よくある質問

Oracle Key Vaultハイブリッド・クラウド鍵管理

Oracle Key Vaultは、暗号化鍵、Oracleウォレット、Javaキーストア、資格証明ファイルを堅牢な方法で一元管理できるようにすることで、暗号化およびその他のセキュリティ・ソリューションの容易な導入を可能にします。

現在、Oracle Key Vaultはオンプレミス・エンドポイントとクラウド・エンドポイントの両方で鍵管理をサポートしています。このドキュメントでは、Oracle Key Vaultハイブリッド・クラウド鍵管理に関する、よくある質問を取り上げます。

ハイブリッド・クラウド鍵管理

Q：ハイブリッド・クラウド鍵管理とは何ですか。

A：ハイブリッド・クラウド鍵管理は、暗号化鍵をオンプレミスのOracle Key Vaultから管理しながら、データをクラウド内で暗号化する、クラウド暗号化ソリューションのデプロイメント・トポロジです。

オンプレミスのOracle Key Vaultが、オンプレミスのOracleデータベースのTDEマスター暗号化鍵に加えて、Oracle Database Cloud Service（Oracle DBCS）のOracle Advanced Security TDEマスター暗号化鍵も管理します。ハイブリッド・クラウド鍵管理では、オンプレミスのOracleデータベースで使用するマスター暗号化鍵だけでなく、Oracle Cloudで使用するマスター暗号化鍵も制御および可視化できます。

Q：ハイブリッド・クラウド鍵管理の利点は何ですか。

A：オンプレミスの一元化された鍵管理インフラストラクチャをオンプレミスとクラウドの両方のデータベース・エンドポイントに利用すると、エンドポイントの場所に関係なく鍵を制御および可視化し続けられる上、一貫性のある鍵管理ポリシー、オンプレミスとクラウド間でのリソース共有、TCOの削減など、数多くの利点が得られます。

Q：ハイブリッド鍵管理はマスター鍵にのみ適用されますか。それとも、Oracle Key Vaultに格納されるウォレットやその他の資格証明ファイルにも適用されますか。

A：ハイブリッド・クラウド鍵管理でサポートされているのは、Oracle DBCSインスタンスのオンラインTDEマスター鍵管理のみです。Oracle Cloud内のリソースのウォレットや資格証明ファイルの管理には、ハイブリッド・クラウド鍵管理は適用されません。

Q：どのような場合に、Oracle DBCSインスタンスのTDEマスター鍵を一時停止する必要がありますか。

A：OSレベルで不正侵入が発生したと考えられる場合など、極めて重大な状況でのみ、TDEマスター鍵へのアクセスを一時停止する必要があります。鍵へのアクセスを一時停止すると、機密データへのすべてのアクセスを停止すると同時に、侵入を調査して証拠を収集するための時間を確保できます。TDEマスター鍵を一時停止すると、Oracleデータベースでデータベース内の暗号化データに一切アクセスできなくなり、データにアクセスしようとすると、ORA- 28353：“failed to open wallet（ウォレットを開くことができませんでした）”エラーが発生します。

Q：Oracle DBCSインスタンスのTDEマスター鍵を一時停止する方法を教えてください。

A：アクセスを一時停止するには、Oracle Key Vaultシステム管理者がKey Vault管理コンソールで、該当するOracle DBCSインスタンスに対応する「Suspend」ボタンをクリックします。エンドポイントに対する「Suspend」ボタンをクリックすると、暗号化鍵へのアクセスが一時的に停止されて、クラウド内のアプリケーションと管理者の両方が暗号化データにアクセスできなくなります。十分な調査を行ったら、「Resume」

ボタンをクリックすると、鍵へのアクセスが再開されます。エンドポイントに対する「Suspend」ボタンをクリックして暗号化鍵へのアクセスを一時停止するこの方法は、オンプレミスのOracle Databaseエンドポイントにも適用できます。

Q：オンプレミスのOracle Key Vaultで、Oracle以外のクラウド環境内に配備されているOracle DatabaseのTDEマスター鍵を管理できますか。

A：Oracle Key Vaultサーバーと Oracle Databases（11gR2以降）の間にネットワーク接続が存在する場合は、任意のクラウド環境内に配備されているOracle DatabaseのTDEマスター鍵をOracle Key Vaultによって管理できます。

ハイブリッド・クラウド鍵管理のデプロイ

Q：オンプレミスのOracle Key VaultでOracle DBCSを使用する、ハイブリッド・クラウド・デプロイメントをセットアップする方法について、おおまかに教えてください。

A：Oracle Key Vaultがオンプレミスにインストール済みの場合、Oracle Key Vault 12.2 BP1以降にアップグレードします。それ以外の場合は、オンプレミスでOracle Key Vault 12.2.0.1以降をインストールして構成します。Oracle Key Vaultの管理UIを使用し、Oracle DBCSインスタンス（TDEを使用）とプライマリOracle Key Vaultサーバーの間にSSHトンネルを設定します。Oracle Key Vaultのドキュメントに記載されている通常の手順に従って、Oracle DBCSデータベース・インスタンスをOracle Key Vaultエンドポイントとして登録およびプロビジョニングします。

Q：ハイブリッド・クラウド・デプロイメントをサポートしているOracle Key Vaultのバージョンを教えてください。

A：ハイブリッド・クラウド鍵管理は、Oracle Key Vault 12.2.0.1.0（12.2 BP1）以降でサポートされています。

Q：Oracle Key Vaultハイブリッド・クラウド鍵管理はどのOracle Database Cloud Servicesをサポートしていますか。

A：Oracle Key Vaultハイブリッド・クラウド鍵管理はOracle Database as a Service（DBaaS）をサポートしています。

Q：オンプレミスのプライマリOracle Key Vaultサーバーがスタンバイ Oracle Key Vaultサーバーにフェイルオーバーした場合、どうなりますか。

A：プライマリOracle Key Vaultサーバーがスタンバイ・サーバーにフェイルオーバーした場合、スタンバイ・サーバーがアクティブなすべてのデータベース・クラウド・サービス・エンドポイントへのSSHトンネルを自動的に確立します。

Q：可用性に関して、考慮しておくべきことはありますか。Oracle Key Vaultが使用不可の場合にデータベースがハングしたり、インターネット・アクセスの問題のためにデータベースのパフォーマンスが低下したりしませんか。

A：構成された時間間隔で、Oracle Databaseエンドポイントがメモリ内に鍵をキャッシュします。短時間のネットワーク停止にデータベースが対処できるように、デフォルトではこの時間間隔は5分間になります。ビジネス・ニーズやセキュリティ・ニーズに合わせて、このキャッシュの値を変更できます。

Q：Oracle Key VaultをオンプレミスのHSMと統合できますか。

A：Key Vaultに格納されている暗号化データを保護する鍵階層の"信頼の起点"として、オンプレミスのHSMをオンプレミスのKey Vaultと統合できます。この"信頼の起点"はHSM内で生成され、HMS外に流出することはありません。オンプレミスのHSMとの統合は、Key Vault 12.2.0.1以降の新規インストールでのみサポートされています。

詳しくは、『Oracle Key Vault Hardware Security Module (HSM)との統合』を参照してください。

ネットワークとSSHトンネルのデプロイ

Q：ネットワーク・ファイアウォールに穴を開ける必要はありますか。

A：通常、ネットワーク・ファイアウォールの変更は不要です。ただし、ファイアウォールでアウトバウンドSSH接続を許可していない場合、アウトバウンドSSHポート（22）のブロックを解除する必要があります。Oracle Key VaultとOracle DBCSインスタンスの間のSSH設定について、詳しくはOracle Key Vaultのドキュメントを参照してください。

Q：ハイブリッド・モデルでは、一時的なネットワーク異常はどのように処理されますか。

A：短時間のネットワーク異常のために暗号化データへのアクセスが中断されないように、クラウド・データベースPKCS#11ライブラリがTDEマスター鍵を短期間キャッシュします。ネットワーク停止でSSHトンネルが中断された場合は、Oracle Key Vaultが自動的にSSHトンネルを再確立します。

Q：Oracle DBCSデータベース・インスタンスとオンプレミスのOracle Key Vaultサーバーの間のトラフィックはどのように暗号化されますか。

A：オンプレミスのOracle Key VaultとOracle DBCSインスタンスの間の通信では、暗号化されたSSHトンネルを使用します。また、すべてのOracle Key Vaultエンドポイントが、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転送を介してOASIS KMIP（Key Management Interoperability Protocol）を使用します。

Q：オンプレミスのOracle Key VaultとOracle DBCSインスタンスの間にSSHトンネルを設定する方法を教えてください。

A：Oracle Key Vaultハイブリッド・クラウド鍵管理用のSSHトンネルの設定では、標準の鍵ベース認証を使用します。

まず、SSH鍵設定用のOracle DBCS管理UIインタフェースを使用し、プライマリOracle Key Vaultサーバー管理コンソールからOracle DBCSインスタンスに公開鍵をコピーします。次に、Oracle Key Vaultのシステム管理者として管理コンソールにログオンし、Oracle DBCSインスタンスのパブリックIPアドレスおよびポート番号を指定してSSHトンネルを作成します。詳しくは、Oracle Key Vaultのドキュメントを参照してください。

Q：Oracle Cloud内の各Oracleデータベース・インスタンスにSSHトンネルを設定する必要はありますか。

A：Oracle Key Vaultでは2つのシナリオをサポートしています。各Oracle DBCSインスタンスとプライマリOracle Key Vaultサーバーの間に個別のSSHトンネルを設定することが可能です。または、Oracle DBCSインスタンス（またはクラウド内のその他のホスト）を、すべてのSSHトラフィックをOracle DBCSインスタンスにルーティングするOracle Key Vaultゲートウェイとして指定することが可能です。

Oracle Key Vaultゲートウェイを使用するかどうかの選択は、見込まれるクラウド・エンドポイントの数、ゲートウェイへの依存度、およびクラウド・エンドポイント間で必要となるネットワーク分離に基づきます。いずれを選択する場合でも、KMIP通信はTLS 1.2によってエンド・ツー・エンドで保護されるため、通信が中継デバイスに表示されたり中継デバイスによって改ざんされたりすることはありません。

Q：Oracle Key Vaultからクラウド内のエンドポイントにネットワーク接続するには、SSHトンネルが必要ですか。

A：いいえ、Oracle Key Vaultからクラウド内のエンドポイントに直接接続できない場合にのみ、SSHトンネルが必要です。

製品ライセンスとサポート

Q：Key Vaultハイブリッド・クラウド鍵管理は、個別にライセンス供与される機能ですか。

A：いいえ、Oracle Key Vaultハイブリッド・クラウド鍵管理には、個別のライセンスは必要ありません。Oracle Key Vaultのライセンスで、オンプレミス・エンドポイントとOracle DBCSエンドポイントの鍵を管理できます。

Q：Oracle Key Vaultハイブリッド・クラウド鍵管理で問題があった場合の問い合わせ先を教えてください。

A：My Oracle Support（https://support.oracle.com）までお問い合わせください。

OTNのOracle Key Vaultページを参照してください。

Q：Oracle Key Vaultに関する全般的な情報はどこで入手できますか。

A：データシート、FAQ、製品ドキュメントのリンクなど、製品の補足資料については、OTNのOracle Key Vaultページを参照してください。

詳細情報

Q：Oracle Key Vaultハイブリッド・クラウド鍵管理のデプロイに関する詳細な情報はどこで入手できますか。

A：Key Vaultオンライン・ドキュメント・サイトの『Oracle Key Vault管理者ガイド』（12.2）を参照してください。また、詳しくはKey Vault OTNページを参照してください。

Q：Oracle Key Vaultに関する全般的な情報はどこで入手できますか。

A：データシート、FAQ、製品ドキュメントのリンクなど、製品の補足資料については、OTNのOracle Key Vaultページを参照してください。

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

海外からのお問い合わせ窓口
電話：+1.650.506.7000
ファクシミリ：+1.650.506.7200

CONNECT WITH US

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

Integrated Cloud Applications & Platform Services