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

2020年7月 | バージョン20.1

目的

この技術レポートでは、Oracle Audit Vault and Database Firewallの概要が説明されています。機能、オプション、ユースケースに関する解説も含まれます。本書は、ご使用のデータベースのセキュリティ上のリスクを軽減させ、より適切に規制に準拠するための選択肢を評価するのに役立ちます。対象となるデータベースは、Oracle Database、Oracle MySQL、Microsoft SQL Server、PostgreSQL、IBM Db2、SAP Sybaseなどで、その他の多くのエンタープライズ・データベース・プラットフォームをサポートする簡単な拡張機能も対象となります。

対象読者

本書の対象読者は、企業データベースのセキュリティ制御を設計、実装、保守、運用する担当者です。

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。この機密文書へのアクセスと使用は、締結および遵守に同意したOracle Software License and Service Agreementの諸条件に従うものとします。本文書は、ライセンス契約の一部ではありません。また、オラクル、オラクルの子会社または関連会社との契約に組み込むことはできません。

本書は情報提供のみを目的としており、記載した製品機能の実装およびアップグレードの計画を支援す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。本書に記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。

エグゼクティブ・サマリー

データベース・アクティビティ監視（DAM）は、ネイティブのデータベース監査と、ネットワークベースのデータ取得によって情報を収集し、データベース・アクティビティを監視および記録して、分析とレポート作成に役立てるためのデータベース・セキュリティ・テクノロジーです。DAM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重要な部分であり、予防対策が失敗したときに、疑わしいアクティビティを可視化します。

リレーショナル・データベースの保護に使用されるテクノロジーでもう1つ重要なのは、Database Firewallです。
Database Firewallは、受信するSQLコマンドを監視および評価し、ポリシーに外れた動作を特定してアラートを発信します。
適切な場合は、Database Firewallによって、ポリシーに外れたSQLをブロックし、データベースに一切到達できないようにすることができます。

Oracle Audit Vault and Database Firewallでは、2つのテクノロジーが1つの製品にまとめられています。
Audit Vault and Database Firewallは2012年に登場し、2つの既存の製品、つまりOracle Audit VaultとOracle Database Firewallが初めて1つの製品に統合されました。ネイティブの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の相乗効果を活用して、データベース・アクティビティを総合的に見守ります。

最新リリースはAudit Vault and Database Firewall 20で、ユーザビリティ、保守作業、対象範囲が大幅に強化されています。

目次

はじめに

世界中のリレーショナル・データの半分以上がOracle Databaseに保存されており、そのデータの大半は機密度が高く、かつ金銭的な価値を持つものです。そのため、データベース、特にOracle Databaseは、データ詐取の標的になりやすくなっています。

データベース・アクティビティ監視（DAM）は、ネイティブのデータベース監査と、ネットワークベースのデータ取得によって情報を収集し、データベース・アクティビティを監視および記録して、分析とレポート作成に役立てるためのデータベース・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重要な部分であり、予防対策が失敗したときに、疑わしいアクティビティを可視化します。

監査データと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を組み合わせることは、データベース・アクティビティの全体像を把握するのに最適な方法です。ネットワーク監視だけでは、疑わしい動作をすべて捕捉することはできず、ネットワーク監視のみに特化したソリューションでは、データベースのシノニム、ファンクションベースの表示、ストアド・プロシージャのアクティビティを把握できません。反対に、データベースのあらゆる動作を監査するのも現実的ではなく、監査のみに特化したソリューションでは、すべてのデータベース・アクティビティを総合的に確認して、異常を検出し、悪意あるアクティビティの発見に役立て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、これらの問題を解決し、セキュリティと規制準拠の目標を達成できます。

リレーショナル・データベースの保護に使用されるテクノロジーでもう1つ重要なのは、Database Firewallです。Database Firewallは、受信するSQLコマンドをネットワーク・レベルで監視および評価し、異常やポリシーに外れた動作を特定して、アラートを発信します。適切な場合は、Database Firewallによって、ポリシーに外れたSQLをブロックし、データベースに一切到達できないようにすることができます。

Oracle Audit Vault and Database Firewallでは、2つのテクノロジーが1つの製品にまとめられています。Audit Vault and Database Firewallは2012年に登場し、2つの既存の製品、つまりOracle Audit VaultとOracle Database Firewallが初めて1つの製品に統合されました。ネイティブの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の相乗効果を活用して、データベース・アクティビティを総合的に見守ります。

最新リリースはAudit Vault and Database Firewall 20で、ユーザビリティ、自動化、対象範囲が大幅に強化されています。

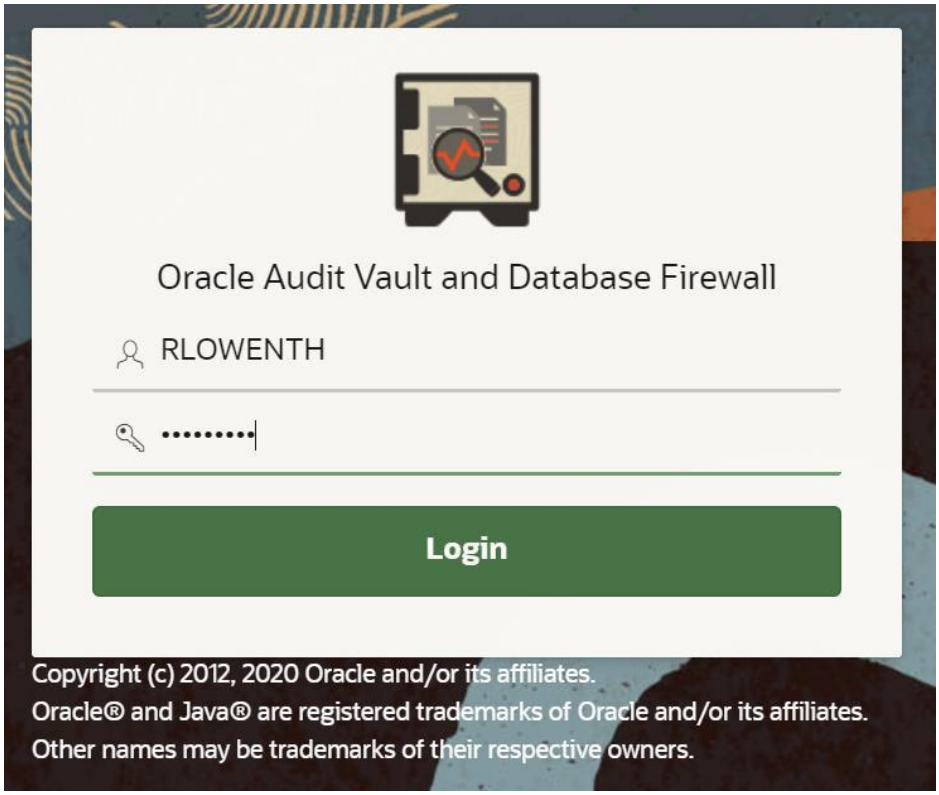

図1 - Audit Vault and Database Firewallへのログイン

Oracle Audit Vault and Database Firewallの概要

Oracle Audit Vault and Database Firewall（Oracle AVDF）は、スケーラブルで柔軟性の高いデータベース・アクティビティ監視（DAM）システムで、データベース、オペレーティング・システム、ディレクトリ、ファイル・システム、アプリケーションの監査データを1つのリポジトリに統合して、分析、アラートの発信、レポート作成に利用することができます。Oracle AVDFはネットワークを介してデータベースに送信されるSQL文も監視して、検証、許可、記録し、不正なSQL文をブロックすることもできます。

Oracle AVDFでは、シンプルなフィルターベースのレポート用インタフェースから、多様なレポート機能を利用できるため、関連する情報まで簡単にドリルダウンすることができます。Oracle AVDFがあれば、1つのシステムで非常に多くのデータベースのアクティビティを監視し、1つのコンソールから全データベース環境（サポートされるインフラストラクチャを含む）のセキュリティ・イベントをレポートしたり分析したりできます。

Oracle Audit Vault and Database Firewallは、一般的なエンタープライズクラスのデータベースをサポートしています。設定不要で使用できる監査収集は、Oracle Database、Oracle MySQL、Microsoft SQL Server、SAP Sybase、IBM Db2 LUW、PostgreSQLなどをサポートしています。他のほとんどのデータベースやアプリケーションは、付属のカスタム・コネクタ・フレームワークを使用するとサポートされます。このフレームワークでは、JDBCやRESTful APIによってデータが収集されます。カスタム収集は、監査データをXMLやJSONのファイルに書き込むシステムで使用することもできます。Javaベースのソフトウェア開発キット（SDK）も付属しており、どのカスタム・コネクタ・フレームワークのオプションを使用してもアクセスできない例外的なターゲットにも対応します。

Oracle Audit Vault and Database Firewallリリース20の新機能

Oracle AVDF 20は、Oracle AVDFを複数年にわたって更新してできたバージョンで、新しいユーザー・インタフェース、新しいデータベースを含むサポート範囲の拡張、基盤となるインフラストラクチャの更新、前後の値を収集するためのまったく新しいアーキテクチャなどを特徴としています。

ユーザー・インタフェース

オラクルはユーザー・インタフェースをアップグレードして、最新式で応答が早く、分かりやすいルックアンドフィールのインタフェースにしました。UIはシンプルで、一般的なワークフローに合うように、またナビゲーションが簡単になるように最適化されています。Audit Vault ServerもDatabase Firewallも同じコンソールから管理できるため、管理のための操作を一元化し、監視が必要なコンソールの数を減らすことができます。

新しいデータベース・タイプへの対応

Oracle AVDF 20以前から、オラクルはOracle Database、Oracle MySQL、Microsoft SQL Server、SAP Sybase、IBM Db2 LUWをサポートしていました。カスタム・コレクタ・フレームワークによって、監査データをXML形式で生成するデータベース、またはJDBCでアクセスできるデータベース表に監査証跡を書き込むデータベースも追加できるようになりました。

Oracle AVDF 20では、設定不要でサポートするデータベースにPostgreSQLが追加され、カスタム・コレクタ・フレームワークが拡張されて、JSONデータファイルと、RESTful APIでアクセス可能な監査証跡がサポートされるようになりました。

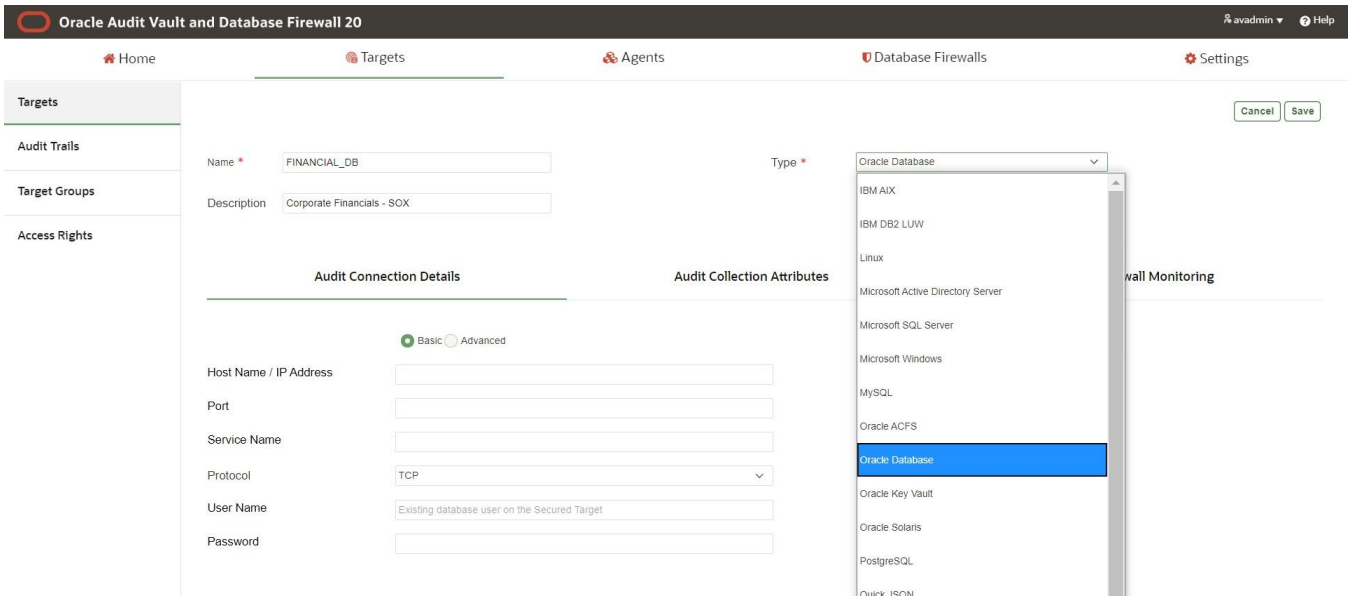

図2 - 新しいターゲットの登録

前後の値の収集

「前後の値の収集」とは、読んで字の如しです。データの値が変更されると、Oracle AVDFは古い値（変更される*前*）と新しい値（変更された後）を記録し、変更したユーザーと変更時刻についても記録します。前後の値の収集は、ヘルスケアや金融サービスの業界、またその他の規制の厳しい業界で広く使われています。
監査者は前後の値の収集を利用することで、あらゆる変更における個別のデータ属性のライフサイクルを追跡できます。これはデータのガバナンス要件の多くで重要な要素となります。

以前のバージョンのOracle AVDFは、Oracle Streamsを使用して前後の値を収集していましたが、Oracle StreamsはOracle Multitenantをサポートせず、Oracle以外のデータベースで使用することはできません。また、19cなどの新しいOracle Databaseをサポートしていません。

Oracle AVDF 20にはOracle GoldenGateが含まれており、Oracle GoldenGateを使用して前後の値を収集するようになっています。GoldenGateを使用することで、スループットの改善、管理の容易さ、マルチテナント・データベースのサポート、Oracle Database 19cのサポートなど、多数の利点が生まれました。

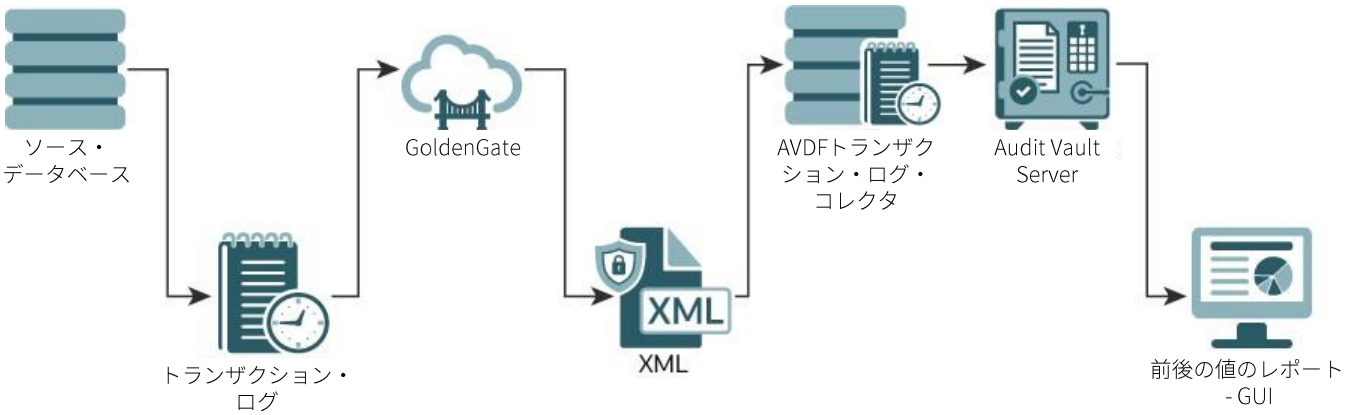

図3 - トランザクションの監査証跡のデータ・フロー

運用環境の改善

Oracle AVDF 20では、収集したデータの自動アーカイブ、Microsoft Active DirectoryまたはOpenLDAPとのAVDFユーザーの統合、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・カードのボンディング、AVDFポートのカスタマイズをサポートするようになりました。Oracle AVDFの管理者とシステム・インテグレーターは、新バージョンのOracle AVDFは使いやすく、最新のデータセンターとクラウド・デプロイメントへの対応が強化されたと感じることでしょう。

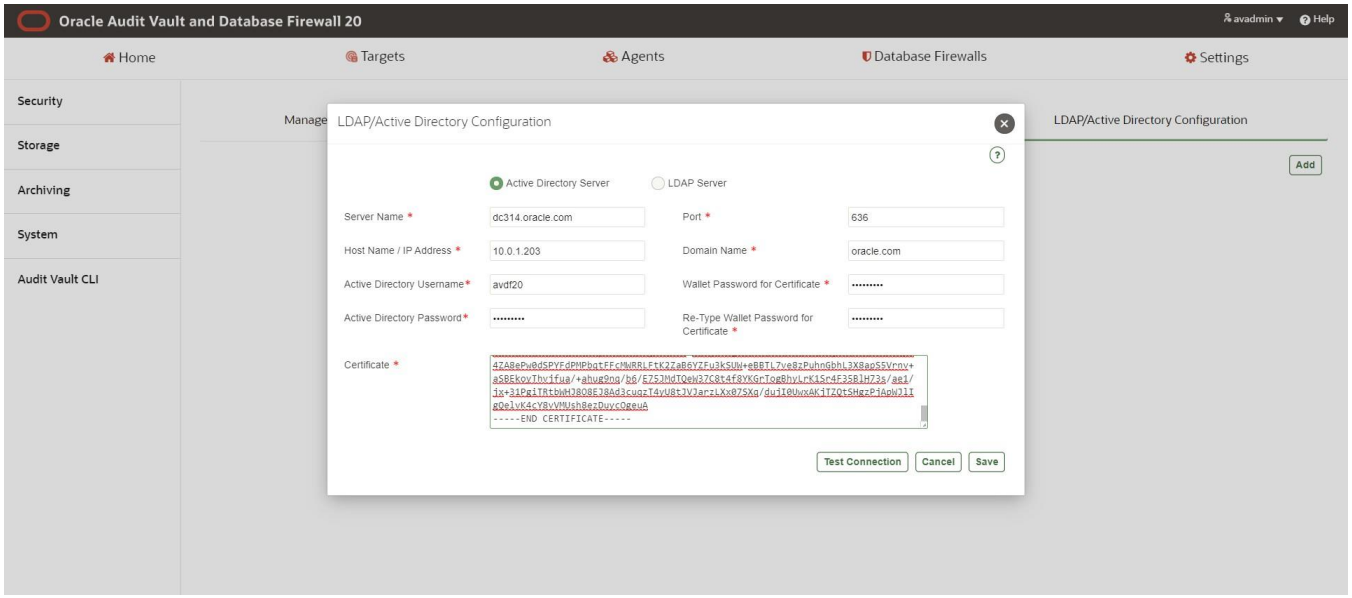

図4 - Active Directoryとの統合

レポートとアラート

Oracle Audit Vault and Database FirewallのようなDAMシステムでメインの出力となるのは、レポートとアラートです。
システムが収集した情報は、レポートという形式で表示され、該当する場合にはアラートが発信されます。

すぐに対応するべき状況が検出された場合に、関係者にアラートが送られます。アラートが発信されるケースとしてよくあるのは、短時間のうちに複数回、ログインの失敗が発生した場合や、機密データに許可のないアクセスがあった場合などです。
Oracle AVDFでは、個別のイベントが起きた場合（非常に機密性の高いデータにアクセスがあった場合など）にアラートを出すことも、イベントの状況（同じIPアドレスからのログインの失敗が1分間に10回を超えた場合など）に応じてアラートを出すこともできます。

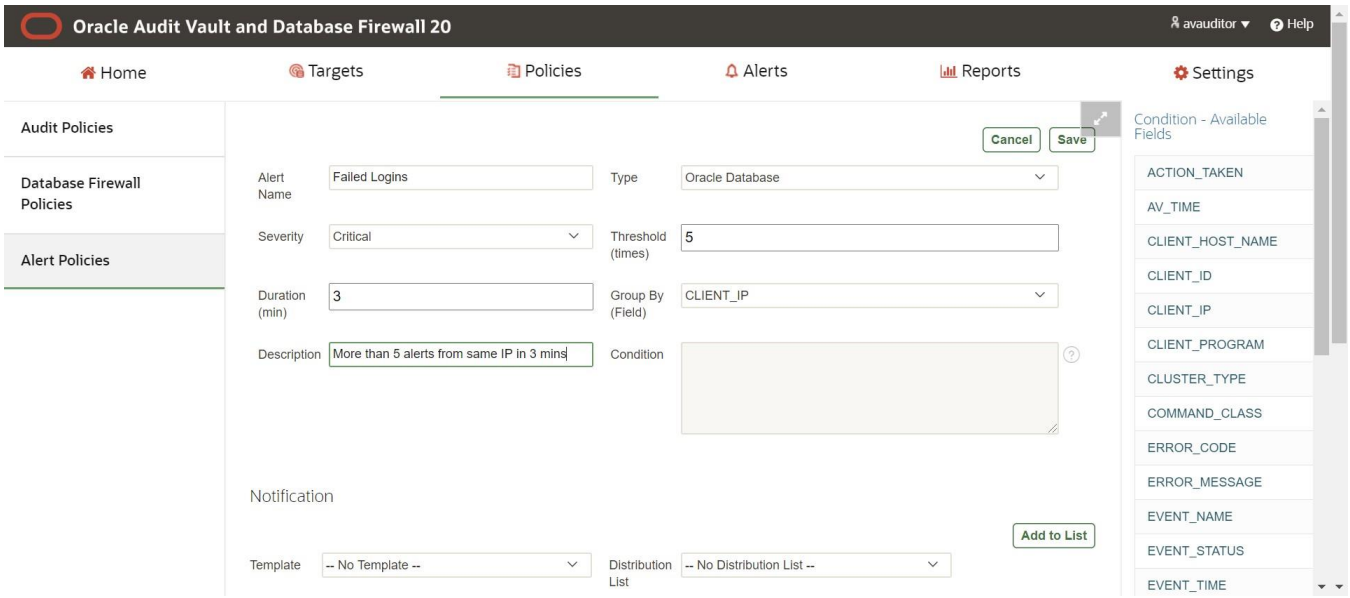

図5 - アラート・ポリシーの作成

記録や規制への対応を目的とした正式なレポートを作成することも、調査用に対話形式の簡易なレポートを作成することもできます。監査者はAudit Vault and Database Firewallコンソールからレポートにアクセスできます。また、スプレッドシートやドキュメントの形式でレポートを自動的に生成して、電子メールで配信するスケジュールを設定することもできます。必要な場合は、レポートが確認されたかどうかをOracle AVDF内で追跡し、確認者からのコメントを付けることもできます。

Oracle AVDFでは、HIPAA、PCI、GDPRのような規制に対応したコンプライアンス・レポートや、ログイン失敗などの一般的なセキュリティ要件に関するレポート、SUDO操作のレポート、DMLなど、あらかじめ構成された数十種類のレポートを使用できます。レポートを簡単にカスタマイズして保存し、後で使用することができます。

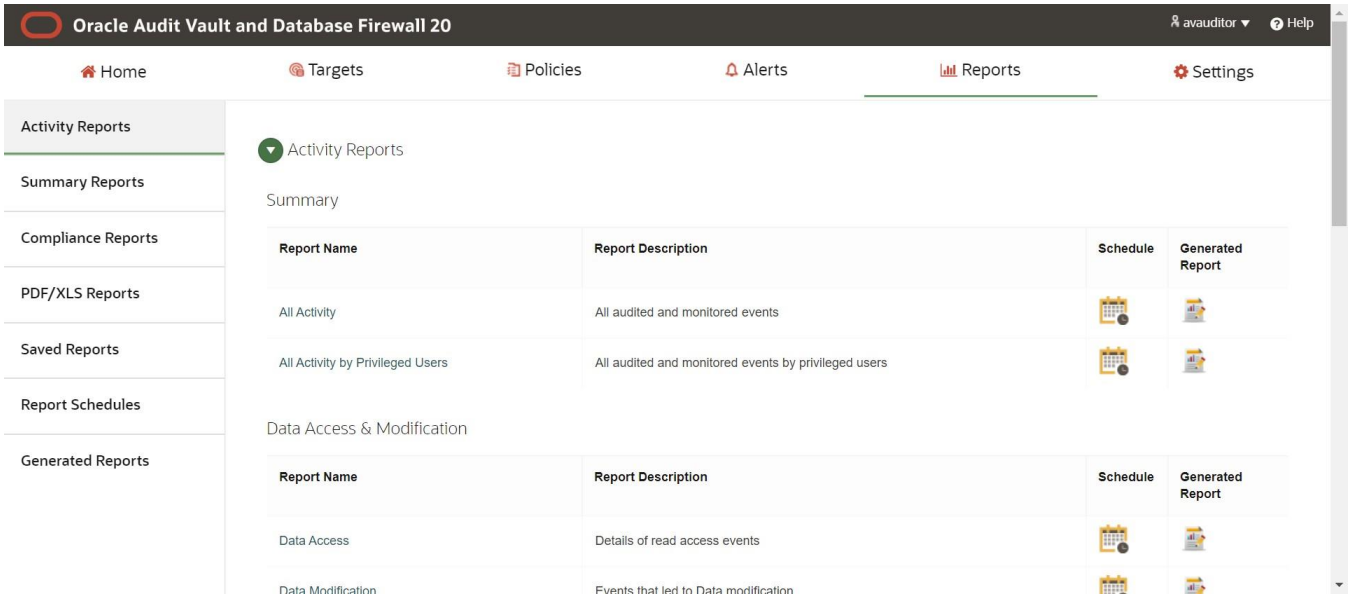

図6 - さまざまな監査レポート

Oracle AVDFでは多彩なレポート機能に加えて、Oracle Databaseとの互換性がある外部のレポート作成ツールや分析ツールを使用できます。また、Oracle Audit Vault and Database Firewallのライセンスには、Oracle Business Intelligence Publisherを限定的に使用できるライセンスが付属しています。

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

Oracle Audit Vault and Database Firewall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です。Oracle AVDFにはおもなコンポーネントが4つあります。

- Audit Vault Server
- Audit Vault Agent
- Database Firewall
- ホスト監視

Audit Vault Server

Audit Vault Serverは、Oracle AVDFの必須コンポーネントです。どのAVDFインストールにも、最低1つのAudit Vault Serverが必要です。このサーバーは、強化されたOracle Linuxオペレーティング・システム、監査リポジトリとして機能するOracle Database、AVDFコンソール用インタフェースおよびAVCLIコマンドライン・インタフェースを備えるAudit Vault and Database Firewallアプリケーションで構成されます。

Oracle Audit Vault and Database Firewallは、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、ディレクトリ、ファイル・システムなどの監査ターゲットと、アプリケーション固有の監査データとを統合します。このデータは、監査ターゲットから収集されて、監査リポジトリ、つまりAudit Vault Server上にあるOracle Databaseに読み込まれます。

監査リポジトリ・データベースは暗号化され（Oracleの透過的データ暗号化を使用）、Oracle Database Vaultで保護されます。

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て、そのデータをAudit Vault Serverに安全に送信します。1つのAudit Vault Agentは、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、ディスク領域をほとんど消費しません。Audit Vault AgentとAudit Vault Serverとの間の通信では、TLS 1.2が使用されます。

Database Firewall

Database Firewallは、データベースに送信されているネットワーク・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検証します。Database Firewallポリシーで、そうしたSQL文をどのように処理するかを制御します。Database Firewallは、それ以上のアクションを起こさずにSQL文をデータベースに渡すこともできますし、SQL文に関する情報をAudit Vault Serverに送信し、監査リポジトリに入れることもできます。Database Firewallがそのトラフィックとインラインで構成されている（データベース・プロキシ・サーバーとして動作している）場合は、SQL文をブロックして、ターゲット・データベースに到達しないようにしたり、ブロックされた文の代わりとなるSQLコマンドを配置したりできます。Database Firewallは複数ステージのポリシーを使用して、SQL文をどのように処理するかを決定します。

最初のステージでは、ポリシーは送信元の接続のIPアドレス、オペレーティング・システムのユーザー名、データベースとの接続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のアカウントを検証します。Database Firewallは、そうした要素に基づいて、条件に合う接続を許可したり、後から検証するために記録したり、（インラインの場合は）ブロックしたりできます。

次のステージは、SQL文の構造に基づいたもので、構文に従って通過/ログ/ブロックのいずれかのアクションを実行します。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したり、アラートを発したりするための優れた方法です。3番目のステージは、アクセスされている表/ビューおよび実行されている操作（挿入/更新/削除など）に基づいたものです。4番目のステージは例外的なものです。前の3つのステージのいずれでも処理されなかったSQL文が、このポリシーで処理されます。CASE文の"else"のフレーズのようなものだと言えるかもしれません。4番目のステージに到達したSQL文には、Database Firewallポリシーのこの部分の設定に従って、通過/ログ/ブロックの処理が行われます。

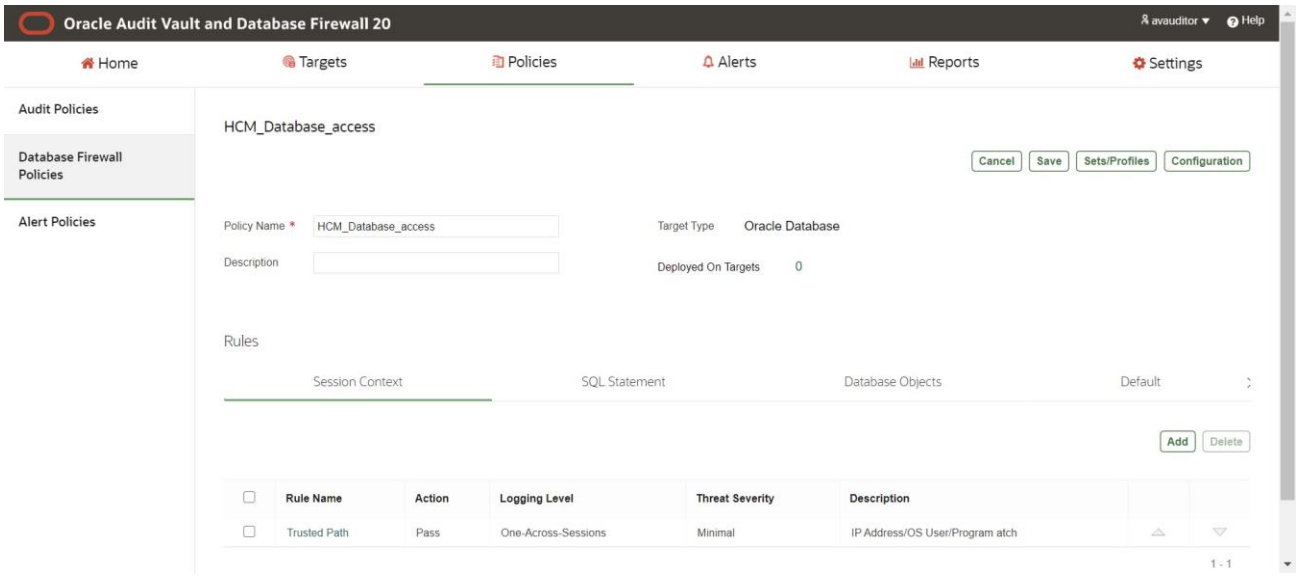

図7 - Database Firewallポリシー

ホスト監視

ホスト監視は、Database Firewallをリモートで監視するものです。ホスト監視は監査ターゲットと同じサーバーにインストールされ、データベースの受信ネットワーク・トラフィックを監視します。ホスト監視はトラフィックの監視のみに使われるため、ブロッキングの操作はできません。ホスト監視に捕捉されたものはすべて、Database Firewallに送信され、そのファイアウォールのターゲットのポリシーに従って分析されます。また、ログに記録されたSQL文はAudit Vault Serverに送信され、監査リポジトリに入ります。

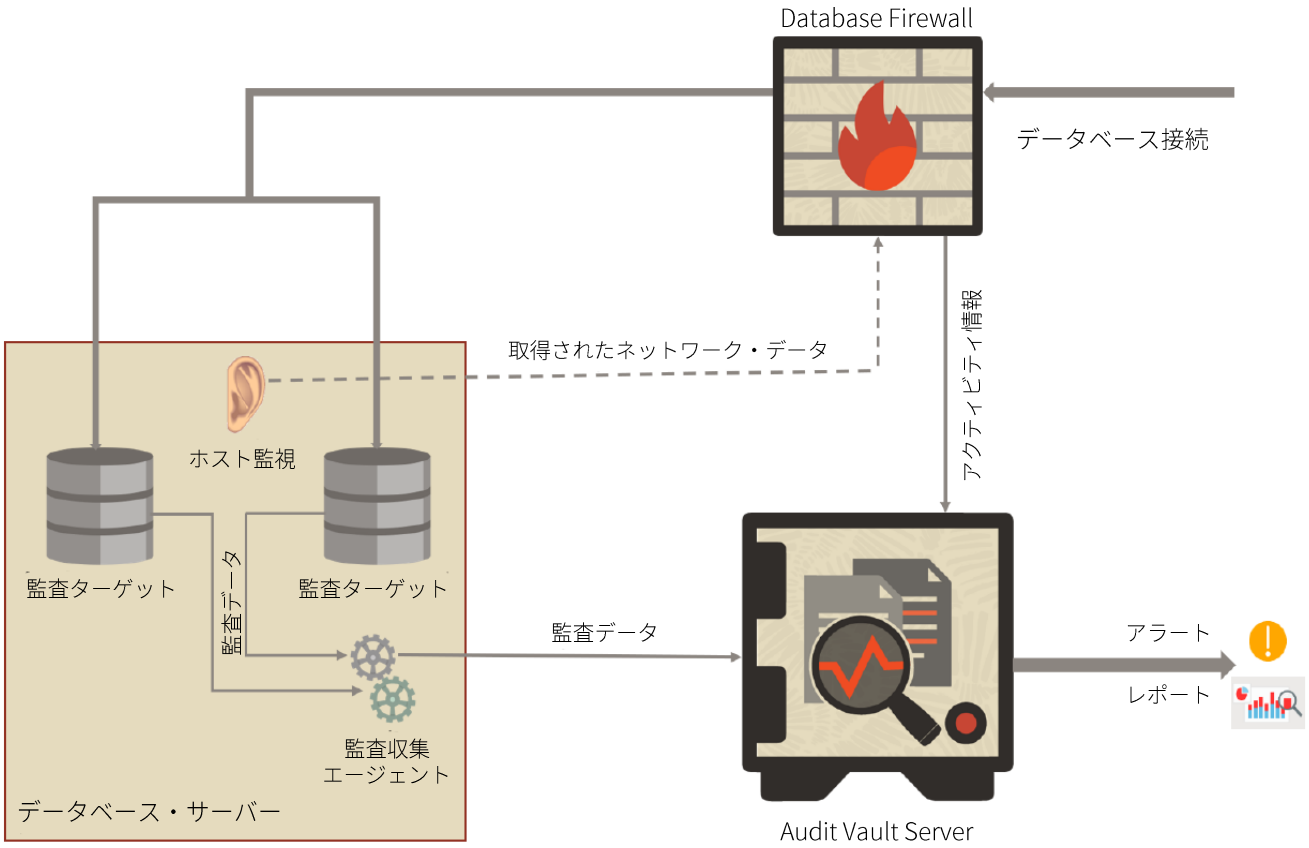

図8 - アーキテクチャの簡易図

スケーラビリティとセキュリティ

監査データは業務の重要な記録の1つであり、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。Oracle Audit Vault and Database Firewall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。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では、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ことが重要です。

Oracle Audit Vault and Database Firewall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ほか、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Database Firewallの起動と停止、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。データベースをさらに分け、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、情報がプライバシ規制やデータ保護要件のそれぞれ異なる複数の国で使用される可能性があ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します。

1つのOracle Audit Vault and Database Firewallで、非常に多くのデータベースをサポートするようにスケーリングできます。唯一の制限となるのは、Audit Vault Serverがインストールされるサーバー・ハードウェアの性能です。

柔軟なデプロイメント・オプション

Oracle Audit Vault and Database Firewallは柔軟性が高いため、ほとんどすべてのデプロイメント・シナリオに対応します。

Audit Vault Agent

Audit Vault Agentは通常、監査ターゲットと同じサーバーにインストールされますが、リモートの監査ターゲットから監査データを取得するのに使われる場合もあります（たとえば、監査の量が少ないデータベースで、そのデータベース・サーバーにエージェントをインストールするのが現実的ではない場合など）。

Database Firewall

Database Firewallによって、データベースへのネットワーク・トラフィックを複数の方法で監視できます。

Database Firewallは、ネットワーク・トラフィックとインラインに配置され、データベースとデータベース・クライアントとの間のプロキシ・サーバーとして機能します。これは、ネットワークへの制御が限定される仮想化環境やクラウドベースの環境でよくあるデプロイメント・モードです。Database Firewallは、データベースに送られるネットワーク・トラフィックとインラインに配置されている場合のみトラフィックをブロックできるため、ブロッキングが必要な場合は必ずこのデプロイメント・モデルが使用されます。

Database Firewallは、ネットワーク・トラフィックの帯域外に配置して、データベース・サーバーに送信されるトラフィックを、ネットワークSPANポート、ネットワーク・タップ、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できます。Database Firewallが、データベースに送信されるSQL文と、それらの文へのデータベースのレスポンスを認識している限り、どのようなテクノロジーが使用されているかは問題にはなりません。これは、ブロッキングが必要ではないオンプレミス・デプロイメント向けにもっともよく使用されるデプロイメント・モデルです。

ホスト監視

Database Firewallにトラフィックを通過させることも、トラフィックをコピーすることも実際的ではない場合は、ホスト監視が使用されることがあります。ホスト監視はデータベース・サーバーのネットワーク・アクティビティを捕捉して、Database Firewallに送信し、分析できるようにします。ホスト監視は、仮想化環境で一般的なデプロイメント・オプションの1つです。

機能

Database Firewallの3つのデプロイメント・モードすべてを、監視アクティビティに使用できます。ブロッキングが可能なのはインライン・プロキシのみです。

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	リターン・トラフィックを含めたすべてのクライアント接続がファイアウォールを経由する	可	可
ホスト監視	データベース・ホストで稼動するエージェントで、受信トラフィックをリスニングする	可	不可
帯域外	SPANポートやパケット・レプリケータを使用して、送信されてきたDBトラフィックを監視する	可	不可

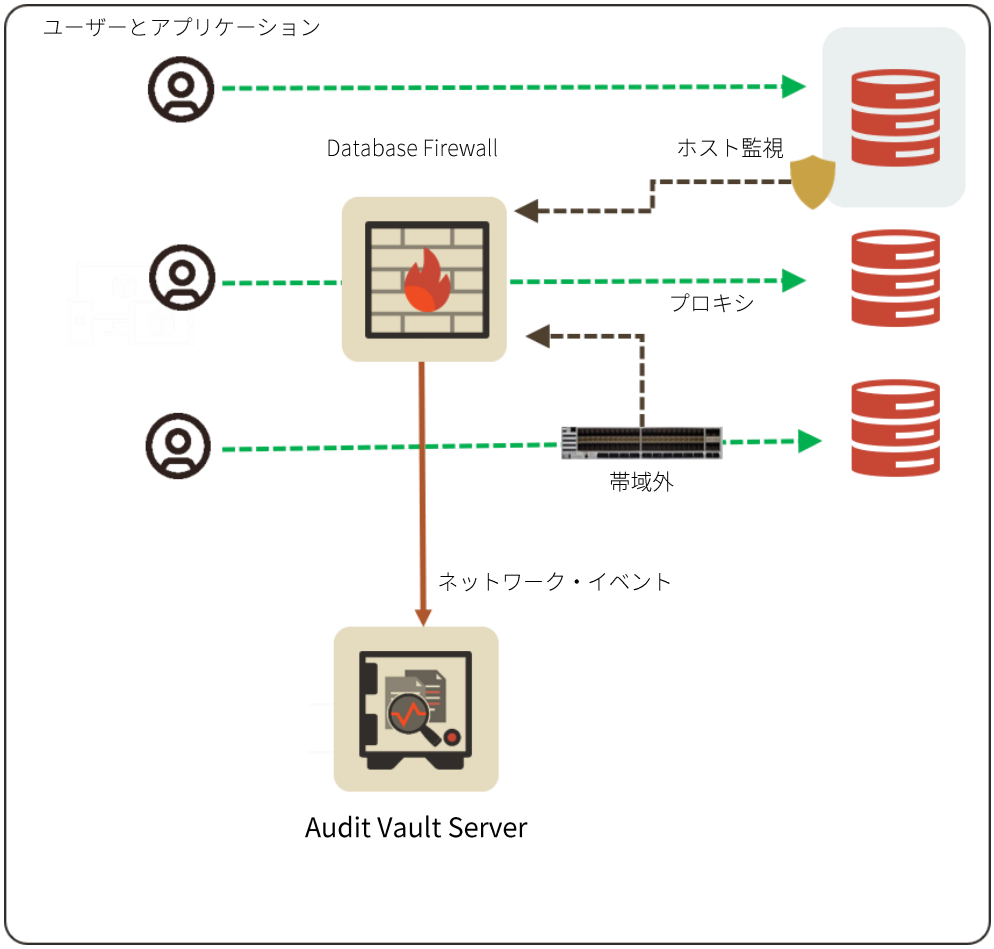

図9 - Database Firewallのデプロイメント・オプション

高可用性

Audit Vault ServerとDatabase Firewallは両方とも、ペアで構成して、高可用性システムのアーキテクチャにすることができます。ペアで構成されたサーバーは、*レジリエント・ペア*と呼ばれます。

Audit Vault Serverの高可用性

Audit Vault Serverがレジリエント・ペアとして構成された場合、1つはプライマリ・サーバーとしてサーバーの全機能を実行し、もう1つはセカンダリ・サーバーとして、Oracle Data Guardを使用してプライマリと同期されます。プライマリのAudit Vault Serverで障害が発生すると、セカンダリ・サーバーが自動的にオンラインになり、両方のAudit Vault AgentとDatabase Firewallは、セカンダリへのデータ送信を開始します。

Database Firewallの高可用性

Database Firewallの高可用性には2つの形式があり、Database Firewallがプロキシ・モードで使われているか、それとも監視のみのいずれかの構成で使われているかによって、どちらの形式であるかが決まります。

帯域外またはホスト監視構成でのDatabase Firewallと高可用性

監視モードでは、Database Firewallはレジリエント・ペアとして構成され、どちらもAudit Vault Serverによって同期される構成になっています。プライマリ・データベースとセカンダリ・データベースのファイアウォールの間には通信が発生せず、それぞれが独立して動作します。プライマリ・データベースとセカンダリ・データベースのファイアウォールは同じトラフィックを受信し、両方がAudit Vault Serverにログを送信します。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は無視して破棄します。

プロキシ構成でのDatabase Firewallと高可用性

Database Firewallがプロキシ構成で使用されている場合、希望するレベルのフォルト・トレランスを実現するために、2つ以上のDatabase Firewallが使用される場合があります。

トラフィックは、DNSや、クライアントベースの構成（ロードバランスまたは透過的なアプリケーション・フェイルオーバーなど）を使用して、ロードバランサからDatabase Firewallに送信されることがあります。

構成内のすべてのファイアウォールはオンラインで（インラインにプライマリ/スタンバイがあるというコンセプトではない）、Audit Vault Serverは、すべてのDatabase Firewall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

Oracle Audit Vault and Database Firewallは、SIEM、Splunk、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、サード・パーティ製ソリューションにデータをプッシュすることも、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直接データを*プル*することもできます。

データは、syslog経由でアラートを送信することによって、サード・パーティのソリューション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することで、Oracle AVDFからデータを*プル*し、監査データを抽出して、さらに分析したり、他のデータ・フィードと関連付けたりできます。サード・パーティ製ソリューションによる監査データへのアクセスは、AVDF監査者に使用されるものと同じ権限モデルで制御されるため、監査情報の特定の部分のみへのアクセスを許可することができます。

まとめ

Oracle Audit Vault and Database Firewallにより、組織は、ネットワーク上やデータベース内部のデータベース・アクティビティを積極的に監視し、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。さまざまなオペレーティング・システムやディレクトリ・サービスから取得した監査データの統合が標準でサポートされているため、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。
Oracle Audit Vault and Database Firewall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。

オラクルの情報を発信しています

+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

Oracle Audit Vault and Database Firewall
2020年7月

Database Security Product Management、Russ Lowenthal