ORACLE

Oracle Audit Vault and Database Firewall 20

よくある質問

2021年2月

目的

この技術レポートでは、Oracle Audit Vault and Database Firewall 20について、もっとも多く寄せられる質問の一部に答えます。

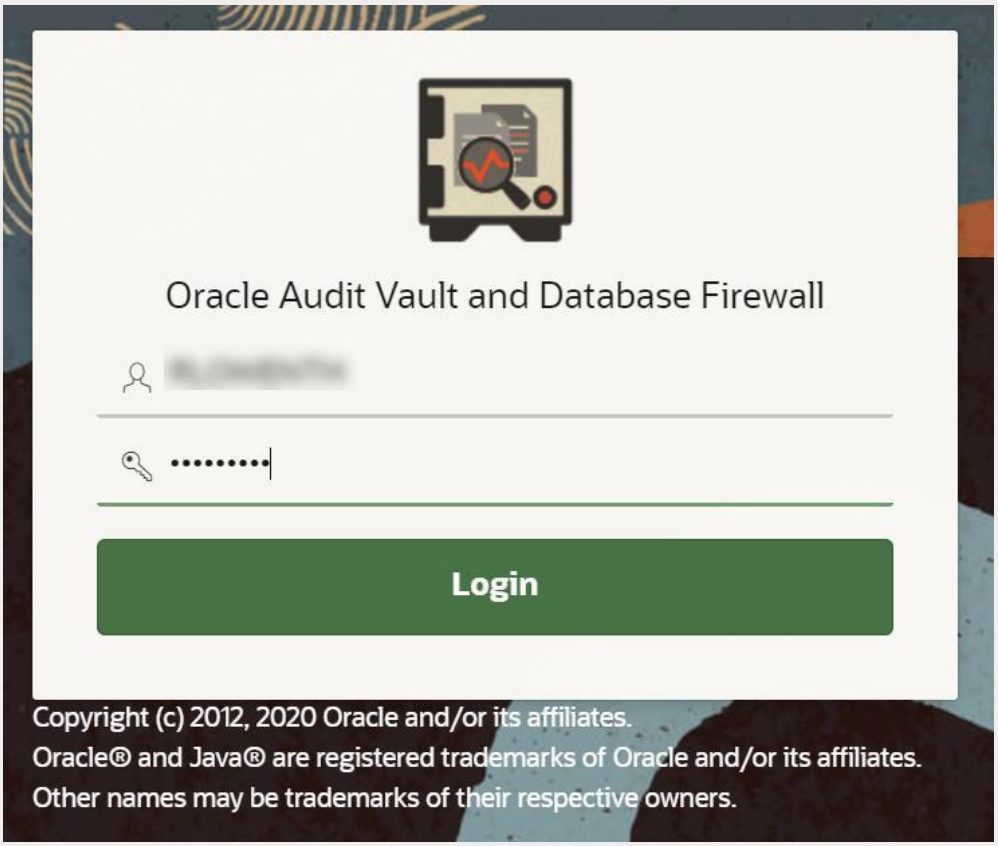
対象読者

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。



1. 製品の概要

a. Oracle Audit Vault and Database Firewall（Oracle AVDF）の新機能は何ですか。

Oracle AVDF 20は、一般的なワークフローを簡単に進めることのできる、改良された最新のユーザー・インタフェース、新しいターゲットの種類（PostgreSQL、MongoDB（シンプルな属性マッピング表を使用））に対応する拡張された監査収集、簡便化されたファイアウォール、企業での使用をサポートするその他の機能を備えています。
全機能を確認するには、Oracle AVDF 20.1のリリース・ノートを参照してください。この後の「追加情報」のセクションに、PowerPoint、データシート、その他の参考資料へのリンクがあります。

b. Audit VaultとDatabase Firewallにはどのような関連がありますか。両方とも必要なのでしょうか。

Oracle AVDFはネイティブの監査収集と、ネットワークベースのSQLトラフィック監視をサポートしています。
監査データは、Database Firewallからのネットワーク・イベントと一緒に、Audit Vault Serverに保存されます。
そのため、アクティビティ・データを関連付けて、レポートを作成することができます。

オラクルは総合的なアプローチを推奨しており、データベースの監査とネットワークベースのSQLトラフィック監視の両方をサポートしています。どちらの機能から開始しても構いません。必要に応じてアーキテクチャを拡張し、両方を利用してください。

c. Oracle AVDFでは、どのようなターゲットの種類とバージョンがサポートされていますか。

Oracle AVDFでは、Oracle Database、Microsoft SQL Server、MySQL、IBM Db2、PostgreSQL、SAP Sybase、およびLinux、Windows、Solaris、AIXのオペレーティング・システム・ログがサポートされています。カスタム・コレクタを使用すると、アプリケーションの監査表、XML、JSON、MongoDBからのデータを収集できます。
詳しくは、Installation Guideのプラットフォーム・サポート・マトリックスを参照してください。

d. Oracle AVDFはアプリケーションなどの他のソースからの監査データをどのようにまとめますか。

Oracle AVDFは、アプリケーション表やファイル（XML、JSON）からの監査データを収集し、標準の形式にマッピングし、すべてのソースからのデータを1つのレポートにまとめます。詳しくは、Developer's Guideを参照してください。

e. 監査とネットワーク監視の違いは何ですか。両方とも必要なのでしょうか。

監査では通常、特定のイベントが発生した後に詳細情報を取得します。SQL文から直接の場合もありますし、ストアド・プロシージャ・コールを経由する場合もあります。SQLトラフィックを監視すると、SQL文がデータベースに到達する前に分析して、対応できるため、疑わしい文をブロックできます。どちらの場合も、監査ログやイベント・ログを収集する条件を指定できます。一方は発生後、もう一方は発生前というように、2つの方法によって、同じイベントを異なる視点で確認できます。両方とも、アラートを発することができます。

オラクルは総合的なアプローチを推奨しており、データベースの監査とネットワークベースのSQLトラフィック監視の両方をサポートしています。どちらか一方の機能で開始してから、アーキテクチャを拡張し、両方を利用することができます。

f. 監査ポリシーとデータベース・ファイアウォール・ポリシーをどのようにプロビジョニングすれば良いですか。

Oracle AVDFは監査ポリシーを表示するためのインタフェースを備えており、1回のクリックで、ターゲット・データベースにポリシーをプロビジョニングできます。ファイアウォール・ポリシーもUIから構成可能で、SQLの許可、記録、アラートの発信、置換、ブロックが可能です。詳しくはAuditor's Guideを参照してください。

g. データベース・トラフィックを監視する方法には何がありますか。

Database Firewallを構成して、監視とブロッキングの両方を実行することも、監視のみを実行することもできます。監視とブロッキングを実装するには、ファイアウォールをプロキシ・モードで構成して、すべてのデータベース・トラフィックがファイアウォールを通過するように設定する必要があります。ネットワークベースのSQLトラフィック監視を実装する場合は、ネットワーク・スイッチのspanポートからデータベース・ファイアウォールにトラフィックを送信するか、データベース・マシンにホスト監視をセットアップして、SQLトラフィックをDatabase Firewallに送信します。詳しくは、Administrator's Guideを参照してください。

h. 監査データ・ログとネットワーク・ログの両方をまとめたレポートを取得できますか。

Audit Vault Serverは、監査データとネットワークSQLトラフィックを統合し、監査ログまたは取得したSQLトラフィックをもとにして、すべてのデータベース・アクティビティをまとめて確認できるようにします。この統合されたデータから、アラートとレポートが作成されます。

i. OSのアクティビティとデータベースのアクティビティを関連付けて、全体像を確認することはできますか。

はい、Oracle AVDFでは、SUまたはSUDOによる移行前の元々のLinux OSユーザーと関連付けられた、データベース・イベントの詳細情報が表示されたレポートを作成できます。

2. おもなユースケース

a. Oracle AVDFはコンプライアンス・レポートの要件にどのように準拠していますか。

Oracle AVDFでは、GDPR、PCI、GLBA、HIPAA、IRS 1075、SOX、UK DPA向けのコンプライアンス・レポートがあらかじめ用意されています。特定の目的や、業界/地域特有のコンプライアンス要件に合わせてレポートをカスタマイズできます。サード・パーティのレポート・ツールをAudit Vaultスキーマに接続して、分析やレポートに利用することもできます。

b. Oracle AVDFは特権ユーザーのアクティビティも監査および追跡できますか。

管理者のアクティビティと指定ユーザーに対する監査ポリシーを有効にできます。Oracle AVDFには、特権ユーザーを対象にするレポート（特権ユーザーによるすべての監査アクティビティが表示される）を含めた複数のレポートがあらかじめ定義されています。

c. Oracle AVDFはデータベース内の機密データへのアクセスを追跡できますか。

機密性の高いオブジェクトのリストをファイルとしてインポートできます。このファイルは、Oracle Database Security Assessment Tool（Oracle DBSAT）またはEnterprise Manager（アプリケーション・データ・モデル）を実行することで生成できます。Oracle AVDFはこのリストを使用して、機密データへのアクティビティ、特権ユーザーによる機密データへのアクティビティなどに関する、定義済みのレポートを生成します。

d. アクセスの悪用や無許可のアクセスについて調査するときにOracle AVDFはどのように役立ちますか。

Oracle AVDFユーザーは、"All Activity Report"を使用して、どのオブジェクトへのアクセスがあったかを分析できます。Oracle AVDFでは、ユーザー、オブジェクト、日付などでフィルタリングし、取得されたデータを分析して、無許可のユーザーがオブジェクトにアクセスしていなかったかを確認できます。

e. Oracle AVDFはユーザー、ロール、権限、エンタイトルメントの変更を追跡できますか。

Oracle AVDFは、スケジュール設定に基づいてエンタイトルメントをチェックし、最終レポートから変更された箇所に関する差分レポートを作成するように構成できます。Oracle AVDFはユーザー、ロール、権限への変更を認識します。

f. 前後の値についてのレポートは、セキュリティとコンプライアンスにどのように役立ちますか。

企業のセキュリティ・ポリシーやHIPAAのような規制によって、機密データに加えられた変更は監査の対象となり、レコードの前後の値を取得しておく必要が生じています。Oracle AVDFはOracle GoldenGate Integrated Extractプロセス（制限付きライセンスが含まれる）を使用して前後の値を取得し、その値をAVDFレポートで分析用に使用できるようにします。詳しくは、Oracle AVDFのAdministrator's GuideおよびAuditor's Guideを参照してください。

g. Oracle AVDFはデータベース・アクティビティ監視（DAM）とSIEMの取組みにどのように役立ちますか。

Oracle AVDFは、ネイティブの監査データ収集とネットワークベースのSQLトラフィック監視の機能を備えるDAMソリューションです。Oracle AVDFはアラート、レポート、監査データのアーカイブをサポートします。
Oracle AVDFでは、SIEMシステムとの統合のために、Syslogにイベントを送信できます。Oracle AVDFのスキーマはオープンで、問合せ可能です。

3 セキュリティ

a. Oracle Database Firewallはターゲットに送信される暗号化されたトラフィックを監視しますか。

Database Firewallは、Oracle Native Network Encryptionが使用されている場合に、Oracle Databaseへのトラフィックや、Oracle Databaseからのトラフィックを監視できます。Oracle以外のデータベースや、TLSネットワーク暗号化を使用するOracle Databaseの場合は、Database FirewallはそのようなSQLトラフィックを解析しません。SSLまたはTLSターミネーションのソリューションを使用すると、Database Firewallに到達する直前にSQLトラフィックを停止させることで、Database FirewallがSQLトラフィックを解析し、ポリシーを適用できるようになります。

b. Oracle AVDFで保存されたデータはどのように保護されますか。

Oracle AVDFは透過的データ暗号化を使用して、収集されたデータを暗号化し、ターゲットからのネットワーク・トラフィックを暗号化します。Oracle AVDFは管理者と監査者の責任を分離し、Database Vaultを使用して、データへのアクセスを制限します。詳しくは、Administrator's Guideの「General Security Guidelines」を参照してください。

c. Oracle AVDFではActive Directoryを使用して認証できますか。

Oracle AVDF 20ではActive Directoryを統合して、ユーザーを認証できます。Oracle AVDFの管理者/監査者をActive Directoryユーザーとして作成することもできます。詳しくは、Administrator's Guideを参照してください。

4. エンタープライズ向け機能

a. 多数のターゲットや、大量の監査/ログ・データによるOracle AVDFのスケーリングはどのように行われますか。

サイジングのガイドに基づいて構成されたAudit Vault Serverは、最大1000の監査証跡について監査およびファイアウォール・イベント・データの収集をサポートし、各エージェントは最大20の監査証跡をサポートします。
サイジングのガイドについては、『Audit Vault and Database Firewall Best Practices and Sizing Calculator』（MOS Note：2092683.1）を参照してください。ご使用の環境に基づいて、Audit Vault Server、Audit Vault Agent、Database Firewallで必要になるCPU、メモリ、ディスクのサイズを設定できます。サイジングのガイドを生成するには、ターゲットの数、1日に生成される平均的な監査データ、保存期間、ファイアウォールのターゲット数などの情報が必要です。

b. Oracle AVDFはOracle Exadataやクラスタ化されたデータベースなどからの高い負荷を処理できますか。

Oracle AVDFをスケーリングして、Oracle Exadataや他のクラスタ化されたデータベースからの監査データ収集をサポートすることができます。ターゲットの合計数と、予想される監査の取込み率に基づいて、エージェント数を構成できます。サイジングのガイドについては、『Audit Vault and Database Firewall Best Practices and Sizing Calculator』（MOS Note：2092683.1）を参照してください。

c. Oracle AVDFはオンプレミスのターゲットだけではなく、クラウドのターゲットもサポートしますか。

オンプレミスのAudit Vault Serverは、Oracle Database Cloud Service（Oracle DBCS）とオンプレミスのデータベース・インスタンスの両方から監査データを収集します。オンプレミス（またはクラウド）のAudit Vaultエージェントは、DBCSのデータベース・インスタンスから監査データを収集します。現在、Audit Vault Serverは従来の監査証跡、ファイングレイン監査、Database Vault監査、Unified Auditのデータを、クラウドまたはオンプレミスのデータベースの監査証跡から収集します。詳しくは、Administrator's Guideの「Oracle Audit Vault And Database Firewall Hybrid Cloud Deployment」の章を参照してください。

d. Oracle AVDFは高可用性をどのようにサポートして、フォルト・トレランスを実現していますか。

Oracle AVDFはAudit Vault ServerとDatabase Firewallで高可用性構成をサポートし、動作停止時にはスタンバイ・サーバーがプライマリ・サーバーになります。詳しくは、Administrator's Guideを参照してください。

e. 規制による保存の要件を満たすために、Oracle AVDFで監査/ログ・データをアーカイブできますか。

Audit Vault Serverは、ターゲット単位でのデータ保存ポリシーをサポートしているため、社内または外部のコンプライアンス要件を満たすことができます。監査データを低コストの外部リポジトリに自動でアーカイブして、ターゲットごとのポリシーに基づいて取得できます。詳しくは、Administrator's Guideを参照してください。

f. Oracle AVDFでは異常なアクティビティについてアラートを発信して、分析の時間を最小限にすることはできますか。

Oracle AVDFには強力なアラート機能が搭載されており、さまざまな条件に基づいて、収集された監査データおよびファイアウォールのデータについてのアラートを構成できます。Oracle AVDFはダッシュボードにアラートを表示させたり、電子メールで送信したり、Syslogに送信したりできます。

g. Oracle AVDFはDatabase VaultやOracle DBSATなどのオラクルのセキュリティ製品とどのように統合されていますか。

Database Security Assessment Tool（DBSAT）の出力（ご使用のスキーマでの機密性の高い列/表のリストを含む）はOracle AVDFにインポートでき、そのような表の監査アクティビティはAVDFレポートで確認できます。
Oracle AVDFはDatabase Vault監査証跡からの監査データを読み取り、AVDFレポートで表示させることができます。

5. デプロイメント

a. Oracle AVDFはどのようなハードウェアやVMで動作しますか。サイズを決定するにはどうしたら良いですか。

Oracle Linux release 7でサポートされている、インテルx86 64ビットのハードウェア・プラットフォームであればどれでも、AVDFコンポーネントをデプロイできます。認定ハードウェアの一覧は、ハードウェア認定リストをご覧ください。Audit Vault ServerとDatabase Firewallは、それぞれ専用のx86 64ビット・サーバーにインストールする必要があります。

サイジングのガイドについては、『Audit Vault and Database Firewall Best Practices and Sizing Calculator』（MOS Note：2092683.1）を参照してください。ご使用の環境に基づいて、Audit Vault Server、Audit Vault Agent、Database Firewallで必要になるCPU、メモリ、ディスクのサイズを設定できます。サイジングのガイドを生成するには、ターゲットの数、1日に生成される平均的な監査データ、保存期間、ファイアウォールのターゲット数などの情報が必要です。

Oracle AVDFはOracle VM ServerやVMwareなどの仮想化環境でも動作しますが、物理ハードウェアへのインストールが推奨されています。

b. Oracle AVDFのインストール/デプロイにはどれほどの時間がかかりますか。コンサルティングを依頼する必要はありますか。

一般的な概念実証に要する期間は2日～2週間ですが、ターゲットやポリシーの数によって異なります。
デプロイメントまでには3つの重要なステップがあります。

1. 任意のサーバー・マシンに、Audit Vault Serverと、オプションでDatabase Firewallをインストールする。ISOイメージを使用したプロセス全体はきわめて簡単なもので、数時間で終えられます。
2. ターゲット上またはDatabase Firewall上で、適切な監査ポリシーまたは監視ポリシーを有効にするか、作成する。Oracle AVDFでは、ユーザーが数回のクリックで非常に簡単にデフォルトのポリシーを作成できるようになっていますが、ユースケースによってはもっと時間がかかる場合もあります。
3. レポートとアラートを分析する。Oracle AVDFには設定不要で使える数十種類のレポートが用意されており、レポートをカスタマイズして、コンプライアンス要件やセキュリティ要件に合わせることができます。

概念実証が終了したら、AVDFコンソールを使用して、バックアップ、アーカイブ、高可用性などを、さらに時間をかけてセットアップするのが一般的です。次に、カスタム・コレクタ・フレームワークを使用して、独自のアプリケーション向けにコレクタを追加することもできます。

オラクルのお客様の多くが、コンサルティング・サービスを利用せずに、Oracle AVDFを実装してきました。

インストールの前に、Installation Guideのデプロイメント・チェックリストを参照し、サイジングのスプレッドシート（MOS Note：2092683.1）を使用して、適切なハードウェア構成を決定してください。

c. Oracle AVDFによってデプロイメントとアップグレードの時間をどのように抑えられますか。

Oracle AVDFはフルスタックのソフトウェア・アプライアンスで、Oracle Linuxオペレーティング・システム、Oracle Database、AVDFソフトウェアが含まれているため、すべてのコンポーネントを一度に、簡単にデプロイおよびアップグレードできます。Audit Vault Serverのアップグレード時には、エージェントが自動でダウンロードおよび更新されるため、デプロイメントとアップグレードの時間を最小限に抑えられます。

6. アップグレード

a. 現在、Oracle AVDF 12.2を使用しています。Oracle AVDF 20にアップグレードするべきでしょうか。

Oracle AVDF 20へのアップグレードを検討するべき理由には、以下のものがあります。

- さまざまなワークフロー向けに最適化されて新たに用意された、最新式のUI。管理者や監査者の生産性向上に役立ちます。
- 統合された監査のサポート。従来の監査から統合された監査への移行を目指すお客様には重要です。
- 以前のリリースと比べて簡単になった、Database Firewall設定の構成。
- PostgreSQL、MongoDBなどの新しいターゲット（シンプルな属性マッピング表を使用）。
- マルチテナントのOracle DB構成をサポートするOracle GoldenGate Integrated Extractプロセス（制限付きライセンスが含まれます）を使用した、変更されたレコードの前後の値の収集。
- AVDFユーザーを一元管理しやすくする、Active Directoryとの統合。

- Audit Vault Serverからの監査/ネットワーク・イベント・データの自動アーカイブ。
- 旧バージョンのOracle AVDFのサポートは2021年3月で終了し、新しい機能はおもにOracle AVDF 20に追加されることになります。そのため、Oracle AVDF 20へのアップグレードを検討することを強くお勧めします。

b. Oracle AVDFのどのバージョンからのアップグレードが可能ですか。

Oracle AVDF 12.2.0.9.0以降のバージョンであれば、Oracle AVDF 20にアップグレードできます。
12.2 BP9より古いバージョンを使っている場合は、まず12.2 BP9にアップグレードしてから、Oracle AVDF 20にアップグレードする必要があります。詳しくは、Installation Guideを参照してください。

c. 現時点で登録済みのターゲット、カスタマイズされたレポート、アーカイブ済みのデータは移行されますか。

アップグレードが済むと、現時点で登録済みのターゲット、カスタマイズされたレポート、アーカイブ済みのデータは、Oracle AVDF 20に自動的に移行されます。

7. 追加情報

a. Oracle AVDFを使用し始めるにはどうしたら良いですか。どのような参考資料がありますか。

Oracle Technology NetworkのWebサイトから、製品の詳しい情報を確認したり、ホワイト・ペーパーやデータシートなどの資料を入手したり、お近くのオラクルの担当者に問い合わせたりできます。

b. AVDFソフトウェアはどこからダウンロードできますか。製品のドキュメントはありますか。

Oracle AVDFは、Oracle Software Delivery Cloudからダウンロードできます。
Oracle Software Delivery Cloudに移動して、製品パックとしてOracle Audit Vault and Database Firewallを検索します。

製品のドキュメントは、こちらで参照できます。

c. 外部にディスカッション・フォーラムはありますか。

はい、Oracle Audit Vault and Database Firewallフォーラムは、製品に関する疑問点をOracleコミュニティの専門家に質問できるプラットフォームです。