日日是Oracle APEX

Oracle APEXを使った作業をしていて、気の付いたところを忘れないようにメモをとります。

2021年8月16日月曜日

データベース・セキュリティの活用(0) - はじめに

Oracle APEXのアプリケーションを開発するにあたって、Oracle Databaseが提供するセキュリティを強化する機能を活用することができます。それらの機能をAlways FreeのAutonomous Database上に実装することにより、機能の概要と活用方法について理解します。

作業および機能ごとに、それぞれ以下のように記事にしています。

0. はじめに - こちらの記事
1. ワークスペースの準備

   アプリケーションを開発するためのワークスペースAPEXDEVと表EMP/DEPTを保持するワークスペース(=データベース・スキーマ)HRを作成します。

2. 権限の追加

   ユーザーAPEXDEVからスキーマHRの表EMPおよびDEPTにアクセスする権限を与えます。標準のGRANT文を実行します。

3. アプリケーションの作成

   テストに使用するため、意図的にSQLインジェクションへの脆弱性を持つアプリケーションを作成します。

4. 統合監査(Unified Audit)

   統合監査ポリシーを定義し、表EMPへのアクセスの監査証跡を取得します。

5. ファイングレイン監査(Fine Grained Audit)

   監査証跡を取得する際に、詳細な条件を与えます。

6. 権限分析(Privilege Analysis)

   アプリケーションの実行時に使用されているデータベースの権限と、使用されていない権限を分析したレポートを生成します。

7. 仮想プライベート・データベース(Virtual Private Database)

   仮想プライベート・データベースを構成し、SQLインジェクションを防ぎます。

8. Real Application Security

   Real Application Securityを構成し、SQLインジェクションを防ぎます。

9. Data Redaction

    Data Redactionを構成し、機密データを伏字に変えて表示します。

10. 透過型機密データ保護(Transparent Sensitive Data Protection)

    透過型機密データ保持を構成し、機密データを保護します。

11. Database Vault

    管理者権限を持つユーザーによる、ユーザー・データのへのアクセスを禁止します。

記事の1から3までは準備作業になります。それ以降はできるだけ独立して参照できるように記述しています。例外として、仮想プライベート・データベースとReal Application Securityでの認証スキームは前出の構成を引き継いでいます。

記事の順番に従って作業を行い、内容が正しく実施できることを確認しています。

それぞれの機能についての説明は限られています。無料で利用可能な環境を使って、実際に手を動かして動作を確認することを目的としています。

続く

Yuji N. 時刻: 17:47

共有

自己紹介

Yuji N.

日本オラクル株式会社に勤務していて、Oracle APEXのGroundbreaker Advocateを拝命しました。
こちらの記事につきましては、免責事項の参照をお願いいたします。

詳細プロフィールを表示