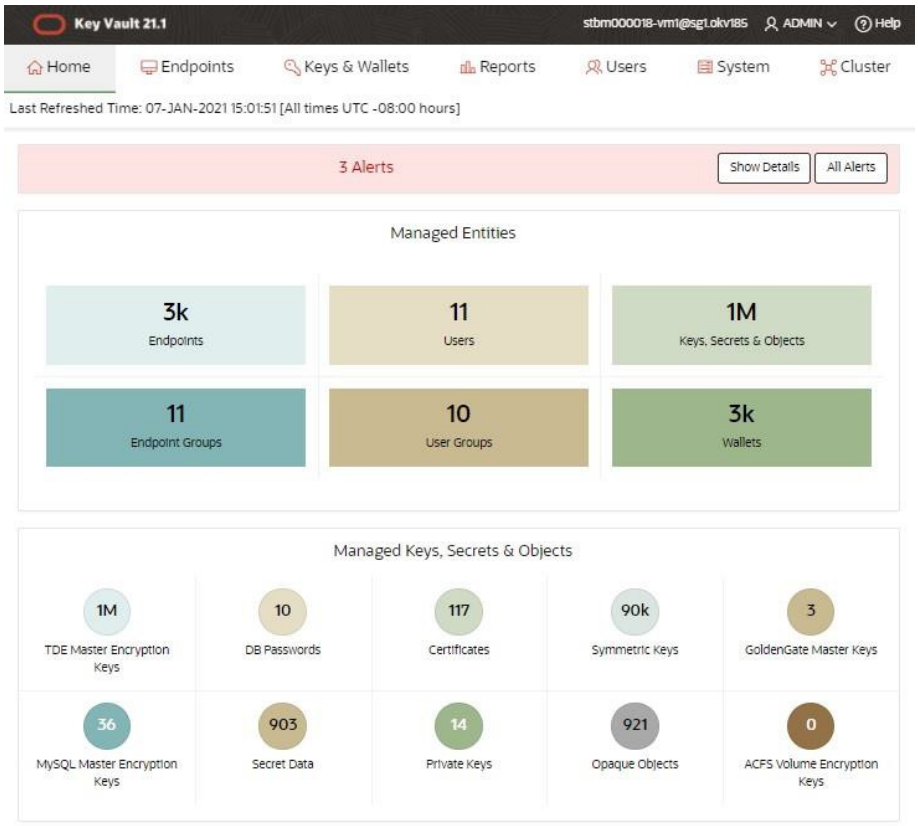
おもな機能

- TDEマスター鍵、Oracle Wallet、Javaキーストア、および資格証明ファイルを管理
- オンラインのTDEマスター鍵管理によって、ローカルの鍵ストアが不要に
- Oracle Cloud MarketplaceからOCIテナンシーに数分でプロビジョニング
- 16台の読取り/書込みノードをサポートし、可用性を維持
- 使用できるノードをエンドポイントが自動選択し、何らかの故障発生時には透過的にフェイルオーバー
- RESTfulサービス一式により、鍵ライフサイクルの管理、エンドポイントの登録、Oracle Key Vaultの管理を自動化
- インメモリと永続キャッシュの各オプションにより、ネットワーク接続が切断された場合も暗号化されたシステムの稼働を継続
- 信頼の起点としてのハードウェア・セキュリティ・モジュール（HSM）と統合
- OASIS KMIP標準をサポート

Oracle Key Vault独自のクラスタ・デプロイ・アーキテクチャは非常にスケーラブルです。ユーザーはデータセンター全体に読取り/書込みノードのペアを展開させて、エンドポイントからローカルのノードに確実にアクセスできるようにし、読取りと書込みの両方の操作を行うことができます。また、クラスタ・アーキテクチャは追加の読取り専用ノードの展開をサポートしているため、小規模なデータセンター向けにローカルの鍵サービスを提供できます。さらに、Oracle Key Vaultの各サーバーは、もっとも要件の厳しいサービスの負荷に対応できるサイズに変更可能な、汎用ハードウェア・プラットフォームに展開されます。結果として、鍵サービスは世界中に展開されたデータベースを多数サポートできるようになり、可用性も非常に高く、高度なサービス・レベルが保持されます。

容易な管理

ブラウザベースの管理コンソールにより、Oracle Key Vaultサーバーの管理、クラスタの管理、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作成を容易に行うことができます。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。エンドポイントの登録とプロビジョニングは、保護されたRESTfulインタフェースを使用して自動化し、データベースに大規模展開できます。



Oracle Key Vaultの管理コンソールでは、管理下にあるさまざまなセキュリティ・オブジェクトを一目で把握できます。

ソフトウェア・アプライアンスの保護

エンタープライズ規模の展開では、セキュリティは必須要件の1つです。Oracle Key Vaultは、インフラストラクチャ、管理、および操作などの複数のレイヤーで、セキュリティを確保します。Oracle Key Vaultの提供形態はISOイメージで、事前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インストールされます。

ビジネス上のおもなメリット

- 規制遵守に備えて、鍵と暗号化データを分離
- 鍵ストアの統合により、リスクを軽減させ、コストを削減
- 鍵とシークレットを不注意による紛失や盗難から保護
- ソフトウェア、ハードウェア、またはネットワークに不具合が発生した場合も、鍵とシークレットの可用性を維持
- データセンター全体で非常に多くのデータベースにスケーリング
- ノードをアイドル状態にさせずにハードウェアのコストを削減
- 監査によって鍵管理のライフサイクルのアカウンタビリティを万全に

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ます。たとえば、Oracle Key Vaultは組込みのOracle Database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ます。また、無許可の特権ユーザー・アクセスを制限するために、Oracle Database Vaultを使用します。

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、セキュリティ業務を分離できます。Oracle Key Vaultは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します。監査データをOracle Audit Vault and Database Firewall（Oracle AVDF）またはsyslogサーバーに転送して、レコードを保持したりレポートを作成したりできます。また、リモート監視のためにSNMP v3をサポートしています。

Oracle Key Vaultをハードウェア・セキュリティ・モジュール（HSM）と統合して、パッチ適用およびアップグレード時に、鍵、証明書、その他のセキュリティ・アーティファクトのセキュリティを強化できます。この場合、HSMが信頼の起点となってウォレットのパスワードが保護され、これによってTDEのマスター鍵が保護され、結果として暗号化鍵、証明書といった、Oracle Key Vaultサーバーで管理されているすべてのセキュリティ・アーティファクトが保護されます。

オンプレミスとOracle Cloudでの展開

Oracle Key Vaultはインストールが容易で、ユーザーが選択したx86-64互換ハードウェアに導入できます。Oracle Cloud Marketplaceからも入手でき、OCIテナンシーに数分で展開できるため、オンプレミス、ハイブリッド・クラウド、またはマルチクラウドのデータベース・デプロイメントにフォルト・トレラントで継続的な鍵管理サービスを提供できます。Oracle Linux、Red Hat Linux、Solaris SPARC、Solaris x64、IBM AIX、HP-UX（IA）、Microsoft Windowsなどの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ます。

関連製品

Oracle Key Vaultは、重要なデータベース・セキュリティ管理です。
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 Data Safeクラウド・サービス

オラクルの情報を発信しています

+1.800.ORACLE1までご連絡いただくか、oracle.comをご覧ください。北米以外の地域では、oracle.com/contactで最寄りの営業所をご確認いただけます。

blogs.oracle.com　facebook.com/oracle　twitter.com/oracle