ORACLE

Oracle Key Vault：よくある質問

エンタープライズ向けの鍵およびシークレット管理

2024年3月、バージョン21.8

公開

ORACLE

目次

ORACLE

概要

Oracle Key Vaultを使用すると、暗号化鍵、Oracleウォレット、Javaキーストア、SSH鍵ペア、およびその他のシークレットが、スケーラブルでフォルト・トレラントな高可用性クラスタに安全に格納されます。ユーザーは、Oracle Cloud Infrastructure（OCI）、Microsoft Azure、Amazon AWS、および専用ハードウェアまたは仮想マシンのオンプレミス環境にKey Vaultサーバーを導入できます。Key Vaultでは、OASIS KMIP標準がサポートされます。

このドキュメントでは、Oracle Key Vaultの機能、ユースケース、導入に関するよくある質問に回答しています。

機能

Oracle Key Vaultで管理できる鍵およびシークレットの種類を教えてください。

Oracle Key Vaultでは、以下を一元管理できます。

- Oracle Advanced Securityの透過的データ暗号化（TDE）のマスター暗号化鍵
- リモート・サーバー・アクセス制御および一元管理される公開鍵認証のSSH鍵ペア
- Oracleウォレット
- Javaキーストア
- Kerberosキータブ・ファイル
- GoldenGate証跡ファイルのマスター暗号化鍵
- Oracle ACFS（Oracle ASM Cluster File System）のボリューム暗号化鍵
- ZFS Storage Applianceのマスター暗号化鍵
- MySQL TDEのマスター暗号化鍵
- MongoDBのマスター暗号化鍵
- dbms_cryptoの暗号化鍵

Oracle Key VaultでOracleウォレットを管理できますか。

Oracle Databaseサーバーおよびクライアントは、Oracleウォレットを使って、Oracle Advanced Securityの透過的データ暗号化（TDE）マスター鍵や証明書、サーバー・パスワード、接続文字列を格納します。Oracleウォレットは標準PKCS #12ファイルであり、パスワードから生成された鍵で暗号化されています。Oracle Key Vaultは、Oracleウォレットのコンテンツを項目化したものを一元的に格納し、管理します。これにより、サーバー・クラスタ間でウォレット・コンテンツの共有が可能になります。Oracle Key Vaultでは、ウォレット・コンテンツへのアクセス権も監査されます。

Oracle Key Vaultでは、鍵やウォレット、キーストアの共有を容易にするために、どのような手法を使用していますか。

Oracle Key Vault管理者は、関連するサーバー・エンドポイントと一連の鍵およびシークレットとの間にアクセス制御ポリシーを定義できます。Oracle Key Vault内の一連の鍵およびシークレットは仮想ウォレットと呼ばれます。仮想ウォレットをエンドポイントに割り当てると、すべてのサーバー・エンドポイントが仮想ウォレットのコンテンツにアクセスできるようになります。この共有方法は、Javaキーストアが必要なOracle Data Guard、Oracle Real Application Clusters（Oracle RAC）、シャード・データベース、ミドルウェア・サーバーを使用したデータベースに有用です。

ORACLE

TDEオンライン・マスター暗号化鍵の管理

Oracle Key Vaultを使用したオンラインTDE鍵管理の利点は何ですか。

Oracle Key VaultでTDE鍵が一元管理されることで、数百または数千のデータベースでTDEを実行している場合は特に、管理が容易になります。暗号化データをホスティングしているサーバーとは別の場所で暗号化鍵を保守することは、多くのコンプライアンス要件に対処するためにも不可欠です。Oracle Key Vaultで鍵管理を一元化すると、Oracle RACインスタンスとスタンバイ・データベース全体でのセキュアな鍵共有が容易になります。鍵管理の一元化によって、鍵の管理、バックアップ、取消し、一時停止、回復が可能になるため、最終的にガバナンスとセキュリティが向上します。

Oracle Key VaultではどのOracle Databaseがサポートされますか。

UNIXおよびWindowsエンドポイント・プラットフォームで実行されている、バージョン12.1.0.2～23cのすべてのOracleデータベースで、Oracle Key Vaultのオンライン・マスター暗号化鍵管理を利用できます。オンプレミスのOracle Databaseに加えて、仮想マシン、OCIのコンピュート・インスタンス、サード・パーティ・クラウドで実行中のデータベースでも利用できます。Oracle Key Vaultでは、Oracle Cloud at Customerデータベース（ExaDB-C@CおよびADB-C@Cを含む）、Oracle Exadata Database Service on Dedicated Infrastructure（ExaDB-DおよびExaDB-D@Azure）もサポートされます。サポート対象のエンドポイント・プラットフォームについて詳しくは、Oracle Key Vaultのドキュメントを参照してください。

Oracle TDEマスター鍵は、Oracle Key Vaultに移行した後も、Oracleウォレットで保守する必要がありますか。

いいえ。Oracle Databaseで透過的データ暗号化（TDE）を使用している場合、ローカル・ウォレット・ファイルを使用する代わりに、Oracle Key VaultでTDEマスター鍵を一元管理できます。現行の鍵と廃止済みのすべての鍵をウォレットからOracle Key Vaultにアップロードした後に、SQL*Plusコマンドの"ADMINISTER KEY MANAGEMENT MIGRATE"を実行すれば、暗号化されたデータベースをOracle Key Vaultに容易に移行できます。詳しくは、Oracle Key Vaultのドキュメントを参照してください。

Oracle Key VaultはTDE暗号化のパフォーマンスに影響を与えますか。

TDEマスター鍵は、Oracle Key Vaultからアクセスされ、データ暗号化鍵の複号化に使用されます。データ暗号化鍵は不明瞭化され、データベースにキャッシュされるため、Oracle Key Vaultを使用してもTDEのパフォーマンスには影響しません。

SSH鍵管理

Oracle Key Vaultを使用してSSH鍵を格納および管理する利点は何ですか。

管理者は、SSH鍵を使用してサーバーやITシステムにアクセスするため、クラウド・コンピューティングの拡大に伴い、SSH鍵の使用は急激に増加しています。公開鍵認証に使用される管理対象外のSSH鍵ペアは、セキュリティと管理における課題です。Oracle Key Vaultは、次の2つの方法で、組織がSSH鍵の管理を向上できるよう支援します。

- **アクセス制御の一元化** – ユーザーのSSHホスト用公開鍵をOracle Key Vaultで管理すると、システムへのアクセスの提供と取消しを管理者が容易に管理できるようになります。管理者は、ユーザーの公開鍵を、Oracle Key Vault内の特定のSSHサーバー・ウォレットにアップロードすることで、そのユーザーがリモート・サーバーにアクセスできるようにすることができます。リモート・サーバーへのアクセスを拒否するには、SSH管理者は拒否するユーザーの公開鍵をSSHサーバー・ウォレットから削除するだけで済みます。SSH公開鍵の管理を一元化すると、管理者はアクセス試行の追跡とレポート作成が可能になります。

- **SSH鍵のガバナンス向上** – フォルト・トレラントかつスケーラブルで、継続的な可用性を備えた鍵管理システムで秘密鍵と公開鍵の両方を一元管理すると、鍵のガバナンスを向上できます。企業は鍵管理の一元化によって、必要な鍵の長さやアルゴリズム、定期的な鍵のローテーション、鍵の使用状況のレポート作成や監査など、自社のセキュリティ・ポリシーを強化できます。さらに管理者は、セキュリティ・インシデントが継続した場合に、すべてのリモート・アクセスを迅速に制限できます。Key Vault内でSSH公開鍵とSSH秘密鍵のペアを生成し、秘密鍵を抽出できない（Key Vaultクラスタ境界を離れることができない）ようにすることで、SSH鍵のセキュリティを強化できます。ユーザーの公開鍵を、Key Vault内のSSHサーバー・ウォレットにコピーすれば、ユーザーはサーバーにアクセスできるようになります。リモート・サーバーへのアクセスを試行しているエンドユーザーは、a）リモート・サーバーのSSHウォレットに公開鍵が存在し、b）Key Vault内の一致する秘密鍵にアクセスできれば、アクセスは成功します。Key Vault内で鍵を管理すると、ディスクベースの秘密鍵に付随するリスク（鍵の盗難、不正コピー、共有、紛失など）が低減されます。

SSHユーザー管理とOracle Key Vaultはどのように連携していますか。

鍵の管理者は、標準のSSHコマンドを使用して、Oracle Key VaultにSSHユーザーのSSH鍵ペアを作成できます。Oracle Key VaultのPKCS-11ライブラリを一度だけインストールすれば、SSHクライアントは、Oracle Key Vaultの署名を利用して、SSHホストへのアクセスを提供する機能を検証できます。秘密鍵をクライアントに保管する必要はありません。

SSHアクセス管理とOracle Key Vaultはどのように連携していますか。

Oracle Key Vaultの管理者は、各SSHホスト・ユーザーのために、Oracle Key Vaultに仮想ウォレットを作成できます。一度だけエンドポイント・ソフトウェアをインストールし、SSHホストでSSHデーモンを構成すれば、これらのホストは、SSH接続リクエスト時にOracle Key Vaultの仮想ウォレットに動的にアクセスできます。SSHユーザーがSSHホストにアクセスできるようにするには、そのユーザーの公開鍵をホストの仮想ウォレットに追加するだけです。SSHユーザーの公開鍵をOracle Key Vaultの仮想ウォレットで管理すると、SSHホストへのユーザー・アクセスの提供、提供解除、および一時停止を一元化でき、アクセスとアクティビティのレポート機能を向上できます。秘密鍵と公開鍵をOracle Key Vaultで管理することで、鍵の管理者は、SSHユーザーやクライアント・ソフトウェアの介入なしでSSH鍵をローテーションできます。

規模

Oracle Key Vaultで格納および管理できる鍵の数を教えてください。

Oracle Key Vaultでは、数十万個の鍵を格納して管理できます。

Oracle Key Vaultで管理できるサーバー・エンドポイントの数を教えてください。

ほとんどのエンドポイントは断続的にOracle Key Vaultアプライアンスに接続します。そのため、Oracle Key Vaultクラスタは数千のエンドポイントに対応できます。追加のKey Vaultサーバーを既存のクラスタに導入することで、エンドポイントの数を増やし、可用性と局所性のレベルを向上できます。

鍵の可用性とバックアップ

Oracle Key Vaultでは、鍵の継続的な可用性をどのように実現していますか。

ユーザーは、最大16個のOracle Key Vaultインスタンスを導入して、鍵管理クラスタを形成できます。これにより、地理的に分散されたオンプレミス・データセンターとクラウド・データセンターを網羅できる可能性があります。鍵はクラスタ内のすべてのノードで共有されるため、エンドポイントは利用可能な任意のノードにアクセスすれば、自身の鍵にアクセスできます。

Oracle Key Vaultでは、鍵の紛失の可能性をどのように軽減していますか。

各Oracle Key Vaultクラスタには、同期されたKey Vaultノードのペアが少なくとも1つ存在します。エンドポイントが新しい鍵をペアの一方のノードに書き込むと、そのノードと同期されるもう一方のノードが更新されるまで、更新処理は完了しません。これらの同期ペアをリージョンやデータセンター全体に分散させれば、ハードウェアや施設の障害が発生しても、鍵の更新を確実に記録できます。

Oracle Key Vaultアプライアンスをバックアップする方法を教えてください。

Oracle Key Vaultは、手動でバックアップすることも、構成可能なスケジュールに基づいて自動的にバックアップすることもできます。バックアップ・プロセスでは、内部のバックアップ・スクリプトが実行され、バックアップ・ファイルが暗号化されてから、セキュアな接続を介して暗号化バックアップ・ファイルがリモートの宛先に自動的に移動されます。詳しくは、Oracle Key Vaultのドキュメントを参照してください。

管理

Oracle Key Vaultを管理する方法を教えてください。

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。また、Key Vaultには、アップグレードやパッチ適用などの管理機能を実行できるコマンドライン・インタフェースが用意されています。さらに、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でユーザーを一元管理する方法を教えてください。

Oracle Key Vaultコンソール・ユーザーは、ローカルに管理することも、Microsoft Active Directoryとの統合によって一元管理することもできます。コンソールでは、SAMLトークンを使用したユーザー認証もサポートされているため、Azure Active Directory（Azure AD）、Active Directoryフェデレーション・サービス（ADFS）などのフェデレーション・アイデンティティ・プロバイダに認証されたユーザーに、シームレスなシングル・サインオン体験が提供されます。

Oracle Key Vaultで管理上の職務分離を行う方法を教えてください。

Key Vaultの管理者ロールを鍵、システム、監査の各管理機能に分割することで、職務を分離できます。管理を容易にするために、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各自の鍵およびウォレットへのアクセス権限を付与できます。

セキュリティ

Oracle Key Vaultでは、格納された鍵とシークレットはどのように保護されていますか。

Oracle Key Vaultでは、さまざまなOracle Databaseセキュリティ・テクノロジーを使用して、格納されている鍵とシークレットを保護しています。使用するテクノロジーには、鍵とシークレットを暗号化して機密性を維持するOracle Advanced Securityの透過的データ暗号化、特権ユーザーへの機密データ公開を防止するOracle Database Vault、ユーザー・レベルでアクセスを制御するOracle Virtual Private Databaseが含まれます。Oracle Key Vaultでは、格納されている鍵とシークレットへのすべてのアクセスが監査されます。分析と統合のために、監査ログをOracle Audit Vault and Database Firewallに転送することもできます。

Oracle Key Vaultとエンドポイント間で鍵はどのように転送されますか。

データベース・サーバーやミドルウェア・サーバーなどのエンドポイントは、Oracle Key Vaultサーバーとの通信に、相互認証されたセキュアなTLS 1.2転送で固定ポート5696を介してOASIS KMIP（Key Management Interoperability Protocol）を使用します。ブラウザ・ベースのOracle Key Vault管理コンソールは、HTTPS（固定ポート443）を使用します。ブラウザ・ベースの管理コンソールはサード・パーティ製の証明書をサポートしています。

Oracle Key VaultではFIPSモードを有効化できますか。

Oracle Key Vaultでは、FIPS 140–2モードでのインストールがサポートされます。FIPS 140–2モードを使用してインストールするオプションを選択すると、インストール中に必要な変更がすべて実行されます。FIPS 140-2モードは、インストール後に有効化することもできます。

Oracle Key Vaultと自社のHSMを統合できますか。

はい。ハードウェア・セキュリティ・モジュール（HSM）がOracle Key Vaultとともに導入されている場合、信頼の起点（RoT）はHSMにとどまります。信頼の起点としてのHSMによ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マスター鍵が保護され、その結果、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。この3つの階層により、管理者が物理的にアクセスできるシステムから鍵や資格証明を抽出するリスクが緩和されます。信頼の起点を使用したこのシナリオでは、顧客の暗号化鍵はHSMに格納されません。顧客の鍵は、Oracle Key Vaultサーバーに直接格納され、管理されます。信頼の基点としてのOracle Key Vaultの認証済みHSMについて詳しくは、Oracle Key Vaultのドキュメントを参照してください。

インストール要件とハードウェア要件

Oracle Key Vaultはどのように提供されますか。

Oracle Key Vaultはソフトウェア・アプライアンスとしてパッケージ化されています。パッケージには、オペレーティング・システムのほか、専用ハードウェアに、または仮想マシンとして本製品をインストールするために必要なものすべてが含まれています。インストール中にKey Vaultインストーラによってディスクのパーティション化とフォーマットが行われ、ベースOS、ユーザースペース・ライブラリ、Oracle Database、およびOracle Key Vaultソフトウェアがインストールされます。ユーザーの介入を最小限に抑えて、すべてのソフトウェア・コンポーネント（OS、ネットワーク、データベース）が自動的に構成されます。システム強化のベスト・プラクティスに従って、オペレーティング・システム、ネットワーク構成、データベースが強化されます。また、不要なパッケージとソフトウェアは削除され、未使用のサービスとポートは無効化されます。

専用ハードウェア上のOracle Key Vaultに推奨されるハードウェア仕様を教えてください。

Oracle Key Vaultソフトウェア・アプライアンスを導入するための最小ハードウェア要件は以下のとおりです。

- CPU：最小：x86-64 16コア。推奨：暗号化アクセラレーション・サポート（インテルAES-NI）付きの24～48コア。
- メモリ：最小16 GBのRAM。推奨：32～64 GB。
- ディスク：最小2 TB。推奨：6 TB。

  Oracle Key Vaultでは、BIOSとUEFIの両方のブート・モードがサポートされます。ディスク・サイズが2 TBを超えるシステムでは、Oracle Key VaultはUEFIモードのブートのみに対応しています。

  注：Oracle Key Vaultでは、ブート・ディスクにマルチパスを使用したファイバー・チャネル・ストレージはサポートされません。

すべての要件については、Oracle Key Vaultのドキュメントを参照してください。

OCIにOracle Key Vaultを導入できますか。

はい。Oracle Cloud infrastructureにOracle Key Vaultを導入する最も簡単な方法は、Oracle Cloud Marketplaceから導入することです。

サード・パーティのクラウドにOracle Key Vaultを導入できますか。

サード・パーティのクラウドでOracleデータベースを実行しているお客様は、データベースと一緒に1つまたは複数のOracle Key Vaultノードを導入することで、ネットワークの待機時間を最小限に抑えることができます。Microsoft AzureおよびAmazon Web Services（AWS）のコンピュート・ノードにKey Vaultを導入すると、同様のフォルト・トレラント性、高いスケーラビリティ、および高可用性を備えた鍵およびシークレット管理ソリューションを実現できます。最大16個のKey Vaultノードを、単一クラスタの一部として稼働させることができ、OCI、オンプレミス・データセンター、またはお客様の要件に基づいてこれらを組合せた環境に展開できます。

Oracle Key Vaultのソフトウェアはどこでダウンロードできますか。

Oracle Key Vaultは、以下のようにOracle Software Delivery Cloudからダウンロードできます。https://edelivery.oracle.comに移動し、"Oracle Key Vault"を検索します。「Continue」を選択し、「Oracle Key Vault, Platform Linux x86-64」を選択して.isoイメージをダウンロードします。

仮想マシンにOracle Key Vaultを導入する際に利用できる機能を教えてください。

Oracle Key Vaultでは、クローン・テンプレートがサポートされています。この機能を使用すると、Oracle Key Vaultノードをさらに追加して、複数のデータセンターに分散されたデータベースの高可用性やローカル・アクセスを実現できます。Oracle Key Vaultテンプレートをクローニングした後に、少数のRESTコマンドを実行すれば、ノードをOracle Key Vaultクラスタに数分で追加できます。クラスタの作成、ノードの追加、ノードの削除を自動化することもできます。

対象のエンドポイントとの統合

エンドポイント・ソフトウェアのダウンロード方法と導入方法を教えてください。

Oracle Key Vaultを使用して鍵およびシークレットを管理するデータベース・サーバー、ミドルウェア・サーバー、およびシステムは、エンドポイントと呼ばれます。Oracle Key Vault管理コンソールは、必要なエンドポイント・ソフトウェアをダウンロードおよびプロビジョニングするためのリンクを提供します。エンドポイント・ソフトウェア・パッケージには、必要なバイナリと構成ファイルがすべて含まれており、エンドポイントとOracle Key Vault間に相互認証されたセキュアな接続を確立するためのTLS証明書も含まれています。Key Vaultシステム管理者がエンドポイントを登録すると、Oracle Key Vaultによってワンタイムの登録トークンが自動的に生成されます。エンドポイント管理者は、この登録トークンを使ってエンドポイント・ソフトウェアをダウンロードします。Oracle Key Vaultはテスト環境内での自己登録に対応しており、管理者の関与を最小限に抑えます。

エンドポイントの構成とプロビジョニングには、どのくらいの停止時間を計画する必要がありますか。

エンドポイントでOracleウォレットまたはJavaキーストアをOracle Key Vaultにアップロードする場合、停止時間は必要ありません。Oracle DatabaseでTDEマスター鍵をOracleウォレットからOracle Key Vaultに移行する場合、停止時間は発生しません。

機能の互換性

Oracle Key Vaultでサポートされ ているOracleデータベースとミドルウェアのバージョンを教えてください。

Oracle Key VaultでオンラインTDE鍵管理がサポートされるのは、Oracle Linux、Red Hat Linux、SuSE Linux Enterprise Server、Solaris Sparc、Solaris x64、AIX、HP-UX、およびWindows上のOracle Database 12.1.0.2～23cです。また、Oracleウォレットのアップロード元とリストア元としてサポートされるのは、Oracle Linux、Red Hat Linux、SuSE Linux Enterprise Server、Solaris Sparc、Solaris x64、AIX、HPUX、およびWindows上のすべてのサポート対象Oracleミドルウェア・リリースとOracle Databaseリリースです。

Oracle Key Vaultでサポートされている鍵格納ファイルの種類を教えてください。

Oracle Key Vaultは、OracleウォレットとJavaキーストア（JKSおよびJCEKS）の鍵格納ファイルをサポートしています。Oracle JDK 1.4、1.5、1.6、7、8を使ったJavaキーストアがテストされています。

Oracle Key Vaultに格納できる資格証明ファイルの種類を教えてください。

Oracle Key Vaultには、Kerberosキータブ やSSH鍵の格納ファイルなど、任意の資格証明ファイルを格納できます。一元管理する資格証明ファイルはどのようなファイルでも構いません。Oracle Key Vaultにアップロードするには、1つの資格証明ファイルのサイズが128 KB未満である必要があります。

Oracle Key Vaultで機密データを暗号化できますか。

Oracle Key Vaultは、データを暗号化するエンドポイントの鍵とシークレットを管理します。データの署名と検証処理もサポートしています。Oracle Key Vaultでは、鍵やシークレットといった管理対象データが暗号化されますが、データの暗号化はエンドポイントの責任となります。

Oracle Key VaultでDBMS_CRYPTO鍵を管理できますか。

はい。本製品には、JavaおよびC言語のSDKが含まれています。このSDKを使用して、DBMS_CRYPTOアプリケーションとOracle Key Vaultを統合できます。

詳細情報

Oracle Key Vaultに関する詳細情報の入手先を教えてください。

詳細情報については、Oracle.comのOracle Key Vaultのページを参照してください。このページには、データ・シート、ホワイト・ペーパー、顧客事例、製品ドキュメントなどの役立つ情報へのリンクが記載されています。Oracle Key Vaultをお試しになる場合は、Oracle LiveLabsにアクセスしてください。

ORACLE

Connect with us

+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