ORACLE

Oracle Audit Vault and Database Firewall

エンタープライズ向けのデータベース・アクティビティ監視とセキュリティ体制管理

2025年5月、バージョン20.14

ORACLE

本書の目的

このテクニカル・ペーパーでは、Oracle Audit Vault and Database Firewall（AVDF）の概要について説明します。機能、オプション、ユースケースについても説明します。本書は、セキュリティ・リスクを低減し、データベース（Oracle Database、Oracle MySQL、Microsoft SQL Server、PostgreSQL、IBM Db2、SAP Sybaseを含む）の規制遵守を向上するための選択肢を評価できるよう支援することを目的としています。これは、その他大半のエンタープライズ・データベース・プラットフォームのサポートにも及んでいます。

免責事項

本文書には、ソフトウェアや印刷物など、いかなる形式のものも含め、オラクルの独占的な所有物である占有情報が含まれます。この専有資料へのアクセスおよび使用には、すでに締結され、ユーザーによるその遵守が確約されている、オラクルとユーザーとのソフトウェア・ライセンスおよびサービス契約の諸条件が適用されます。本書は、ユーザーとのライセンス同意書の一部をなすものではなく、またオラクルやその子会社および関連会社とのいかなる契約上の合意事項にも含まれるものではありません。

本書は情報提供のみを目的としたものであり、ここで説明する製品の機能を実装およびアップグレードする際の資料として使用されることのみを意図しています。マテリアルやコード、機能の提供をコミットメント（確約）するものではなく、購買を決定する際の判断材料になさらないでください。本文書に記載されている機能の開発、リリース、時期および価格については、弊社の裁量により決定されます。製品アーキテクチャの性質上、本書に記述されているすべての機能を安全に組み込むことができず、コードの不安定化という深刻なリスクを伴う場合があります。

ORACLE

目次

ORACLE

図のリスト

表のリスト

ORACLE

はじめに

Oracle Databaseには、世界中のリレーショナル・データの半分以上が含まれています。このデータの大半は機密性が高く、金銭的価値があります。それが、データベース、特にOracle Databaseがデータ窃盗の魅力的な標的となる理由です。

データベース・アクティビティ監視（DAM）は、ネイティブ・データベース監査とネットワークベースのデータ取得から情報を収集し、分析とレポートのためにデータベース・アクティビティを監視して記録するデータベース・セキュリティ・テクノロジーです。データベース・アクティビティ監視は、リレーショナル・データベースのデータを保護する上で極めて重要です。これにより、予防的制御が失敗したときに、悪意のある可能性があるアクティビティを可視化します。

データベース・アクティビティを正確に把握する最善の方法は、監査データをネットワークベースのアクティビティ監視およびブロッキングと組み合わせる方法です。ネットワーク監視のみでは、疑わしい動作をすべて捕捉することはできません。ネットワーク監視のみに焦点を当てたソリューションでは、データベースのシノニム、機能ベースのビュー、またはストアド・プロシージャ・アクティビティを理解することはできません。逆に、データベース内のすべての動作を監査するのは非現実的であるため、監査のみに焦点を当てたソリューションでは、異常を特定し、疑わしいアクティビティの特定をサポートするために必要なすべてのデータベース・アクティビティの全体像を把握することはできません。監査とネットワークベースの監視を組み合わせることで、これらの問題が解決され、セキュリティと規制遵守の両方の目的がサポートされます。

Oracle Audit Vault and Database Firewall（AVDF）には、その製品名が示すように、データベース・ファイアウォールが含まれます。データベース・ファイアウォールは、受信するSQLコマンドをネットワーク・レベルで監視して評価し、異常やポリシーに違反している動作を特定してアラートを生成します。必要に応じて、データベース・ファイアウォールを使用して、ポリシーに違反しているSQLがデータベースに到達するのを一切ブロックできます。

アクティビティ監視は極めて重要ですが、組織は、データベースのセキュリティ体制についても懸念しています。データベースの構成時にベスト・プラクティスに従ったでしょうか。データベースはセキュリティ標準に準拠しているでしょうか。Oracle Databaseをさらに強化するために他に何について検討すべきでしょうか。これらの質問の回答の役に立つのは、データベース・セキュリティ体制管理（DSPM）です。DSPMでは、データベース構成とセキュリティ設定を機密データの検出と組み合わせることで、データベースのリスクとセキュリティ体制が統合された全体像を示します。

AVDFは当初、2012年に導入されました。AVDFは、既存の2つの製品（Oracle Audit VaultとOracle Database Firewall）を単一の統合製品に結合した製品です。AVDFは、ネイティブ・データベース監査とネットワークベースのアクティビティ監視間の相乗効果を活用し、データベース・アクティビティの包括的なビューを提供した初の製品です。AVDF 20.9は、この製品の機能をデータベース・アクティビティ監視（DAM）からデータベース・セキュリティ体制管理（DSPM）に拡張しています。

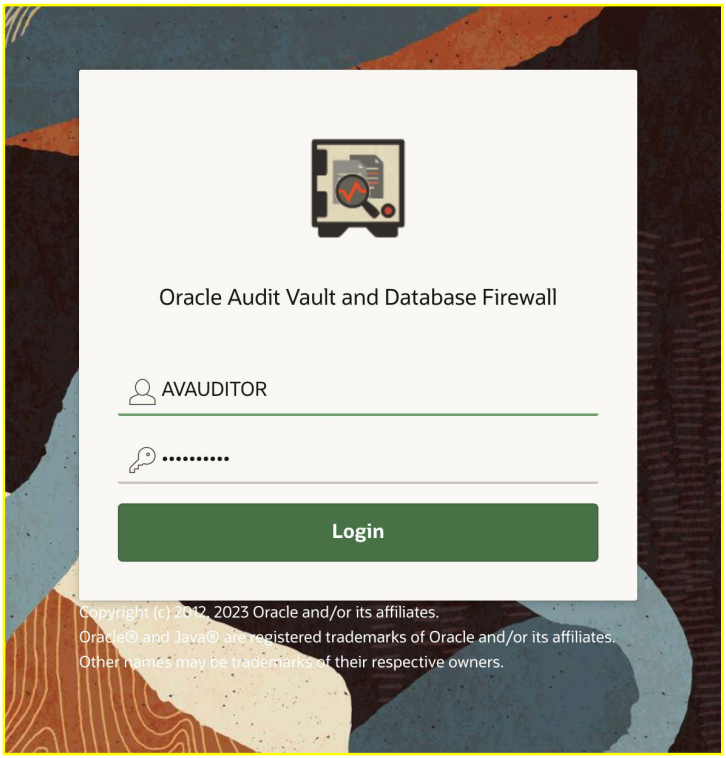


図1：Oracle Audit Vault and Database Firewallのログイン・ページ

Oracle Audit Vault and Database Firewallの概要

Oracle Audit Vault and Database Firewall（Oracle AVDF）は、Oracle Databaseのセキュリティ体制を管理するためにデータベース・アクティビティ監視を超えて機能が拡張されています。AVDFのクラス最高のアクティビティ監視機能は、セキュリティ構成、ユーザー・エンタイトルメント、ストアド・プロシージャ、データベース内のデータの量とタイプの可視化によって強化されています。

AVDFは、クラウドとオンプレミスのどちらにあるかとは関係なく、Oracleデータベースと Oracle以外のデータベース、オペレーティング・システム（OS）、ディレクトリからのユーザー監査データを分析、アラート、レポート用の単一のリポジトリに集約します。AVDFは、スケーラビリティ、セキュリティ、自動化を備えたエンタープライズレベルの監査プラットフォームです。また、AVDFは、ネットワーク経由でデータベースに送信されたSQL文を監視し、不正なSQL文を調査、許可、ログ記録、さらにはブロックすることもできます。データベース・ファイアウォールは、異常を特定し、不正なSQLまたはSQLインジェクション攻撃をブロックするための簡単なルールを使用してネットワークベースのSQL検査を実現します。

強力なレポートとアラートを介して、AVDFは、コンプライアンス監査とインシデント調査をサポートし、全方位を対象とした最新のスケーラブルなプラットフォームを提供します。AVDFには、関連情報に迅速にアクセスすることを可能にする簡単なフィルタベースの対話型レポート・インタフェースを使用した広範なレポート機能が用意されています。AVDFを使用すると、単一のシステムで、数千のデータベース全体のアクティビティを監視し、アプリケーション、オペレーティング・システム、Active Directoryなどのサポート・インフラストラクチャを含むデータベース資産全体にわたるセキュリティ・イベントをレポートおよび分析するための単一のコンソールを実現できます。

AVDFは、一般的なエンタープライズクラスのデータベース向けのデータベース・アクティビティ監視をサポートしています。追加設定が不要な監査収集サポートには、Oracle Database、Oracle MySQL、Microsoft SQL Server、SAP Sybase、IBM Db2 LUW、PostgreSQLが含まれます。その他大半のデータベースとアプリケーションのサポートは、JDBCまたはRESTful APIを介してデータを収集する付属のカスタム・コネクタ・フレームワークを使用して実現されます。また、カスタム収集キットは、監査データをXMLまたはJSONファイルに書き込むシステムもサポートしています。QuickCSVコレクタを使用して、MariaDB、EnterpriseDB（Postgres）、およびCSVで監査データを作成するその他のシステムから監査データを収集することもできます。カスタム・コネクタ・フレームワークのオプションを使用してはアクセスできない珍しいターゲットを収容するために、Javaベースのソフトウェア開発キット（SDK）が用意されています。

データベース・セキュリティ体制管理は現在、Oracle Databaseに対してのみ提供されています。AVDFのフリートレベルのビューは、Oracle Database構成のインサイトを促進し、データベース資産全体にわたる問題の検出を可能にします。管理者は、この情報を使用して問題を迅速に軽減して、リスクを削減し、データ漏洩を制御できます。

Audit Vault and Database Firewallのおもな機能

AVDFは、10年以上の継続的な開発の成果です。AVDFには、簡素化されたユーザー・インタフェース、普及しているすべてのデータベースを対象とした広範なカバレッジ、スケーラブルかつ堅牢な基礎となるインフラストラクチャ、変更前と変更後の値を収集するためのスケーラブルな実証済みのアーキテクチャなどが用意されています。

ユーザー・インタフェース

AVDFのユーザー・インタフェース・エンジンは、応答性の高い最新の直観的なルック・アンド・フィールを備えています。このUIは、一般的なワークフローと簡単なナビゲーションのために簡素化および最適化されています。Audit Vault Serverとデータベース・ファイアウォールは、同じコンソールで管理されます。このコンソールは、管理アクティビティを一元化し、監視が必要なコンソールの数を削減します。

大半のデータベース・タイプのカバレッジ

AVDFは、Oracle Database、Oracle MySQL、Microsoft SQL Server、SAP Sybase、IBM Db2 LUWを対象として監査収集とネットワーク収集をサポートしています。また、監査収集は、PostgreSQLデータベースとMongoDBデータベースでもサポートされています。カスタム・コレクタ・フレームワークを使用すると、XML、JSON、またはCSV形式で監査データを生成するデータベースまたはアプリケーションに監査収集を追加したり、JDBCを介してアクセスできるデータベース表に監査証跡を書き込んだりできます。

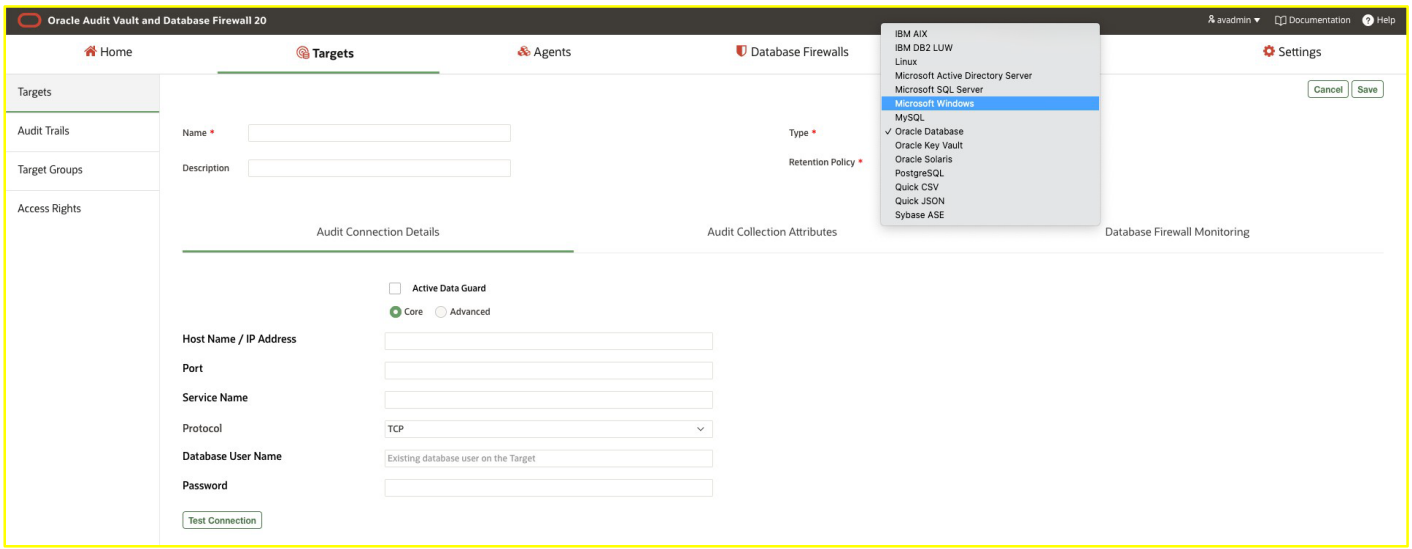


図2：新しいターゲットの登録

データベース・セキュリティ体制管理

データベース・セキュリティ体制管理（DSPM）は、Oracle Database向けのセキュリティ構成評価と、セキュリティの評価結果や関連するリスクを含む、フリート全体の簡単かつ一元的なビューを提供します。要約されたリスク評価結果は、Oracle Databaseフリートに関連する潜在的なリスクに対する即時措置の優先順位付けとガイドの役に立ちます。

高リスクと中リスクについて理解することから始めて、アドバイザリを確認し、カテゴリを評価することで、セキュリティ体制をさらに強化できます。AVDFが提供する強力な対話型レポートを備えた評価レポート・ページで、興味のあるリスクについてより詳しく調べて、さらなる分析を続けること

ができます。DSPMを使用すると、セキュリティのベースラインを定義し、ベースラインのセキュリティ体制からの逸脱を監視できます。セキュリティ評価のずれレポートは、新しく導入されたセキュリティ構成の変更のみに焦点を当てる上で役に立ちます。AVDF 20.13のセキュリティ評価機能には、組織の要件に応じてセキュリティ・チェックのデフォルトの重大度レベルを変更したりセキュリティ・チェックを延期したりし、その結果をスケジュールされているその後の評価のベースラインとして設定できる柔軟性があります。

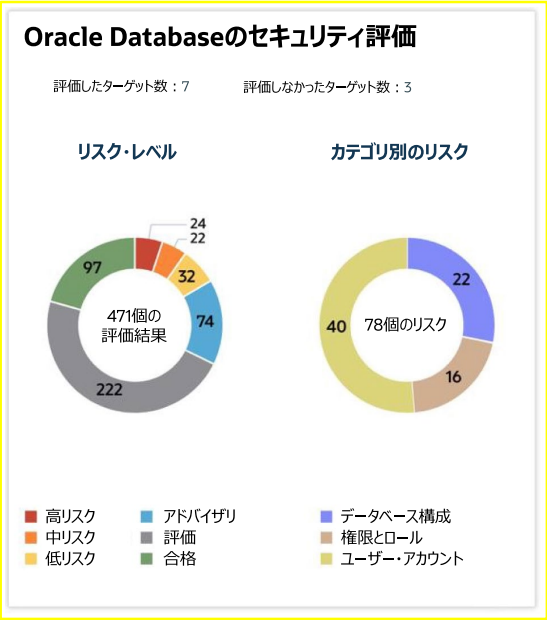


図3：Oracle Databaseのセキュリティ評価

監視対象外のデータベースの検出

セキュリティ監視内のギャップを回避するには、ネットワーク上のすべてのデータベースを可視化することが極めて重要です。AVDF 20.12の新しいデータベース検出機能を使用すると、Nmapスキャンを実行し、スキャン結果をAVDFにアップロードすることで、以下のユースケースを達成できます。

1. AVDFを使用して監視したいデータベースを迅速に特定して登録できます。
2. また、AVDFが現在は監視していない新しいデータベースを特定し、Nmapファイルを定期的にスキャンしてAVDFにアップロードすることで、これらを登録することもできます。

この機能を使用すると、いずれのデータベースも監視対象外にならないよう徹底できます。

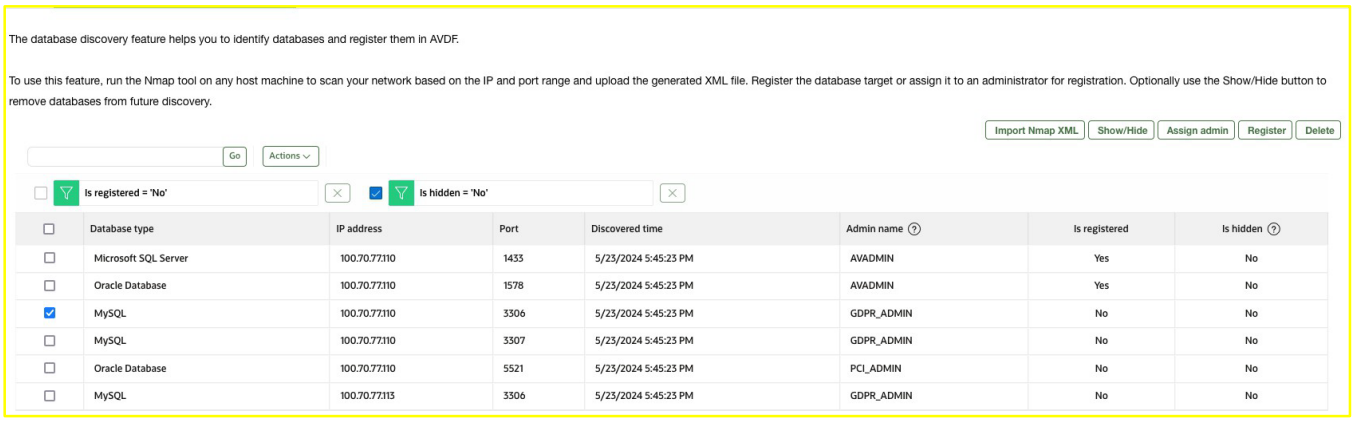


図4：未登録ターゲットのデータベースの検出

変更前と変更後の値の収集

変更前と変更後の値の収集は、まさにその言葉どおりの作業です。データ値が変更されると、AVDFは、古い値（変更前）と新しい値（変更後）とともに、誰が変更したか、いつ変更が行われたかに関する情報を記録します。変更前と変更後の値の収集は、医療と金融サービスやその他多くの規制業種で幅広く使用されています。変更前と変更後の値の収集を使用すると、監査者は、多くのデータ・ガバナンス指令の構成要素である変更全体にわたる個々のデータ属性のライフサイクルを追跡できます。

AVDFは、変更前と変更後の値の収集にOracle GoldenGateを使用します。（GoldenGateの制限付き使用はAVDFに付属しています。詳細については、『AVDFライセンス情報ガイド』を参照してください。） GoldenGateを使用すると、スループットの改善、管理の簡易化、マルチテナント・データベースのサポート、OracleデータベースとOracle以外のデータベースのサポートなどの多くのメリットがもたらされます。AVDFの最近の更新により、変更前と変更後の値をMicrosoft SQL ServerとMySQLに取り込む機能が拡張されています。この新しい機能により、組織は、コンプライアンス・レポートを改善しやすくなり、データのライフサイクル全体を通じて重要なデータ要素を監視できるようになります。

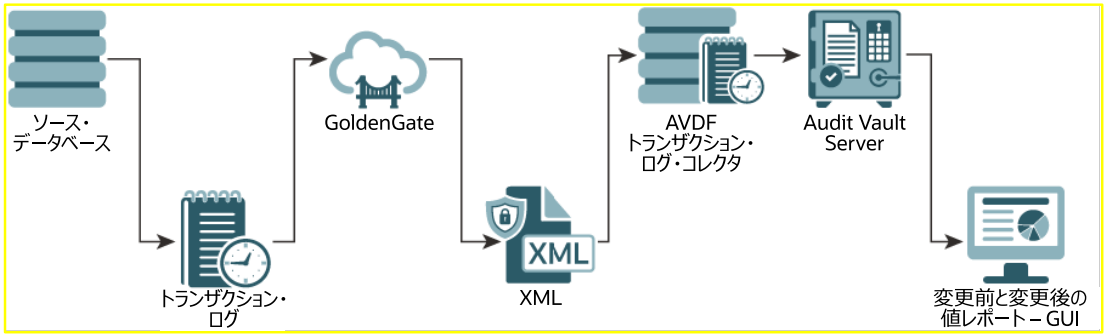


図5：トランザクション監査証跡データ・フロー

操作エクスペリエンスの改善

AVDFは、SAML 2.0を使用してAVDFユーザーとMicrosoft Active Directory/OpenLDAPおよびIDプロバイダ（IDP）（Microsoft Entra ID、Active Directory Federation Services（ADFS）、Oracle Access Manager（OAM）など）との統合を介して一元的なユーザー認証をサポートしています。また、AVDFは、収集データの自動アーカイブ、マルチパス・ファイバ・チャネル、ネットワーク・インタフェース・カード・ボンディング、AVDFポート・カスタマイズもサポートしています。AVDFの管理者とシステム・インテグレータは、AVDFは操作が簡単であり、最新のデータセンターやクラウド・デプロイメントに適していることに気付くでしょう。

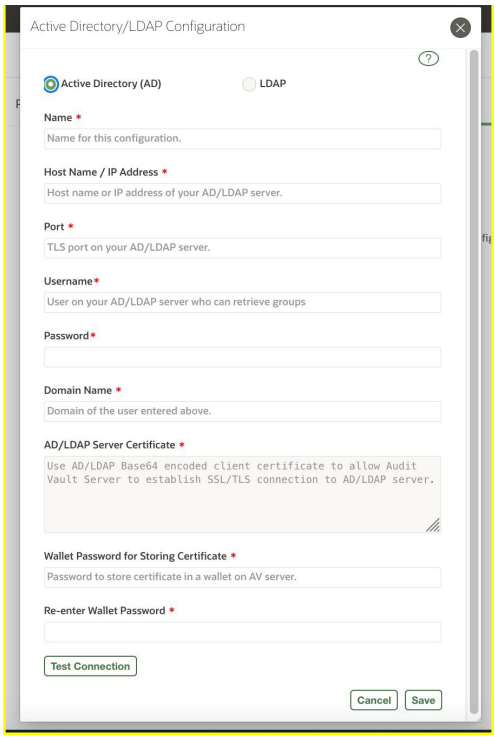


図6：Active Directory統合

レポートとアラート

レポートとアラートは、AVDFなどのDAMシステムのプライマリ出力です。このシステムは、レポートの形式で収集された情報を提示し、必要に応じてアラートを生成します。

アラートにより、即座に注意を向ける必要がある状態が検出されたときに関係者に通知されます。一般的なアラートには、短時間に複数回失敗したログインの試みや、機密データに対する不正なアクセスの試みなどがあります。AVDFでは、個々のイベント（非常に機密性の高いデータに誰かがアクセスを試みたなど）またはイベント傾向（1分間に1つのIPアドレスから10回以上のログインの試みが失敗したなど）に基づいてアラートをトリガーできます。

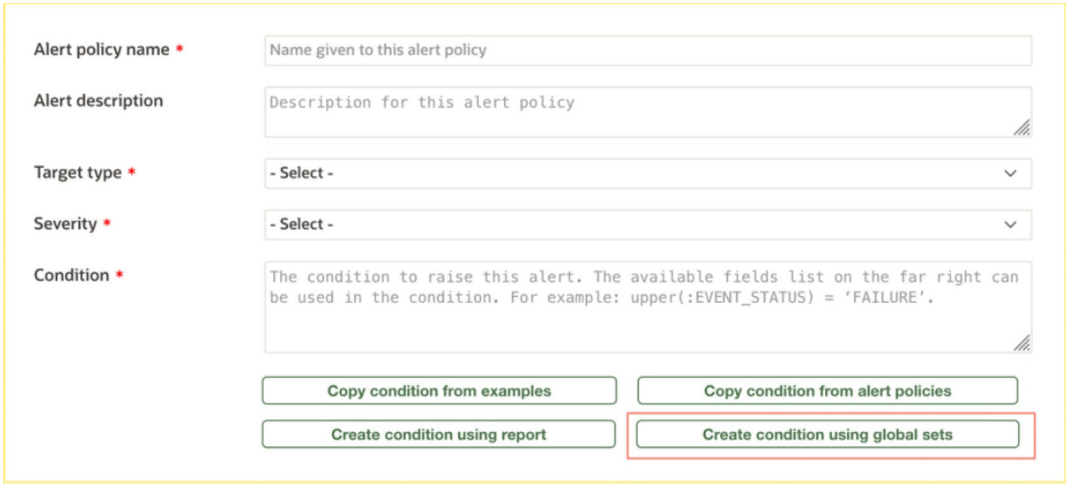


図7：アラート・ポリシーの作成

レポートは、記録または規制目的の正式なレポートにすることも、調査をサポートする非定型のインタラクティブ・レポートにすることもできます。監査者がAVDFコンソールを介してレポートにアクセスすることも、レポートをスプレッドシートまたはドキュメント形式で自動的に生成されるようスケジュールし、電子メールを介して配信することもできます。必要な場合、レポートがレビューされたことの証明とともに、レビューアからのメモをAVDF内で追跡することもできます。

AVDFには、HIPAA、PCI、GDPRなどの規制をサポートするコンプライアンス・レポートから、ログイン失敗のレポート、SUDOアクティビティ・レポート、DMLなどの標準のセキュリティ要件まで、実行する準備が整った数十のレポートが事前に構成されています。カスタム・レポートを簡単に作成し、後で使用するために保持できます。

監査インサイト・ダッシュボードには、包括的なビューが表示され、1つ以上のデータベース全体にわたる上位のユーザー・アクティビティに関するインサイトが即時提供されます。

図8：監査インサイト・ダッシュボード

広範なレポート機能に加えて、AVDFでは、Oracle Databaseと互換性のある外部レポート・ツールまたは分析ツールを使用できます。また、AVDFにはOracle Business Intelligence Publisherの限定使用ライセンスが付属しています。

Audit Vault and Database Firewallのコンポーネント

AVDFは、データベース・システムを監視して保護する包括的で柔軟なソリューションを提供します。AVDFは、以下のプライマリ・コンポーネントで構成されています。

- Audit Vault Server
- Audit Vault Agent
- データベース・ファイアウォール
- ホスト・モニター

Oracle Audit Vault Server

Audit Vault Serverは、AVDFの必須コンポーネントです。すべてのAVDFインストールに、少なくとも1つのAudit Vault Serverがあります。このサーバーには、以下のコンポーネントがあります。

- 強化されたOracle Linux OS
- Oracle Database（監査リポジトリとして機能します）
- AVDFアプリケーション（AVDFコンソール用のインタフェースとAVCLIコマンドライン・インタフェースを提供します）

AVDFは、監査ターゲットからのデータを統合します。これには、Oracleデータベースと Oracle以外のデータベース、OS、ディレクトリ、ファイル・システム、アプリケーション固有の監査データが含まれます。データは監査ターゲットから収集され、監査リポジトリにロードされます。監査リポジトリは、Audit Vault Server上に存在するOracle Databaseです。

監査リポジトリ・データベースは、（Oracle Transparent Data Encryptionを使用して）暗号化されており、Oracle Database Vaultを使用して保護されます。

Audit Vault Agent

Audit Vault Agentは、監査ターゲットから監査データを取得し、このデータをAudit Vault Serverにセキュアに転送します。1つのAudit Vault Agentが複数のターゲットと監査証跡からデータを収集できます。Audit Vault Agentは軽量で、CPU、メモリー、またはディスク領域で使用する量はわずかです。Audit Vault AgentとAudit Vault Serverとの通信には、TLS 1.2が使用されます。

AVDF 20.9には、Oracle Database内の統合監査データの“エージェントレス”収集が導入されました。エージェントレス収集を使用する場合、ターゲット・ホスト・マシンにAudit Vault Agentをデプロイする代わりに、Audit Vault Serverに付属のエージェントレス収集サービスを使用します。エージェントレス収集サービスは、Audit Vault Serverをインストールする場合、またはAVDFをリリース20.9以降に更新する場合に自動的にインストールされます。Oracle Databaseに加えて、AVDF 20.10には、ターゲット・マシンにエージェントをインストールせずに、エージェントレス・モードのMicrosoft SQL Serverまたはリモート・ホストから監査データを収集する機能が導入されました。AVDF 20.13以降、エージェントレス収集は高可用性モードのAudit Vault Serverに対してサポートされます。

Oracle Database Firewall

データベース・ファイアウォールは、データベースに送信されたネットワーク・アクティビティを監視し、SQL文がデータベースに到達する前にSQL文を調査します。データベース・ファイアウォール・ポリシーは、これらのSQL文を使用して実行されることを管理します。データベース・ファイアウォールは、追加のアクションなしでSQL文をデータベースに渡す場合や、SQL文に関する情報を監査リポジトリに入力するためにAudit Vault Serverに転送する場合があります。データベース・ファイアウォールがそのトラフィックと一致して（データベース・プロキシ・サーバーとして機能して）構成されている場合、このファイアウォールは、SQL文がターゲット・データベースに到達するのをブロックしたり、ブロックされている文の代替SQLコマンドを置き換えたりすることもできます。

データベース・ファイアウォールは、複数ステージのポリシーを使用して、SQL文を使用して何を行うかを決定します。

- 最初のステージでは、このポリシーにより、元の接続のIPアドレス、OSユーザー名、データベースに接続するために使用されているプログラム、接続に使用されているデータベース・アカウントを確認します。ファイアウォールは、これらの要因に基づいて条件を満たす接続を許可したり、後で調査するためにこれらをログに記録したり、（一致している場合は）これらをブロックしたりできるように構成できます。
- 次のステージは、SQL文の構造、およびSQL文の構文に基づく渡すアクション、ログ・アクション、ブロック・アクションに基づいています。このタイプのポリシーは、SQLインジェクション攻撃をブロックまたは警告するのに優れた方法です。
- 3番目のステージは、アクセス対象の表とビューおよび実行対象の操作（挿入、更新、または削除など）に基づいています。

- 4番目のステージは異常ステージです。このルールにより、以前のステージでは処理されていないSQL文を処理します。このステージは、CASE文の“ELSE”句のようなものとして捉えることができます。ファイアウォール・ポリシーのこの部分の設定に応じて、4番目のステージに到達するSQL文は、渡されるか、ログに記録されるか、またはブロックされます。

オラクルでは、複数のデータベース・ターゲット全体で同じ特権ユーザーのセットを持つデータベース・ファイアウォールのお客様をサポートするために、20.9にグローバル・セットを導入しました。お客様は、すべてのデータベースにこのリストを繰り返す代わりに、データベース・ファイアウォール・ポリシー全体でこの同じセットを使用することを求めています。データベース・ファイアウォール・ポリシーのグローバル・セット機能は、この同じセットをセッション・コンテキスト情報（IPアドレス、OSユーザー、クライアント・プログラム、データベース・ユーザーを含む）にまで拡張します。これらのグローバル・セットは、複数のデータベース・ファイアウォール・ポリシー全体で使用でき、データベース・ファイアウォール・ポリシーの管理を簡素化します。

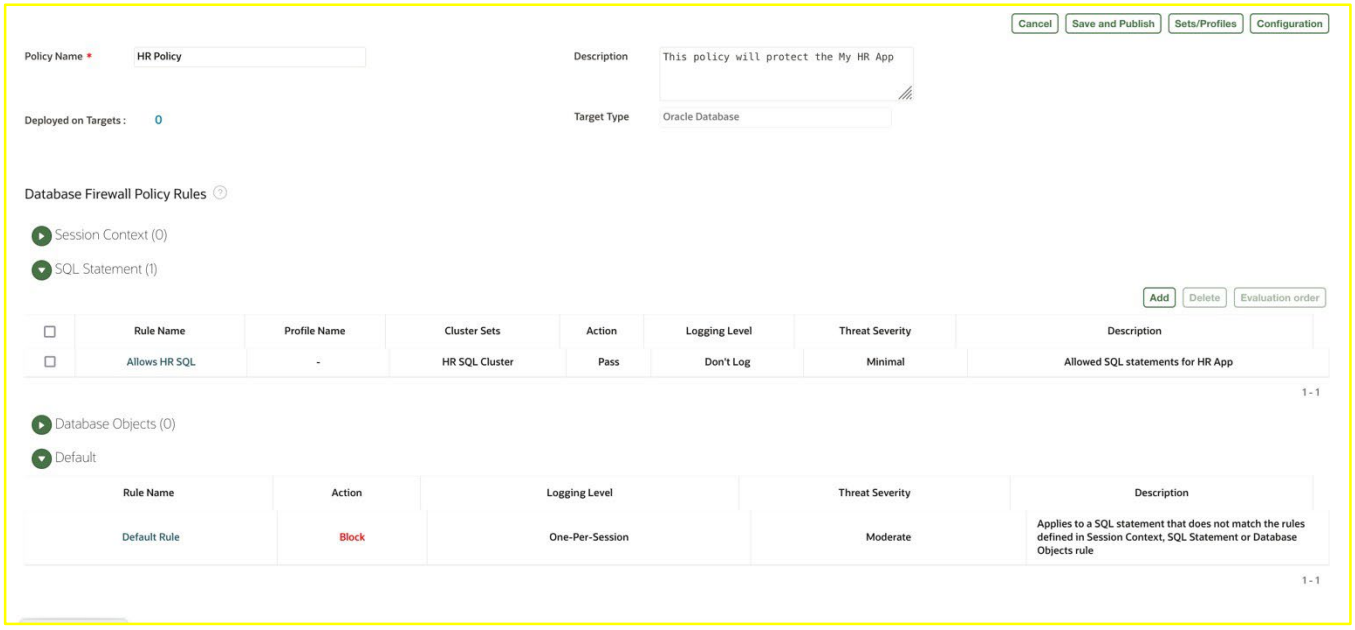


図9：データベース・ファイアウォール・ポリシー

ホスト・モニター

ホスト・モニターは、データベース・ファイアウォール用のリモート・センサーです。ホスト・モニターは、監査ターゲットと同じサーバーにインストールされ、データベース用の受信ネットワーク・トラフィックを監視します。ホスト・モニターはトラフィックのみを監視し、トラフィックをブロックすることはありません。ホスト・モニターによって取得された情報はすべて、そのファイアウォールに関するターゲットのポリシーに応じて分析のためにデータベース・ファイアウォールに転送されます。この場合、ログに記録されたSQL文は、監査リポジトリに挿入するためにAudit Vault Serverに転送されます。AVDF 20.13以降、ホスト・モニターは、ローカル（ループバックまたはBequeath）接続からのアクティビティを取得することもできます。

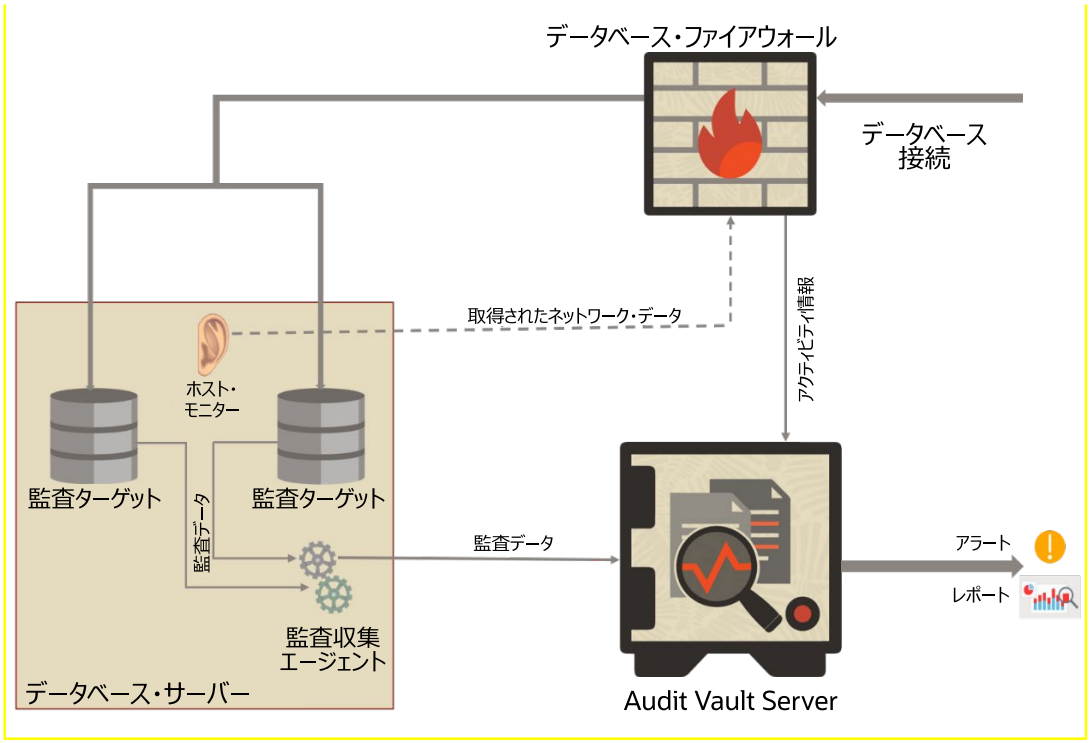


図10：簡易アーキテクチャ図

スケーラビリティとセキュリティ

監査データはビジネス・アクティビティの重要な記録で、レポートと調査の整合性を確保するためにも改ざんから保護する必要があります。AVDFでは、監査データの格納に、オラクルの業界最高レベルのデータベース・テクノロジーに基づくセキュアなリポジトリが使用されます。また、不正アクセスや改ざんを防ぐため、監査データやイベント・データはあらゆる段階で暗号化して送信され、格納されます。監査データを変更して形跡を残さないようにしようとする侵入者に対して道を閉ざすには、ソース・システムからAudit Vault Serverへの監査データのタイムリーな送信が重要です。

AVDFインタフェースでサポートされるユーザーは、監査者と管理者の2つのカテゴリに大きく分類されます。

- 監査者は、監査ポリシーと監視ポリシーを構成する他、監査レポートやアラートの定義、生成およびアクセスを行います。
- 管理者は、保護されたターゲットのネットワークおよびホストの基本設定の構成、Audit Vault AgentとOracle Database Firewallの起動と停止、Oracle Audit Vault Serverの動作の構成と監視を行います。管理者は、監査情報に対するアクセス権を持ちません。

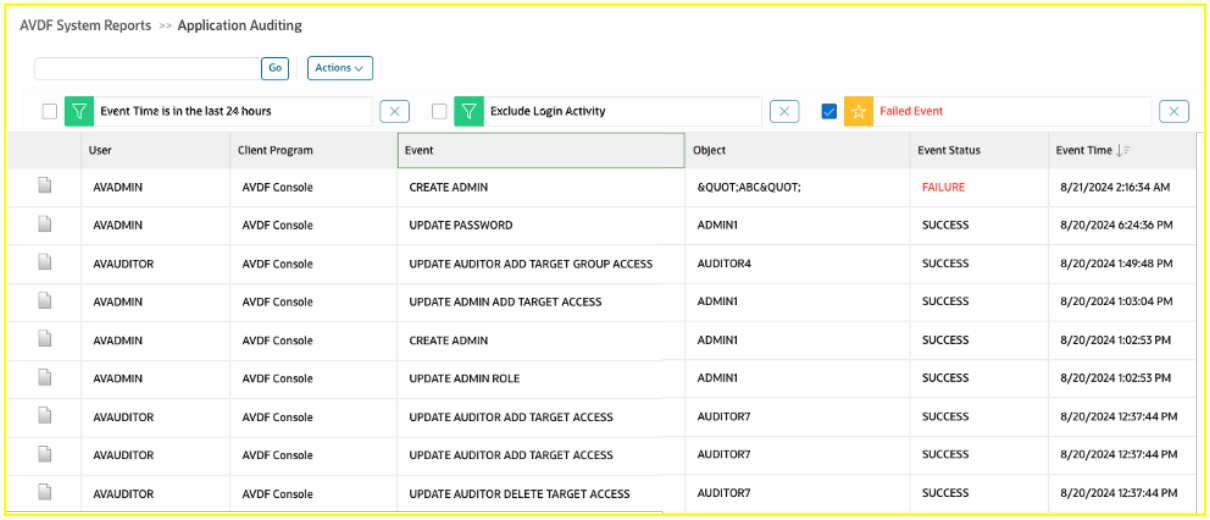
この2つのロール・カテゴリ内で、さらに役割を分割することができます。ファイル名をさらに分け、監査者や管理者それぞれに割り当てることにより、リポジトリを1つデプロイして、複数の組織、子会社、地理的領域にまたがる企業全体を確実にサポートできるようにします。きめ細かい認可は、情報がプライバシー規制やデータ保護の要件のそれぞれ異なる複数の国で使用される場合に特に重要になります。

リポジトリは、圧縮、インメモリ最適化、パーティション、暗号化、特権ユーザーの制御を含むさまざまなOracleテクノロジーを搭載した、組込みのOracle Enterprise Editionデータベース上に構築されます。最適化された統合データのストレージでは、圧縮の使用が特に重要です。これらのテクノロジーとOracle Databaseを組み合わせることにより、高度なスケーラビリティと優れた可用性、強力なセキュリティを兼ね備えたリポジトリが実現されます。

AVDFの1つのインスタンスを拡張して数千のデータベースをサポートできます。唯一の制限は、Audit Vault Serverがインストールされるサーバー・ハードウェアの機能です。

AVDF System Audit：

AVDFの自己監査機能は、重要なオペレーティング・システムと、AVDFアプライアンスで実行されるデータベースレベルのアクティビティを監査します。自己監査機能は現在、管理者と監査者によってWebコンソールとコマンドライン・インタフェースで実行されるアクティビティのAVDFのアプリケーションレベルの監視も提供しています。AVDFシステム監査レポートの下には、アプリケーション、データベース、オペレーティング・システムの監査を含む新しいレポート・セットが導入されています。これらのレポートは、管理者と監査者のアクティビティを表示して分析するのに役立ち、自己監査に関する規制当局の多くの要件を満たしています。



User	Client Program	Event	Object	Event Status	Event Time
AVADMIN	AVDF Console	CREATE ADMIN	"ABC"	FAILURE	8/21/2024 2:16:34 AM
AVADMIN	AVDF Console	UPDATE PASSWORD	ADMIN1	SUCCESS	8/20/2024 6:24:36 PM
AVAUDITOR	AVDF Console	UPDATE AUDITOR ADD TARGET GROUP ACCESS	AUDITOR4	SUCCESS	8/20/2024 1:49:48 PM
AVADMIN	AVDF Console	UPDATE ADMIN ADD TARGET ACCESS	ADMIN1	SUCCESS	8/20/2024 1:03:04 PM
AVADMIN	AVDF Console	CREATE ADMIN	ADMIN1	SUCCESS	8/20/2024 1:02:53 PM
AVADMIN	AVDF Console	UPDATE ADMIN ROLE	ADMIN1	SUCCESS	8/20/2024 1:02:53 PM
AVAUDITOR	AVDF Console	UPDATE AUDITOR ADD TARGET ACCESS	AUDITOR7	SUCCESS	8/20/2024 12:37:44 PM
AVAUDITOR	AVDF Console	UPDATE AUDITOR ADD TARGET ACCESS	AUDITOR7	SUCCESS	8/20/2024 12:37:44 PM
AVAUDITOR	AVDF Console	UPDATE AUDITOR DELETE TARGET ACCESS	AUDITOR7	SUCCESS	8/20/2024 12:37:44 PM

図11：AVDFアプリケーション監査

柔軟なデプロイメント・オプション

AVDFは、大半のデプロイメント・シナリオを満たすのに十分な柔軟性を備えています。

Audit Vault Agent

Audit Vault Agentは通常、監査ターゲットと同じサーバー上にインストールされます。ただし、場合によっては、エージェントを使用して、リモート監査ターゲットから監査データを取得できます。たとえば、監査ボリュームが少ないデータベースから取得する場合や、エージェントをデータベース・サーバーにインストールするのが現実的ではない場合です。前述のとおり、Oracle Databaseターゲットは、AVDF 20.9以降のエージェントレス収集を活用でき、Microsoft SQL Serverデータベースは20.10以降、これを使用できます。

Oracle Database Firewall

データベース・ファイアウォールは、以下の方法でデータベースへのネットワーク・トラフィックを監視できます。

- データベース・ファイアウォールをネットワーク・トラフィックに合わせて配置することで、データベースとデータベース・クライアント間のプロキシ・サーバーとして機能します。このデプロイメント・モードは、ネットワークを介した制御が制限されている仮想環境またはクラウドベース環境では一般的です。データベース・ファイアウォールがトラフィックをブロックできるのは、データベースに流れ込むネットワーク・トラフィックと一致してデータベース・ファイアウォールが配置されている場合のみです。このため、ブロッキングが必要な場合は常に、このデプロイメント・モデルが使用されます。
- データベース・ファイアウォールは、ネットワーク・トラフィックの帯域外に配置できます。この場合、トラフィックは、ネットワークSPANポート、ネットワークTAP、またはネットワーク・パケット・レプリケータを使用してデータベースにコピーされたデータベース・サーバーを着信先としています。データベースに流れ込むSQL文と、これらの文に対するデータベースのレスポンスをデータベース・ファイアウォール

が“見る”ことができる限り、どのようなテクノロジーが使用されるかは問題ではありません。ほとんどの場合、このデプロイメント・モデルは、ブロッキングが必要ないオンプレミスのデプロイメントで使用されます。

ホスト・モニター

データベース・ファイアウォールを経由してトラフィックをルーティングしたり、トラフィックをデータベース・ファイアウォールにコピーすることが現実的でない場合は、ホスト・モニターを使用できます。ホスト・モニターは、データベース・サーバーでネットワーク・アクティビティを取得し、このアクティビティをデータベース・ファイアウォールに転送して分析できるようにします。ホスト・モニターは、仮想環境におけるもう1つの一般的なデプロイメント・オプションです。

機能

データベース・ファイアウォールのデプロイメント・モードはすべて、監視アクティビティに対応しています。インライン・プロキシのみがブロッキングに対応しています。

表1.データベース・ファイアウォールのデプロイメント・モード

デプロイメント・モード	詳細	監視?	ブロッキング?
インライン・プロキシ	すべてのクライアント接続がファイアウォールを経由して行われます（リターン・トラフィックを含む）。	あり	あり
ホスト・モニター	データベース・ホスト上で動作しているエージェントが受信トラフィックをリスニングします。	あり	なし
帯域外	SPANポートまたはパケット・レプリケータから送信されてきたデータベース・トラフィックが監視されます。	あり	なし

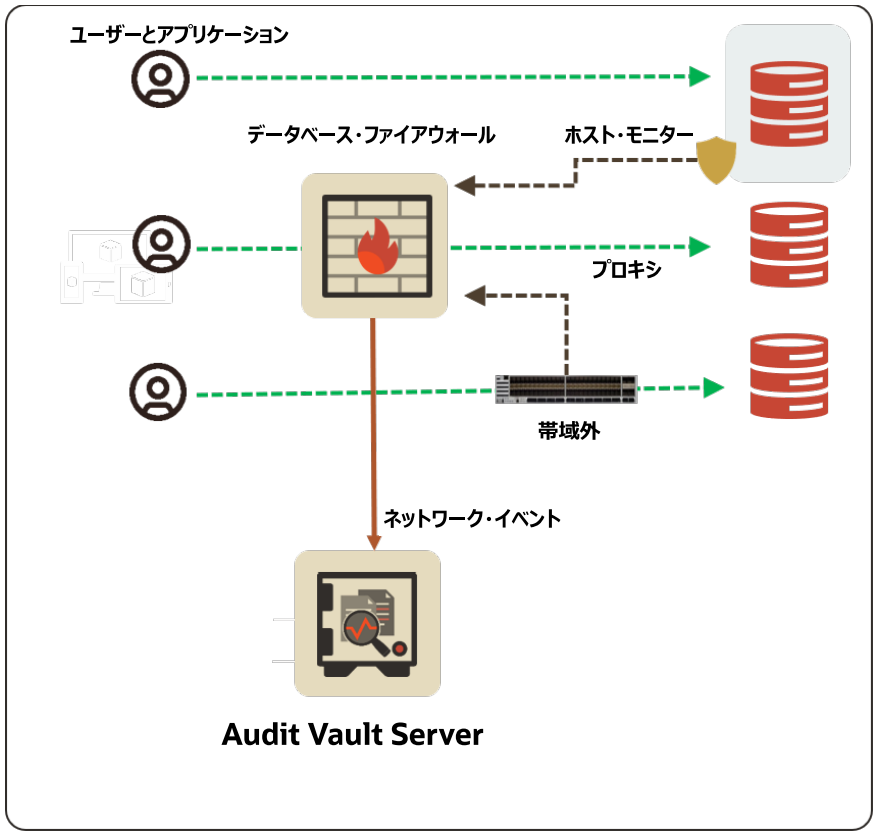


図12：データベース・ファイアウォールのデプロイメント・オプション

高可用性

Audit Vault Serverとデータベース・ファイアウォールの両方をペアで構成して、高可用性（HA）システム・アーキテクチャを実現します。ペアになったこれらのサーバーは、レジリエンスがあるペアと呼ばれます。

Audit Vault ServerのHA

レジリエンスがあるペアとして構成された場合、Audit Vault Serverには、すべてのサーバー機能を実行するプライマリ・サーバーと、Oracle Data Guardを使用してプライマリ・サーバーと同期されたセカンダリ・サーバーがあります。プライマリAudit Vault Serverに障害が発生した場合、セカンダリ・サーバーが自動的にオンラインになり、Audit Vault Agentとデータベース・ファイアウォールの両方がセカンダリ・サーバーにデータを送信し始めます。

データベース・ファイアウォールのHA

データベース・ファイアウォールのHAには2つの形式があります。どちらが使用されるかは、データベース・ファイアウォールが監視専用構成の1つとプロキシ・モードのどちらで使用されているかによって異なります。

帯域外構成とホスト・モニター構成でのデータベース・ファイアウォールとHA

監視モードでは、データベース・ファイアウォールは、Audit Vault Serverによって同期された両方の形式に対応した構成を使用して、レジリエンスがあるペアとして構成されます。プライマリ・データベース・ファイアウォールとセカンダリ・データベース・ファイアウォールの間では通信は行われません。これらは互いに独立して動作します。プライマリ・データベース・ファイアウォールとセカンダリ・データベース・ファイアウォールは同じトラフィックを受信し、両方ともログをAudit Vault Serverに送信します。Audit Vault Serverは、プライマリからのログのみを処理し、プライマリが使用不可になるまではセカンダリからのログを無視して破棄します。

プロキシ構成でのデータベース・ファイアウォールとHA

データベース・ファイアウォールがプロキシ構成で使用される場合、複数のデータベース・ファイアウォールを使用して必要なレベルのフォルト・トレランスを実現できます。

トラフィックは、ロードバランサから、DNSによって、またはロードバランスまたは透過的アプリケーション・フェイルオーバーなどのクライアントベースの構成を使用して、データベース・ファイアウォールに送信されます。

構成内のファイアウォールはすべてオンラインであり（インライン用のプライマリとセカンダリの概念はありません）、Audit Vault Serverはすべてのデータベース・ファイアウォールからのログを処理します。

サード・パーティ製ソリューションとの統合

AVDFは、SIEM、Splunk、またはログ・アグリゲータなどのサード・パーティ製セキュリティ・ソリューションと統合できます。これを行うには、データをこれらにプッシュするか、サード・パーティ製ソリューションが監査リポジトリからデータを直接プルできるようにします。

データは、Syslogを介しアラートを送信することで、サード・パーティにプッシュされます。これらのアラート・メッセージの内容と書式はすべてカスタマイズできます。監査者が定義できるメッセージ・テンプレートの数に制限はなく、そのテンプレートをさまざまなアラート定義に適用できます。

サード・パーティ製ソリューションは、監査リポジトリに直接接続してデータをAVDFからプルして監査データを抽出することで、さらなる分析やその他のデータ・フィードとの相関付けを行うことができます。監査データへのサード・パーティ製アクセスも、AVDF監査者に使用される同じ権限モデルによって制御されるため、監査情報の特定のサブセットに対してのみアクセスを提供することが可能です。

まとめ

Oracle Audit Vault and Database Firewallにより、組織は積極的に、データベースのセキュリティ体制を評価し、ネットワーク上やデータベース内部のデータベース・アクティビティを監視し、SQLインジェクションの脅威から保護し、監査データをセキュアでスケーラブルなリポジトリに統合し、またレポート作成の自動化によって監査およびコンプライアンス業務を支援することにより、セキュリティを強化できます。広範囲にわたるレポート作成およびアラート機能により、監査者やセキュリティ担当者は、潜在的に悪意のあるアクティビティに関する詳細な情報や早期警戒アラートにアクセスできるようになります。さまざまなOSやディレクトリ・サービスから取得した監査データの統合を使用する準備が整っているため、データベースより先にあるソースも監視できます。拡張可能なプラグイン・アーキテクチャにより、収集フレームワークにカスタム監査ソースを追加し、アプリケーション固有の監査データを、リポジトリにあるその他のイベント・データとともに集計し、レポートすることが可能になります。AVDFにより、Oracleデータベースだけでなく Oracle以外のデータベースに対しても同様に、効果的な発見的統制と予防的統制を実現できます。

AVDFはすでに、データベース監査とアクティビティ監視プラットフォームにとってクラス最高のプロバイダとなっています。エンタープライズ向けの包括的なセキュリティ体制管理、機密データの検出、権限ユーザー機能を備えたAVDFは今や、組織の最も重要な資産（データ）を評価、検出、監視、保護するためのワンストップ・ソリューションとなっています。

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