ORACLE
Key Vault

Oracle Key Vault

Oracle Key Vault（Oracle KV）により、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し、暗号化と他のセキュリティのための堅牢なソリューションを容易にデプロイすることができます。このドキュメントでは、Oracle Key Vaultのインストールとデプロイメントに関するよくある質問を取り上げます。

機能

Oracle Key Vaultを使用して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を使用することにより、Oracle Advanced Security Transparent Data Encryption（TDE）のマスター暗号化鍵、Oracle Wallet、Javaキーストア、SSH鍵格納されているファイルやKerberosキータブ・ファイルなどの資格証明ファイルを一元管理できます。また、MySQL TDEマスター暗号化鍵やOracle ACFS（Oracle ASM Cluster File System）のボリューム鍵も管理できます。

Oracle Key Vaultでは、どのような方法で、鍵、ウォレット、キーストアを共有しやすくしていますか。

Oracle Key Vaultの管理者は、関連するサーバーの一連のエンドポイントと、一連の鍵およびシークレットの間のアクセス制御ポリシーを定義できます。サーバーの一連のエンドポイントはエンドポイント・グループとして定義されます。Oracle Key Vaultにおける一連の鍵とシークレットは、仮想ウォレットと呼ばれます。仮想ウォレットがエンドポイント・グループに割り当てられると、サーバーのエンドポイントは仮想ウォレットのコンテンツにアクセス可能になります。この共有手法は、Data GuardかReal Application Clusters（RAC）を使用するデータベースやJavaキーストアが必要なミドルウェア・サーバーの場合に適しています。

Oracle Key Vaultでは、どのような方法でOracle Walletを管理しますか。

Oracleデータベースのサーバーとクライアントでは、Oracle Walletを使用して、Oracle Advanced Securityの透過的データ暗号化（TDE）のマスター鍵、証明書、サーバーのパスワード、接続文字列を保管します。Oracle Walletは、パスワード派生鍵によって暗号化されている標準PKCS#12ファイルです。Oracle Key Vaultは、Oracle Walletの項目別のコンテンツを一元的に保管および管理します。これにより、サーバー・クラスタどうしでウォレットのコンテンツを共有することができます。またOracle KVは、ウォレットのコンテンツへのアクセスも監査します。

規模

Oracle Key Vaultでは、いくつの鍵を保管および管理可能ですか。

Oracle Key Vaultでは、数十万個の鍵を保管および管理できます。

ORACLE

Oracle Key Vaultでは、いくつのサーバー・エンドポイントを管理可能ですか。

ほとんどのエンドポイントは断続的にしかOracle Key Vaultアプライアンスに接続しないため、1,000以上のエンドポイントをOracle Key Vaultでサポート可能です。

Oracle Key Vault 18へのアップグレード

Oracle Key Vault 12.xから18に直接アップグレードすることはできますか。

Oracle KV 18のリリース・ノートの指示に従って、アップグレードにいくつのステップが必要なのか確認してください。

どうすれば、'オンライン・マスター鍵'を使って構成されているデータベースのエンドポイントの停止時間を最小限に抑えてOracle KV 18にアップグレードできますか。

まず、"既知の問題"を十分に把握してから、現行の本番Oracle KVバージョンに適合するテスト環境でアップグレード・サイクル全体を通しで実行することを強くお勧めします。

1) Oracle KVのWeb GUIで、「Persistent Cache」のタイムアウトを3日以上に設定します。
   a) 「Endpoints」タブにナビゲートします。
   b) 「Settings」を選択します。
   c) 「Global Endpoints Configuration Parameters」で「Save Default」をクリックして、テキスト・フィールドに現在のデフォルト値を入力します。
   d) 「PKCS11 Persistent Cache Timeout」の値を、1,440分から4,320分（3日）以上に変更します。
   e) 「Save」をクリックします。

個別の設定が保存されているためにグローバル・エンドポイント設定を使用していない各エンドポイントは、「Endpoint Details」ページの「Clear All」ボタンを使用してグローバル・エンドポイント設定に戻すか、またはその「PKCS11 Persistent Cache Timeout」を4,320分（以上）に設定する必要もあります。

2) すべてのデータベースは、必須の鍵再設定を行って「Persistent Cache」の現在のマスター鍵を新しい"契約"（有効期限）で更新します。DBAは、すべての永続キャッシュ（スタンバイ・データベース、Oracle RACのノンリーフノードなど）が更新されたことを検証した後に、確認してOracle KVの所有者に報告します。
3) Oracle KVの所有者がすべてのエンドポイントを一時停止します。
4) "信頼の起点"が構成されている場合は、HSMからの移行を逆にします。
5) Oracle KVの所有者がすべての鍵を含めてフル・バックアップを作成します（一時停止されたエンドポイントがその「Persistent Cache」の使用を強制されるため、新しい鍵を作成することはできません）。
6) Oracle KVがアクティブ・プライマリ/パッシブ・スタンバイ・モードで実行されている場合は、HA構成を解除します。
7) 古いスタンバイOracle KVが消失します。新しいOracle KV 18をこのホストにインストールします（OKV02以上）。並行して、古いプライマリOracle KV 12.2を18.1にアップグレードします。すべての鍵が保管されているため、これが初期ノード（OKV01）となります。任意で、クラスタに追加する前にすべてのOracle KV 18.1で信頼の起点を構成します。
8) 設定ガイドの指示に従って、2つのスタンドアロンOracle KV（7から）18.1を最初の読取り/書込みペアOKV01とOKV02に接続します。
9) OKV03を読取り専用ノードとして最初のペアに追加します。
10) OKV04を読取り/書込みピアとして読取り専用ノードOKV03に追加して、次の読取り/書込みペアにします。
11) 読取り専用ノードを追加し、次にその読取り専用ノードを使用して別のノードを追加して最大数が16（読取り/書込みペアと読取り専用ノードの合計）になるまで別の読取り/書込みペアを作成することにより、クラスタを構築し続けます。

サーバーをインストール、接続、構成したら、Oracle KVクライアント・ソフトウェアをアップグレードします。

12) 現在インストールされているOracle KVクライアント12.xのバックアップを作成します（$ORACLE_BASEまたは$ORACLE_HOMEのいずれかの"/okv/$ORACLE_SID"サブディレクトリを含む）。
13) データベースをシャットダウンします。
14) 現在インストールされているOracle KVクライアント12.xをアンインストールします（$ORACLE_BASEまたは$ORACLE_HOMEのいずれかの"/okv/$ORACLE_SID"サブディレクトリを含む）。
15) データベース・ホストに新しいOracle KVクライアント・ソフトウェアをインストールします。
16) データベースを再起動します。
17) Oracle KVで、クライアント・ソフトウェアがアップグレードされたエンドポイントを再起動します。

鍵の可用性とバックアップ

Oracle Key Vault（Oracle KV）の鍵の可用性は持続しますか。

最大で16のOracle Key Vaultインスタンスがグループ化され、潜在的に地理的に分散したデータ・センターを包含する鍵管理クラスタが形成されます。このクラスタ内には、必ず1つ以上の他のOracle KVが存在し、即座に更新されます。

Oracle Key Vaultアプライアンスはどのような方法でバックアップしますか。

Oracle Key Vaultは、手動で、または構成可能なスケジュールに従って自動でバックアップ可能です。バックアップ・プロセスにより、内部バックアップ・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、その暗号化されたバックアップ・ファイルがセキュアな接続を通してリモートの移動先に自動で移動されます。詳細については、Oracle Key Vaultのドキュメントを参照してください。

管理

Oracle Key Vaultはどのようにして管理運用しますか。

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作成を容易に行うことができます。Oracle Key Vaultにはコマンドライン・インタフェースもあり、これによりアップグレードやパッチ適用などの特定の管理業務を実施できます。さらに、RESTfulインタフェースを使用してエンドポイント登録とプロビジョニングを自動化し、オンプレミスやクラウドにおいて大量にデプロイすることもできます。

Oracle Key Vaultでは、どのようにして管理上の職務を分離していますか。

Oracle Key Vaultの管理者ロールは、職務を分離するため、鍵、システム、監査の各管理機能に分割可能です。管理しやすくするため、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とウォレットへのアクセス権を付与することが可能です。

セキュリティ

Oracle Key Vaultでは、保管されている鍵とシークレットをどのようにして保護していますか。

Oracle Key Vaultでは、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保管している鍵とシークレットを保護しています。たとえば、鍵とシークレットを暗号化するOracle Advanced Securityの透過的データ暗号化、Oracle Database Vault、機密データが特権ユーザーに公開されるのを防止するOracle Virtual Private Databaseなどがあります。

Oracle Key Vaultは、保管されている鍵とシークレットへのすべてのアクセスの監査も行います。監査ログは、Oracle Audit Vault and Database Firewallに転送してログを統合することが可能です。

Oracle Key Vaultとエンドポイントの間で鍵の転送を安全に行うため、どのプロトコルを使用していますか。

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、固定ポート5696での相互認証されたセキュアなTLS転送を介し、OASIS KMIP（Key Management Interoperability Protocol）を使用してOracle Key Vaultサーバーと通信します。Oracle Key Vaultのブラウザベース管理コンソールでは、HTTPS（固定ポート443）を使用します。ブラウザベース管理コンソールは、サードパーティの証明書をサポートしています。

Oracle Key VaultでFIPSモードを有効にできますか。

Oracle Key Vault Release 18.1インストールはFIPS 140–2に準拠しています。FIPS 140–2準拠でインストールするオプションを選択すると、必要な変更がインストール中にすべて実行されます。インストール後にFIPS 140-2モードを有効に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とともにデプロイされている場合、信頼の起点（RoT）はHSMに残ります。HSMのRoT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のマスター鍵が保護され、これによって暗号化鍵、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。このように階層が3つの層で構成されていることで、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大幅に軽減されます。なお、このRoT使用例の場合、顧客の暗号化鍵はHSMに格納されません。顧客の鍵の格納と管理はOracle Key Vaultサーバーで直接行われます。

Oracle Key VaultのRoTとして認定されているHSMについての詳細は、『Oracle Key Vault HSMとの統合』ガイド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のソフトウェアはどこからダウンロードできますか。

Oracle Key VaultはOracle Software Delivery Cloudからダウンロードできます。

https://edelivery.oracle.comに移動します。

「Oracle Key Vault」を検索します。「*Continue*」をクリックし、「*Oracle Key Vault, Platform Linux x86-64*」を選択して、2つの.isoイメージをダウンロードします。

推奨されるハードウェア仕様を教えてください。

CPU：最小x86-64 16コア、推奨：暗号化アクセラレーション付きの24～48コア（Intel® AES- NI）

RAM：最小16 GB、推奨：32～64 GB

ディスク：最小2 TB、推奨：4 TB

ハードウェア互換性：Oracle Linux Release 6 Update 9のハードウェア互換性リスト（HCL）を参照してください。HCLは、 http://linux.oracle.com/pls/apex/f?p=117:1で入手できます。

Oracle Key Vaultはどのようにしてインストールしますか。

Oracle Audit Vaultはソフトウェア・アプライアンスとしてパッケージされています。つまり、オペレーティング・システムを含め、まったく何もインストールされていないハードウェアへの製品のインストールに必要なものすべてが含まれています。

インストール中は、Oracle Key Vaultのインストーラがハードウェアを完全に制御します。また、ディスクのパーティション化とフォーマットに加えて、基本OS、ユーザースペース・ライブラリ、Oracle Database、Oracle Key Vaultソフトウェアがインストールされます。すべてのソフトウェア・コンポーネント（OS、ネットワーク、データベースなど）を自動的に、かつ最小限のユーザー操作で構成します。強化用のベスト・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、データベースをハードニングします。不要なパッケージとソフトウェアの削除、および未使用のサービスとポートの無効化も行われます。

Oracle Key VaultをWindowsやSolarisにデプロイできますか。

Oracle Key VaultのクライアントソフトウェアをWindowsやSolarisにデプロイできます。ただし、Oracle Key Vault Serverはベア・メタルにのみインストール可能です。Oracle Key Vaultはソフトウェア・アプライアンスとして提供されているため、WindowsやSolarisなどの既存のOSや他のソフトウェアはOracle Key Vaultのインストール・プロセスによって削除されます。

Oracle Virtual Machine上でOracle Key Vaultを実行できますか。

本番環境ではOracle Key Vaultがアーキテクチャ全体の非常に重要なコンポーネントです。Oracle Key Vaultのリポジトリは暗号化されているため、仮想化されたプラットフォームでこれを実行するとわずかながらも露呈するリスクが生じます。しかしながら、仮想化レイヤー、仮想化レイヤーへのアクセス権を持つユーザー、VMのコピーやクローンの作成ができるユーザーをOracle KVの管理者が制御することはできません。したがって、パフォーマンス、可用性、セキュリティ、およびサポート上の理由から、オラクルはベア・メタル・ハードウェアにOracle Key Vaultをインストールすることをお勧めします。

Oracle Database Appliance（Oracle DA）またはOracle ExadataにOracle Key Vaultをインストールできますか。

現時点において、Oracle Key VaultのインストールはOracle Database ApplianceまたはOracle Exadataで認定されていません。ただし、Oracle Key Vaultを使用して、Oracle DAまたはOracle Exadataによって使用される鍵を管理することは可能です。

対象エンドポイントとの統合

エンドポイント・ソフトウェアはどのようにしてダウンロードおよびデプロイしますか。

それ自体の鍵およびシークレットを管理するように設定されているデータベース・サーバー、ミドルウェア・サーバー、システムはエンドポイントと呼ばれます。Oracle Key Vaultの管理コンソールには、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が表示されます。エンドポイント・ソフトウェア・パッケージには、必要なすべてのバイナリ・ファイルと構成ファイル、およびエンドポイントとOracle Key Vaultの間の相互認証されたセキュア接続を確立するためのTLS証明書が格納されています。Oracle Key Vaultのシステム管理者がエンドポイントを登録すると、Oracle Key Vaultはワンタイム登録トークンを自動生成します。DBAなどのエンドポイント管理者が、この登録トークンを使用してエンドポイント・ソフトウェアをダウンロードします。またOracle Key Vaultでは、管理操作を最小限に抑えたテスト環境での自己登録にも対応しています。

Oracle Wallet内のOracle TDEマスター鍵をOracle Key Vaultに移行できますか。

透過的データ暗号化（TDE）を使用しているOracle Databaseの場合、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マスター鍵を一元的に管理することができます。既存のTDEマスター鍵は、SQLコマンドのALTER SYSTEM MIGRATEまたはADMINISTER KEY MANAGEMENT MIGRATEのいずれかを使用することにより、Oracle WalletからOracle Key Vaultに容易に移行できます。詳細については、Oracle Key Vaultのドキュメントを参照してください。

Oracle Key Vaultはエンドポイントでの暗号化パフォーマンスに影響を与えますか。

Oracle Key Vaultは暗号化パフォーマンスに直接影響しません。

エンドポイントの構成およびプロビジョニングには、どれぐらいの長さの停止時間を予定する必要があります。

Oracle WalletまたはJavaキーストアをを Oracle Key Vaultにアップロードするエンドポイントの場合、停止時間は必要ありません。Oracle DatabaseのエンドポイントでTDEマスター鍵をOracle WalletからOracle Key Vaultに移行する場合、スタンドアロン構成ではウォレットをいったん閉じてから開き直す必要があり、共有サーバー構成ではデータベースの再起動が必要になるため、最小限の停止時間を計画する必要があります。

機能の互換性

Oracle Key Vaultでは、どのバージョンのOracle Databaseとミドルウェアがサポートされていますか。

Oracle Key Vaultでは、Oracle Linux、Red Hat Linux、Solaris Sparc、Solaris x64、AIX、HP-UX、WindowsのOracleミドルウェアとOracleデータベースのすべてのサポート対象リリースからのOracle Walletのアップロードとリストアをサポートしています。TDEとOracle Key Vaultの間の直接接続は、Oracle Linux、Red Hat Linux、Solaris Sparc、Solaris x64、AIX、HP-UX、Windows上のOracle Database 11gR2、12.1、12.2、18、19でサポートされています。

Oracle Key Vaultでサポートされる鍵格納ファイルにはどのような種類がありますか。

Oracle Key Vaultでは、Oracle WalletとJavaキーストア（JKSおよびKCEKS）の鍵格納ファイルがサポートされています。Oracle JDK 1.4、1.5、1.6、7、8を使用しているJavaキーストアがテスト済みです。

Oracle Key Vaultには、どのタイプの資格証明ファイルを保管できますか。

Oracle Key Vaultには、KerberosのキータブやファイルなどのSSH鍵が格納されているすべての資格証明ファイルが保管されます。技術的には、一元管理する資格証明ファイルはどの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、各資格証明ファイルのサイズを128 KB未満に制限する必要があります。

Oracle Key Vaultで機密データを暗号化できますか。

Oracle Key Vaultでは、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の管理のみを行います。データ暗号化の責任はエンドポイントに委ねられます。Oracle Key Vaultは管理対象鍵を暗号化します。

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

Oracle Key Vaultでは現在、DBMS_CRYPTO鍵を管理していません。

その他の情報

Oracle Key Vaultに関する詳細情報の入手先を教えてください。

詳しくは、Oracle Technology Network（OTN）のOracle Key Vaultのページを参照してください。データ・シート、ホワイト・ペーパー、顧客事例、エンドユーザー向け文書、ディスカッション・フォーラムなど、有益な各種情報をオンラインで入手できます。Oracle Universityでは、Oracle Key Vaultのトレーニング・コースを提供しています。

https://www.oracle.com/jp/database/technologies/security/key-vault.html

ORACLE
Key Vault

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

Integrated Cloud Applications & Platform Services

ORACLE