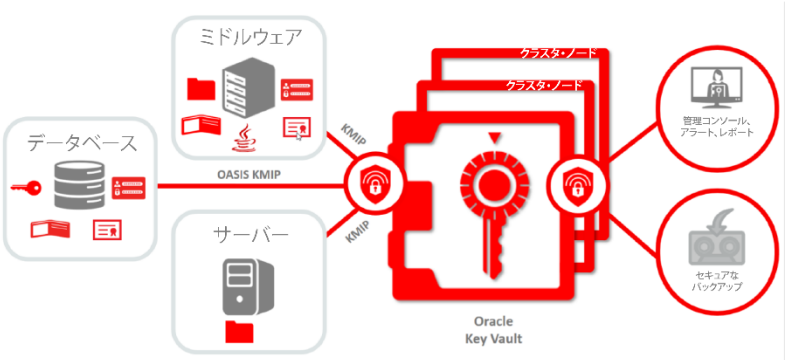
Orale Key Vault

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に対するセキュリティ上の脅威や規制強化を理由に、データセンターでのオラクル**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、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は、**非常に拡張性が高く、常時使用可能な鍵管理**であり、企業全体に暗号化をシンプルに導入できます。

はじめに

Oracle Key Vaultで、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、資格証明ファイルを一元管理することで、暗号化などのセキュリティ・ソリューションを展開できます。Oracle Key Vaultは高可用性クラスタ・デプロイ・アーキテクチャをサポートしているため、鍵サービスの継続的な可用性が維持され、地理的な対応範囲が確保されます。



Oracle Key Vaultの導入の概要

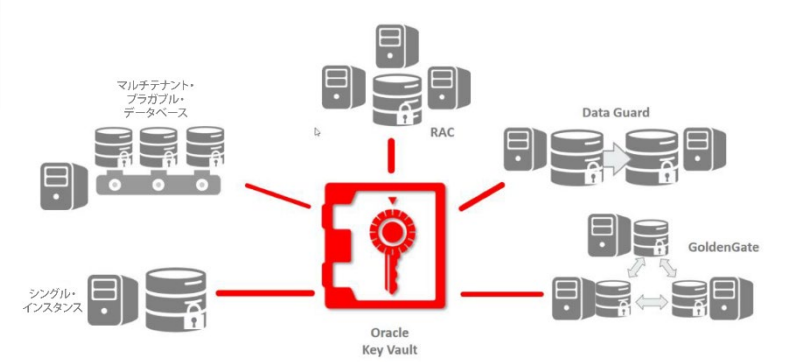
おもな機能

- 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
- 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・ユーティリティによりエンドポイントの登録を自動化
- RESTful API でキーの作成、無効化、削除を自動化
- ネットワーク接続が切断された場合でも、オプションの永続キャッシュにより、暗号化データベースの稼働を継続
- Oracle Wallet から Oracle Key Vault に鍵を移行
- ハードウェア・セキュリティ・モジュール（HSM）との統合
- OASIS KMIP 標準をサポート
- 事前構成済みの安全なソフトウェア・アプライアンスにより導入を簡素化

ORACLE

透過的データ暗号化のマスター鍵管理

Oracle Key Vault は、暗号化鍵と暗号化データを物理的に分離します。規制遵守のためにこのような分離が必要になることは珍しくありません。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。マスター鍵の共有では、Oracle Real Application Clusters（Oracle RAC）、Oracle Data Guard、Oracle GoldenGate に加えて、Oracle Multitenant データベース・インスタンス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 Key Vaultは、オンラインでマスター鍵を管理できます。ローカルのウォレットは不要です。

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
- 鍵や資格証明を、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に、鍵の可用性を維持
- 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

Oracle Wallet、Java キーストア、および資格証明ファイルの管理

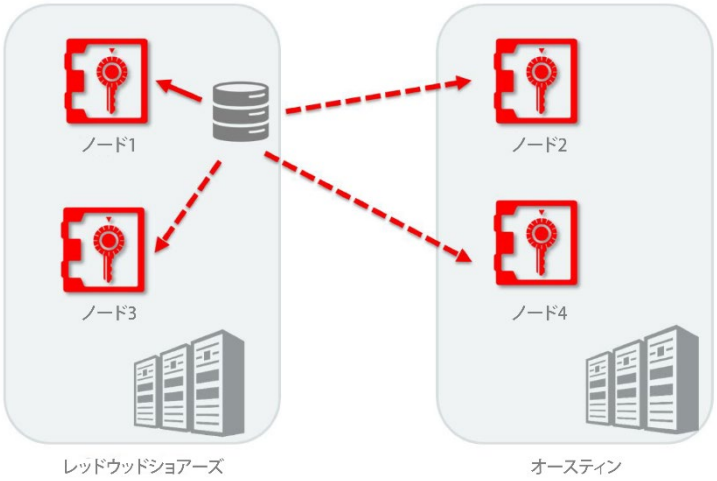
Oracle Wallet と Java キーストアは多くの場合、管理者によってサーバーおよびサーバー・クラスタ全体に手動でコピーされています。Oracle Key Vault は、Oracle RAC、Oracle Data Guard、Oracle GoldenGate などのデータベース・クラスタ全体でウォレットの共有を効率化します。ウォレットをセキュアに共有すると、Oracle Data Pump および Oracle Recovery Manager（Oracle RMAN）を使用して暗号化データの移動も容易に行えます。Oracle Key Vault はこうしたファイルを安全にアーカイブし、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 鍵を含む資格証明ファイル、Kerberos キータブ・ファイル、および類似の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 は長期保存やリカバリを目的として、資格証明ファイルをバックアップします。Oracle Key Vault はこうしたファイルを必要なときに簡単にリカバリし、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ファイルを共有します。

可用性と拡張性が継続的に維持されるクラスタ・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・サーバーに永続キャッシュを作成するオプションがあります。そうすれば、全ノードへのネットワーク接続がダウンした場合でも、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。

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。

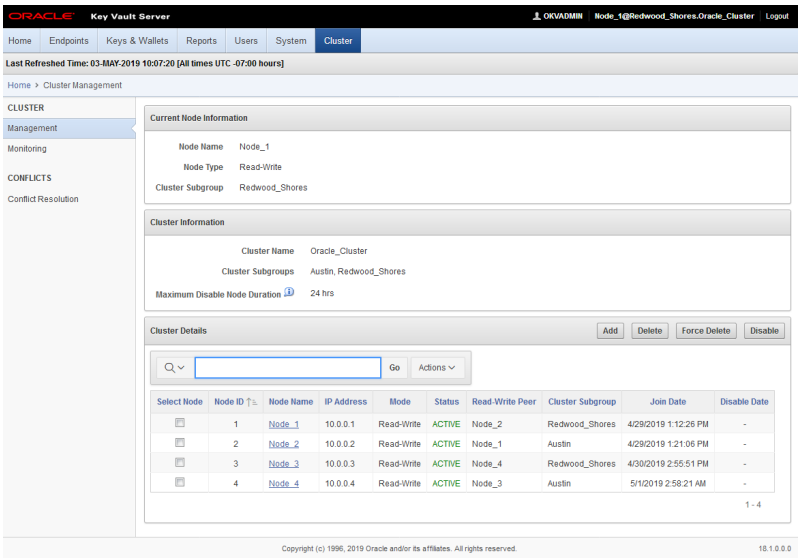
管理

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。

セキュリティ

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。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。



Oracle Key Vaultの管理コンソールは、クラスタからノードを追加したり削除したりするタスクを簡素化します。

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。そのため、物理的にアクセス可能なシステムから管理者が鍵や資格証明を取り出すという潜在的リスクが軽減されます。

米国連邦情報処理標準（FIPS）に準拠する必要がある組織では、Oracle Key Vault は FIPS 140–2 準拠のオプションでインストールされます。このオプションを選択すると、必要なすべての変更がインストール中に実行され、FIPS 140–2 に準拠したライブラリのみが Key Vault サーバーのオペレーティング・システム、組込みの Oracle Database、およびその他のコンポーネントによって使用されるようになります。また、信頼の起点として展開された FIPS 140–2 認証済み HSM が、コンプライアンス上のこうした要件を満たすために利用されます。

インストールとエンドポイントのサポート

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 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。

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。

Integrated Cloud Applications & Platform Services

ORACLE