ORACLE
Cloud Infrastructure

Oracle Cloud InfrastructureへのOracle Audit Vault and Database Firewallのデプロイ

データベースのセキュリティおよびコンプライアンス監査

ORACLE WHITE PAPER | 2018年4月

ORACLE

免責事項

以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。マテリアルやコード、機能を提供することをコミットメント(確約)するものではないため、購買決定を行う際の判断材料になさらないで下さい。オラクル製品に関して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。

注意: このホワイト・ペーパーはさらに改訂される場合があります。最新版をお持ちであることを確認してください。

目次

Oracle Cloud Infrastructureにおけるデータベースのセキュリティ

Oracle Cloud Infrastructureは、多種多様な高パフォーマンスのOracle Databaseをクラウドで提供しています。セキュリティはクラウドで考慮すべき重要な問題の1つであり、Oracle Cloud Infrastructureデータベースは多くのセキュリティ機能をデフォルトで備えています。Oracle Cloud Infrastructureは、Oracle DatabaseをComputeベア・メタル(BM)インスタンス上で提供します。BMインスタンスは、高度な特権を持つOracle Cloud Infrastructure制御のハイパーバイザによって管理されないため、お客様にとって最大限のセキュリティ分離が実現します。Oracle Cloud Infrastructureは仮想マシン(VM)ベースのデータベースも提供します。VMベースのデータベースには、仮想化セキュリティの最新セキュリティ・プラクティスが採用されています。

データベース・オプション

Oracle Cloud Infrastructure Databaseサービス(DBaaS)には、次のデータベース・オプションが用意されています。

- **ベア・メタル(BM)データベース・インスタンス:** 柔軟性に優れたオンデマンドのOracle DatabaseをBMインスタンス上でNVMeローカル・フラッシュ・ストレージとともに、1ノードおよび2ノードのRAC構成で提供します。2ノードのRACは、自動フェイルオーバー機能を持つ共有ストレージを使用しています。BMデータベース・インスタンスには次のような各種シェイプがあります。
    - **1ノードのHighIO:** 36コア、512GBのRAM、12.8TBのNVMeストレージ
    - **1ノードのDenseIO:** 36コア、512GBのRAM、28.8TBのNVMeストレージ
    - **2ノードのRAC:** 1ノード当たり36コア(合計72コア)、512GBのメモリー、24TB(1.2TBのSSDドライブ×20)の直接接続共有ストレージを備えた、2つのBMインスタンス
- **仮想マシン(VM)データベース・インスタンス:** 1ノードおよび2ノードのVM上のOracle Database。各VMノードは1コア、2コア、4コア、8コアまたは16コアで構成可能です。2ノードのVMはRAC構成になります。
- **Exadataデータベース:** 低レイテンシのInfiniBandネットワークで接続されたコンピュート・ノードとストレージ・ノードからなる、フル・ラック、ハーフ・ラックまたはクォータ・ラックのExadata X6システム。最適化されたOracle Databaseソフトウェアを搭載しています。
- **顧客管理データベース:** お客様がOracle DatabaseをBMインスタンスにインストールして管理することができます。大半のお客様が前述のインスタンスを使用されますが、万全を期すためにこのオプションも提供しています。

Oracle Cloud Infrastructure DBaaSインスタンスは、Oracle Databaseリリース11.2、12.1および12.2に加えて、バックアップとリストア、パッチ適用、Oracle Data Guardなど、広く利用され

ている管理機能をサポートしています。Oracle Databaseの無制限ライセンス契約または非制限ライセンス契約を締結しているお客様は、クラウドのOracle Cloud Infrastructure DBaaSインスタンスでご自身のライセンスを使用できます。

サポートされているセキュリティ機能

ミッションクリティカルなお客様のデータベースに高度なセキュリティを提供するために、Oracle Cloud Infrastructure DBaaSインスタンスは様々なセキュリティ機能をデフォルトでサポートしています。

- **デフォルトのデータベース暗号化:** Oracle Cloud Infrastructureデータベースでは、Transparent Data Encryption (TDE)がデフォルトで有効になっています。TDEにより、表領域全体または特定の表の列が、データベースにネイティブに格納されているデータベース暗号化キーで暗号化されます。データベース暗号化キーのラップ(暗号化)にはTDEマスター・キーが使用されます。TDEマスター・キーは、ローカル・ファイルシステムのOracle Walletに格納されるか、クラスタ・アクセス用にAutomatic Storage Management (ASM)ディスク・グループに格納されます。Oracle Key Vaultを使用するか、TDEマスター・キーをハードウェア・セキュリティ・モジュール(HSM)に格納することにより、TDEマスター・キーを管理するためのオプションがあります。
- **多層防御セキュリティ分離:** Oracle Cloud Infrastructureデータベース・インスタンスは、お客様の仮想クラウド・ネットワーク(VCN)で起動されます。これにより、インスタンスのネットワーク・セキュリティ分離が実現します。たとえば、データベース・インスタンスをVCNプライベート・サブネットで起動することで、データベースへの外部アクセスをすべて防止できます。加えて、BMインスタンスでは、お客様のデータベース上のデータとTDEマスター・キーの格納に関して、さらなるセキュリティ分離を提供します。Oracle Cloud Infrastructureデータベース・インスタンスで実行されているデータベース・エージェントがインスタンスのプロビジョニングと管理を担当しますが、Oracle Cloud InfrastructureのオペレータはBMインスタンスにアクセスできません。
- **ネットワーク・アクセス制御:** VCNセキュリティ・リストを使用することで、Oracle Cloud Infrastructureデータベース・インスタンスへのアクセスが、お客様が構成したIPアドレスから行われた場合にのみ許可するようにネットワーク・ファイアウォールを構成できます。
- **IAM認証および認可:** Oracle Cloud Infrastructure IAMを使用すると、Oracle Cloud InfrastructureデータベースをIAMコンパートメント内でインスタンス化して、認可されたユーザーおよびグループにデータベース・インスタンスへの認証済アクセス権を持たせることができます。
- **自動セキュア・バックアップ:** Oracle Cloud Infrastructureデータベースには、データベース・データの暗号化された自動バックアップがあります。このバックアップは、お客様のObject Storageバケットに格納されます。

- **API監査ログ:** お客様のOracle Cloud Infrastructureデータベースのプロビジョニング、停止および構成のために行われたすべてのAPIコールが、セキュリティおよびコンプライアンス監査用にお客様に提供されます。

データベース監査

セキュリティとコンプライアンスには、データベース監査が不可欠です。データベース監査では、どのデータベース・オブジェクトがアクセスまたは変更されたか、どのデータベース・アカウントがアクションを実行したか、いつアクションが実行されたかなどの情報を含めることで、すべてのデータベース・アクセスを監査ログに記録します。データベース監査ログは、セキュリティ・チームが、セキュリティ上重要な特定のイベントが発生したときに通知をトリガーするセキュリティ・アラートを作成したり、潜在的セキュリティ・インシデント(侵入、データ完全性攻撃、データ損失など)を調べる科学捜査の一環として根本原因分析を実行したりするために使用されます。従業員や特権を持つユーザーが、内部関係者による攻撃を検知するためにデータベース・アクセスをモニタリングする機能は、お客様にとってますます重要になっています。

セキュリティ要件に加えて、医療保険の相互運用性と説明責任に関する法律(HIPAA)、新しい欧州連合一般データ保護規則(EU GDPR)、サーベンス・オクスリー法(SOX)といったコンプライアンス規制により、企業はデータベース・アクセスについて行レベルまで詳細に記載されたレポートを提出するよう求められています。

Oracle Audit Vault and Database Firewall (Oracle AVDF)は、データベース(Oracleその他)の監査とモニタリングのための包括的なセキュリティ・ソリューションを、他の関連するホストレベルのログ(OSやネットワークなど)とともに提供します。このホワイト・ペーパーでは、Oracle Cloud Infrastructure DBaaSインスタンスへのアクセスの監査にOracle Audit Vault Serverを使用する方法に焦点を当てます。

注意: このホワイト・ペーパーでは、*Oracle AVDF*はAudit Vault Server機能のみを指します。Database Firewallはこのホワイト・ペーパーの対象とせず、別途扱う予定です。

オンプレミスのOracle AVDFデプロイメントでは、クラウド・データベースとオンプレミス・データベースの両方から監査データを収集できます。このホワイト・ペーパーの目的は、Oracle AVDFを自社のVCN内のBMインスタンスにインストールして構成し、Oracle Cloud Infrastructure DBaaSインスタンスの監査とモニタリングを行うお客様向けに、手順を説明することです。

Oracle Databaseの監査とOracle AVDFの概要

Oracle AVDFは、データベース・アクセス・イベントのモニタリングとアラート送信のためのセキュリティ・ソリューションを提供します。Audit Vaultは、OracleとOracle以外のデータベース

の監査証跡、ネットワーク・ログ、アプリケーション・ログなどの各種ログを取り込んで、統一的なセキュリティ監査およびモニタリング・ソリューションを提供します。ただし、Oracle AVDFを使用するには、Oracle Databaseで監査証跡を有効にするという基本的な前提条件があります。この項では、Oracle Databaseの監査とOracle AVDFの概要を示します。

Oracle Databaseの監査機能

Oracle Databaseには、各種データベース・アクセス・イベントを監査証跡に記録するための包括的なロギング機能セットが用意されています。監査証跡は、SYSTEM表領域のSYS.AUD$表とSYS.FGA_LOG$表に書き込まれます。
Oracle Databaseの監査ログ・オプションは次のとおりです。

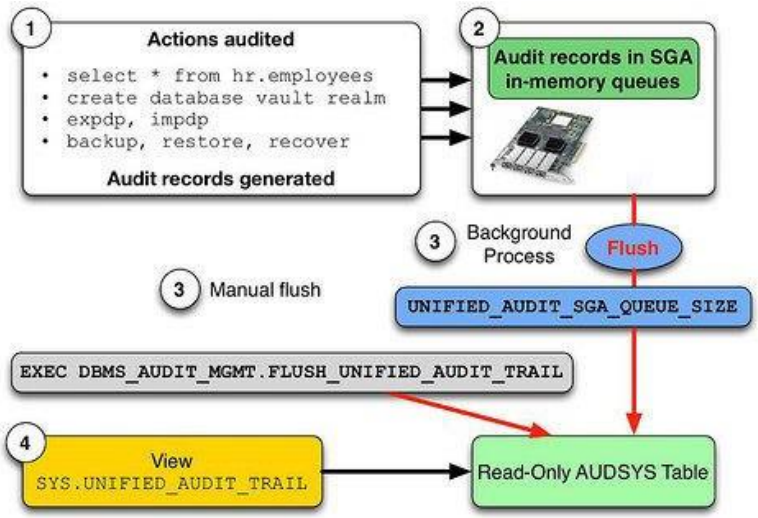
- **必須の監査:** データベース起動、データベース停止、SYSDBAおよびSYSOPERのログインなど、特定のイベントが自動的に記録されます。この監査は必須であり、オフにすることはできません。データベースの起動および停止の場合、監査ログにはデータ、タイムスタンプ、ユーザーおよびユーザー端末情報が含まれます。
- **標準監査:** ユーザーがAUDIT文を使用して、スキーマ・オブジェクトに対する各種アクセスを監査できます。監査ログは、AUDIT_TRAILパラメータの値に応じて、SYS.AUD$表またはOSのsyslogに書き込まれます。AUDIT文は、BY ACCESS (監査対象文ごとに監査レコードを挿入)、BY SESSION (監査対象文を含むセッションについて監査レコードを1つ挿入)、WHENEVER SUCCESSFUL (ユーザー・アクションが成功したときに監査レコードを挿入)、WHENEVER NOT SUCCESSFUL (ユーザー・アクションが失敗したときに監査レコードを挿入)などの識別子を使用して変更できます。次のタイプのイベントが監査されます。
    - **SQL文の監査:** スキーマ・オブジェクトまたはデータベース構造に関連するDML文とDDL文を監査します。ただし、名前付きオブジェクトは対象外です。たとえば、ユーザーBOBによって正常に実行されたすべての文を監査するには、AUDIT ALL STATEMENTS BY bob BY ACCESS WHENEVER SUCCESSFULを使用します。監査対象をbobによる特定の表アクションに制限する場合は、AUDIT SELECT TABLE, INSERT TABLE, DELETE TABLE BY bob BY ACCESSを使用します。
    - **特権の監査:** システム権限の使用を監査します。この監査は、ユーザー・アクションにシステム権限が必要な場合にのみトリガーされます。たとえば、ユーザーBOBにSELECT ANY TABLE権限が付与されており、この権限を監査するとします。ユーザーBOBが自分のスキーマ(BOB.EMPLOYEES)の表を選択した場合、SELECT ANY TABLE権限が使用されないため、監査の対象にはなりません。一方、BOBが別のスキーマ(HR.EMPLOYEESなど)の表を選択した場合は、監査レコードが生成されます。一連の権限(CREATE USER、DROP USER、ALTER USERなど)がデフォルトで監査されます。
    - **スキーマ・オブジェクトの監査:** 表、ビュー、ストアド・プロシージャ、ファンクション、パッケージなど、監査対象のスキーマ・オブジェクトに対するすべてのユーザーのアクションを監査します。たとえば、AUDIT SELECT on BOB.EMPLOYEESを使用すると、BOB.EMPLOYEESオブジェクトに対するすべて

のユーザーのSELECT操作について監査レコードが作成されます。

- **ネットワークの監査:** AUDIT NETWORKを使用して、ネットワーク・レイヤーのエラーを監査します。

- **ファイングレイン監査(FGA):** ファイングレイン監査を使用すると、監査が実行されるための特定の条件を定義したポリシーを作成できます。このタイプの監査では、コンテンツに基づいてデータ・アクセスをモニタリングできます。問合せとINSERT、UPDATEおよびDELETE操作のきめ細かな監査が可能です。

Oracle 12cでは、すべての監査証跡(SYS.AUD$、SYS.FGA_LOG$、DVSYS.AUDIT_TRAIL$など)が単一のビューSYS.UNIFIED_AUDIT_TRAILに統合されています。そのため、Oracle AVDFなどの監査ツールは監査データ全体を1つの場所で分析できるので、データを1つの場所に集める必要がなくなりました。統合監査データの格納には、新しいスキーマAUDSYSが使用されます。次の図は、Oracle 12cの統合監査による処理の概要を示しています。



Oracle 12cでの統合監査

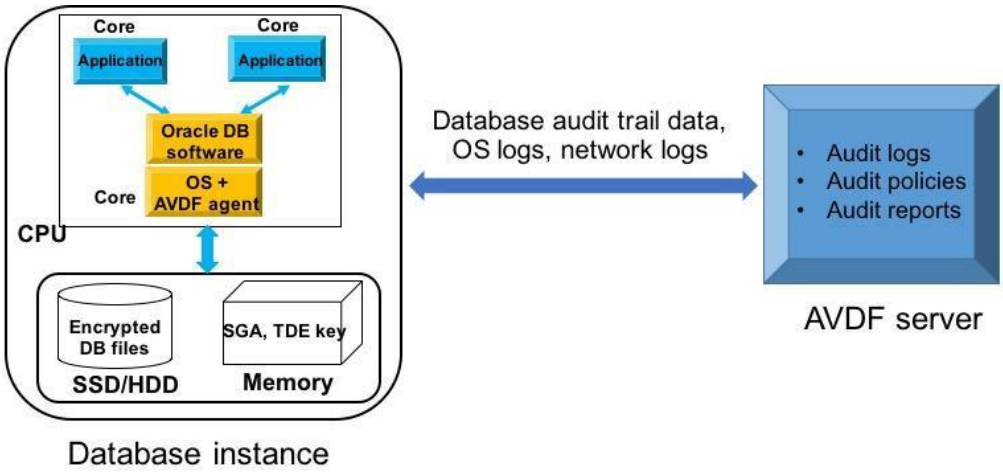
職務分掌を強化するために、2つの新しいデータベース・ロールを監査で使用できます。データベース監査の管理用のAUDIT_ADMINと、監査証跡の表示専用のAUDIT_VIEWERです。Oracle 12cの統合監査の詳細は、http://www.oracle.com/webfolder/technetwork/tutorials/obe/db/12c/r1/security/sec_uni_audit/sec_uni_audit.htmlに記載されています。

Audit Vault and Database Firewallセキュリティ・アプライアンス

Oracle AVDFでは、データベース・インスタンスで実行されているエージェントを利用します。このエージェントがデータベース監査証跡レコードをAudit Vault Serverに送信します。Audit Vault Serverは、物理ホストまたはVM上で動作するよう設計されたセキュリティ・アプライアン

スであると同時に、ログ集約、モニタリングおよびアラート送信のための一元的リソースでもあります。Audit Vault Serverの管理は、Webコンソールを使用して行います。Oracle AVDFには主に2種類のユーザーがいます。データベースと監査ポリシーの構成が可能な*管理者*と、Oracle AVDFの管理と監査レコードの表示が可能な*監査者*です。

次の図は、データベース・インスタンスで実行され、すべての監査データをAudit Vault Serverに送信する、Audit Vault Agentを示しています。Audit Vault Serverは、複数のデータベース・インスタンスからの監査データを集約できます。



データベース・インスタンス上のAudit Vault AgentとAudit Vault Server

集約された監査データを基に、Audit Vault Serverは、アクティビティ・レポートやコンプライアンス・レポートをはじめとする各種監査レポートを生成します。アクティビティ・レポートには、ログインの失敗、データベース・スキーマの変更、SQL文などのイベントが列挙されます。PCI-DSS、HIPAA、SOXなどのコンプライアンス規制に対応した標準の監査評価レポートが用意されています。認可されたセキュリティ監査者は、Oracle AVDF Webコンソールからこうしたレポートのすべてにアクセスできます。

Oracle Cloud Infrastructure BMインスタンスへのOracle AVDFのインストール

Oracle AVDFは、オンプレミスの物理ホストにインストールするように設計されたセキュリティ・アプライアンスです。この物理ホストは、モニタリング対象のすべてのデータベースにネットワーク経由でアクセスできる必要があります。このデプロイメント機能により、現在のバージョンのOracle AVDFをBMインスタンスまたはVMインスタンスにそのままインストールすることはできません。Oracle AVDFをOracle Cloud Infrastructureにデプロイするには、次の2つのオプションがあります。

- Oracle Cloud Infrastructureインスタンスへのインストール用にカスタマイズされた

Oracle AVDFブート・イメージを使用する

- Oracle Cloud Infrastructure BMインスタンスで、お客様のBYOH (bring-your-own hypervisor)上のVMとしてOracle AVDFを実行する

Oracle AVDFの機能と堅牢性の点では、BYOHソリューションはOracle AVDFをBMインスタンスでネイティブに実行するのと変わりません(ただし、ハイパーバイザ管理のオーバーヘッドが発生します)。このホワイト・ペーパーでは、BYOHオプションについて説明します。

BYOHモデルでは、お客様はOracle Cloud Infrastructure BMインスタンスにハイパーバイザをインストールして管理し、Oracle AVDFをハイパーバイザ上のVMとして実行することができます。この場合、お客様はハイパーバイザの管理者であり、BMインスタンスとそこで実行されているOracle AVDF VMを完全に制御できます。このホワイト・ペーパーでは、お客様のBYOHとしてKVMハイパーバイザを使用します。KVMは堅牢でセキュア、かつ高パフォーマンスのハイパーバイザであり、いくつかのLinuxディストリビューションで利用できます。複数のパブリック・クラウドをはじめとする多くの本番環境にデプロイされています。

この項では、Oracle AVDFのイメージとライセンスの取得、ハイパーバイザのインストール、およびOracle Cloud Infrastructure BMインスタンスへのOracle AVDF VMのインストールについて説明します。

Oracle AVDFのイメージとライセンスを取得する

ダウンロード手順に従って、インストール用のOracle AVDF ISOイメージをダウンロードします(最新バージョンを使用)。インストール・タスクと管理タスクについては、ドキュメントを参照してください。

Oracle AVDFは、Oracle Databaseセキュリティ製品ポートフォリオ内の個別ライセンス製品です。本番環境と非本番(テストおよび開発)環境のすべてに必要なライセンスを入手してください。

Oracle AVDF VMを実行するためのBYOH KVMをインストールする

BYOHの場合、最も重要な機能はVCNのセカンダリVNICです。セカンダリVNICを使用すると、追加のVNICをBMインスタンスにアタッチし、VCNルーティング可能なIPアドレスをVNICに割り当てて、BYOH BMインスタンスで実行されているVMにVNICをアタッチすることができます。セカンダリVNICの詳細は、Networkingサービスのドキュメントを参照してください。

この項では、万全を期すためにBYOH KVMの大まかなインストール手順を示します。詳しい手順については、対応する『Installing and Configuring KVM on Bare Metal Instances with Multi-VNIC』ホワイト・ペーパーを参照してください。大まかな手順は次のとおりです。

1. Oracle Linux 7.xイメージを使用してBMインスタンスを起動します。

2. SSHキーを使用してBMインスタンスにログインし、接続をテストします。接続できない場合は、VCNセキュリティ・リストとインスタンスのファイアウォール・ルールを確認してください。VNCクライアントを使用してBMインスタンスに接続できるように、BMインスタンスにVNCサーバーをインストールすることをお薦めします。Oracle Linux上でVNCサーバーを構成する手順は、https://docs.oracle.com/cd/E52668_01/E54669/html/ol7-vnc-config.htmlに記載されています。

3. Oracle Cloud Infrastructureコンソールで、256GB以上のブロック・ストレージ・ボリュームを作成し、それをBMインスタンスにアタッチします。アタッチしたボリュームにファイルシステムをマウントし、マウントしたファイルシステムにOracle AVDF ISOをコピーします。格納する監査レコードの数によっては、1TBのブロック・ボリュームを使用することをお薦めします。

4. コンソールまたはAPIを使用してセカンダリVNICをアタッチし、セカンダリ・インタフェースのIPアドレス、MACアドレスおよびVLANタグを書き留めます。これはOracle AVDF VMに割り当てるセカンダリIPアドレスであるため、Oracle Cloud Infrastructure DBaaSインスタンスをはじめとする他のVCNホストからネットワーク経由でアクセス可能です。

```
sudo yum install qemu-kvm qemu-img virt-manager libvirt libvirt-python
libvirt-client virt-install virt-viewer bridge-utils
```

5. KVMハイパーバイザをBMインスタンスにインストールします。

6. SR-IOVを有効にして、BMインスタンスを再起動します。詳細は付録を参照してください。

7. BMインスタンスが起動したら、OSでSR-IOV仮想機能(VF)を有効にします。VFを選択し、上で作成したセカンダリVNICのMACアドレスでVFを構成します。詳細は付録を参照してください。

8. セカンダリVNICのVLANタグを使用して、ネットワーク・インタフェースを作成します。このインタフェースは、前のステップで構成したVFでブリッジされます。詳細は付録を参照してください。

9. BMインスタンスで`pifconfig`を実行し、作成されたネットワーク・デバイスを表示します。

BMインスタンスにOracle AVDF VMをインストールする

これで、BMインスタンスがKVMハイパーバイザで実行されるようになりました。また、VCNルーティング可能なIPアドレスを持つセカンダリVNICがOracle AVDF VMに割り当てられます。次の手順に従ってOracle AVDF VMをインストールします。

1. `qemu-img`を使用して500G以上の仮想ディスクを作成します。この仮想ディスクはOracle AVDF VMによって使用されます。

   ```
   qemu-img create -f raw <path_to_disk_image> 500G
   ```

2. `virt-install`を使用してOracle AVDF VMをインストールします。

   ```
   sudo virt-install --arch=x86_64 --name=<AVDF_VM_name> --ram 16000 --cpu
   Haswell-noTSX --vcpus=4 --hvm --video qxl --nonetwork --os-type linux --
   noautoconsole --boot hd,cdrom -disk
   <path_to_AVDF_ISO>,device=cdrom,bus=ide -disk
   <path_to_AVDF_VM_disk_image>,format=raw,bus=scsi --graphics
   vnc,port=<VNC_port>,listen=0.0.0.0,password=<VNC_password>
   ```

   前述のコマンドにより、ブート・ログを確認するためのOracle AVDF VMコンソールへのVNC接続も作成されます。

3. localhostにSSHトンネルを作成し、VNCクライアントを使用してOracle AVDF VMコンソールに接続します。これは、インストール中にエラーが発生した場合に特に便利です。

   ```
   ssh -i <BM_SSH_key> -L <VNC_port>:localhost:<VNC_port> opc@<BM_host_IP>
   ```

   `<BM_SSH_key>`はBMインスタンスに接続するためのSSHキー、`<VNC_port>`はステップ2で`virt-install`に指定したポート番号、`<BM_host_IP>`はBMインスタンスのIPアドレスです。

   Macでは、ネイティブVNCクライアント(画面共有)を使用してOracle AVDF VMコンソールに接続できます。その際、ステップ2で構成した`vnc://opc@localhost:<VNC_port>`および`<VNC_password>`を使用します。

4. `virsh`を使用して、VNICネットワーク・インタフェース(前の項で作成したもの)をアタッチします。正しいVNIC MACアドレスとネットワーク・デバイス名を`attach.xml`ファイルに入力する必要があります(このファイルの詳細は、付録を参照してください)。VNICネットワーク・インタフェースをアタッチした後、Oracle AVDF VMを削除して再起動します。

```
sudo virsh attach-device <AVDF_VM_name> ./attach.xml –config

sudo virsh destroy <AVDF_VM_name>

sudo virsh start <AVDF_VM_name>
```

VMのインストールが開始されると、VMにアタッチしたVNICネットワーク・デバイスが検出されます。VMのインストールには約30分かかります。Oracle AVDFのインストールの詳細は、https://docs.oracle.com/cd/E37100_01/doc.121/e27778/install.htm#SIGIG177に記載されています。

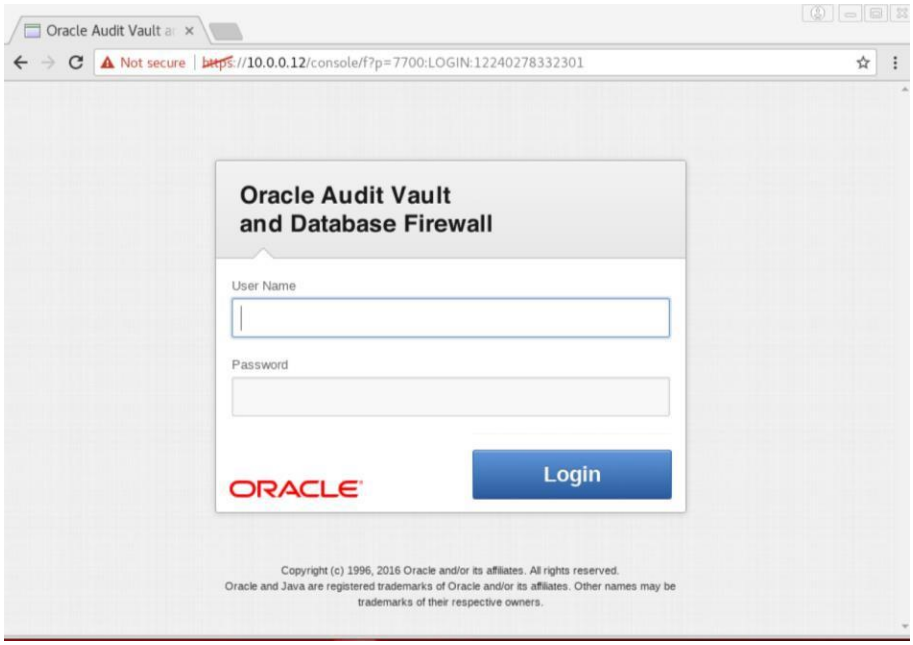
インストール中、次の情報の入力を求められます。

- **Oracle AVDFインストール・パスフレーズ:** このパスフレーズは、Oracle AVDF Webコンソールへの初期ログインに使用されます。
- **Oracle AVDFネットワーク構成:** これには、Oracle AVDF VMのIPアドレス、ゲートウェイIPアドレスおよびネットマスクが含まれます。セカンダリIPアドレス(アタッチしたVNICのもの)をOracle AVDF VMのIPアドレス(AVDF_VM_IP)として指定します。10.0.0.1をゲートウェイIPアドレスとして、255.255.255.0をネットマスクとして指定します。

5. インストールが完了したら、ホストBMインスタンスでWebブラウザを開き、`https://AVDF_VM_IP`と入力します。ここで、`AVDF_VM_IP`はOracle AVDF VMに割り当てられたIPアドレスです。
   ブラウザでOracle AVDFコンソールが開きます。

6. インストール・パスフレーズを使用してログインします。

7. 入力要求が表示されたら、管理者および監査マネージャのユーザー名とパスワードを設定します。次に入力要求が表示されたら、ルート・パスワード(VMでのルート権限)とサポート・パスワード(VMへのSSHアクセス用)も設定します。また、NTPを使用してAudit Vault ServerとDBaaSインスタンスの時間を構成し、時間の同期が取れた状態を維持します。Audit Vault ServerとDBaaSインスタンスの間で時間の同期が取れていないと、データベース監査証跡の収集に悪影響を及ぼします。
   BMインスタンスでグラフィカルなOracle AVDF Webコンソールを開くには、BMインスタンスへのVNC接続を介したBMインスタンスへのX Window接続、またはX Windowを有効にしたSSHが必要です。次の図は、BYOH BMインスタンスで実行されているOracle AVDF VMのOracle AVDF管理者コンソール(IPアドレスは10.0.0.12)を示しています。



8. VCNセキュリティ・リストを構成し、監査対象のDBaaSインスタンスからAudit Vault Serverにアクセスできるようにします。ICMP pingを使用して、Audit Vault ServerとDBaaSインスタンスの間のネットワーク接続を確認します。ここまでのステップをすべて正しく実行していれば、Audit Vault ServerとDBaaSインスタンスは相互にアクセスできるはずです。

Oracle AVDFを使用したDBaaSインスタンスの構成

この項では、DBaaSインスタンスにAudit Vault Agentをデプロイして Audit Vault Serverでデータベース監査証跡を収集する手順を示します。この手順は、Oracle AVDFを使用してDBaaSインスタンスの監査を始めるためのものであり、あらゆる情報を網羅することは意図していません。構成オプションの詳細は、包括的なOracle AVDFドキュメントを参照してください。

DBaaSインスタンスにAudit Vault Agentをインストールする

1. Oracle AVDFコンソールに管理者としてログインします。

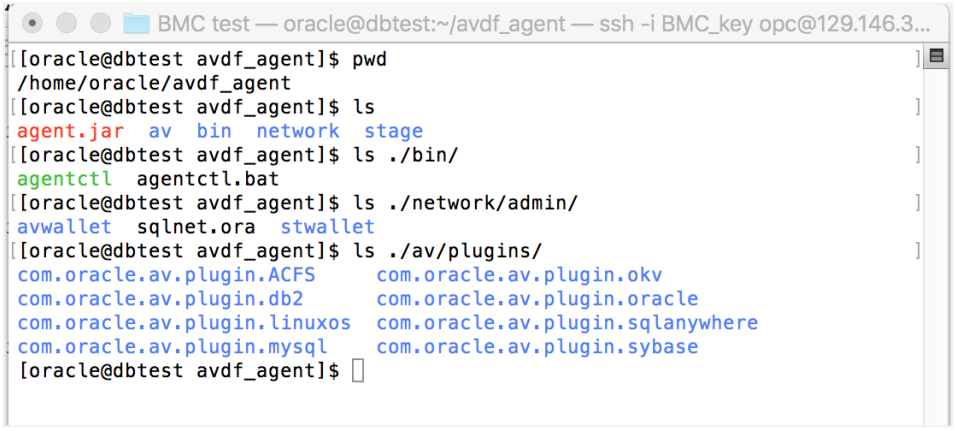
2. **「ホスト」**タブで、**「エージェント」**をクリックして`agent.jar`ファイルをダウンロードします。

3. `agent.jar`ファイルをDBaaSインスタンスにコピーします。

4. $AVDF_AGENT_HOMEを、Audit Vault Agentがインストールされるディレクトリとして設定します。次のコマンドにより、$AVDF_AGENT_HOMEディレクトリが作成され、エージェントがインストールされます。

```
java -jar agent.jar -d $AVDF_AGENT_HOME
```

次の図は、DBaaSインスタンス(dbtest)上の$AVDF_AGENT_HOME(/home/oracle/avdf_agent)とサブディレクトリ内の各種ファイルを示しています。/bin/agentctlはエージェントを有効にするスクリプトです。



Audit Vault ServerにDBaaSインスタンスを登録する

1. 次のコマンドを実行して、データベース監査証跡がDBaaSインスタンスで有効になっていることを確認します。

```
show parameter audit
```

AUDIT_TRAILパラメータには値DBが必要です。AUDIT_TRAILがNONEに設定されている場合、次の手順を実行します。

   A. データベースにSYSとして接続します。

   B. 次のコマンドを使用して監査証跡を有効にします。

```
ALTER SYSTEM SET AUDIT_TRAIL=DB
```

   C. データベースを停止して再起動することで、監査証跡をアクティブにします。

2. Oracle AVDFでは、データベースから監査データを収集する権限と監査ポリシーを管理する権限が必要になるため、ユーザー(adituser)を適切な権限付きで作成する必要があ

ります。Oracle AVDFには、auditeuserを適切な権限で構成するためのPL/SQLスクリプト(oracle_user_setup.sql)が用意されています。このスクリプトは$AVDF_AGENT_HOME/av/plugins/com.oracle.av.plugin.oracle/configにあります。

DBaaSインスタンスのSQLプロンプトで次のコマンドを実行し、auditeuserユーザーを適切な権限付きで作成します。

```
CREATE USER audituser IDENTIFIED BY<password>
```

<password>は、auditeuserの強力なパスワードです。

```
CONNECT SYS / AS SYSDBA

@oracle_user_setup.sql audituser SETUP
```

3. Oracle AVDFコンソールに管理者としてログインします。

4. **「ホスト」**タブで**「登録」**をクリックします。

5. **「ホスト名」**フィールドにDBaaSインスタンス名(DB_NAME)を入力し、**「ホストIP」**フィールドにIPアドレス(DB_IP)を入力します。

6. **「保存」**をクリックします。
一意のアクティブ化キーが生成されます。アクティブ化キーをコピーします。これは、次の項でAudit Vault Agentをインストールする際に使用します。DB_NAMEは、DBaaSインスタンスで実行されているデータベースのORACLE_SIDとは関連がないため、意味のある任意の文字列を指定できます。

DBaaSインスタンスでAudit Vault Agentを起動する

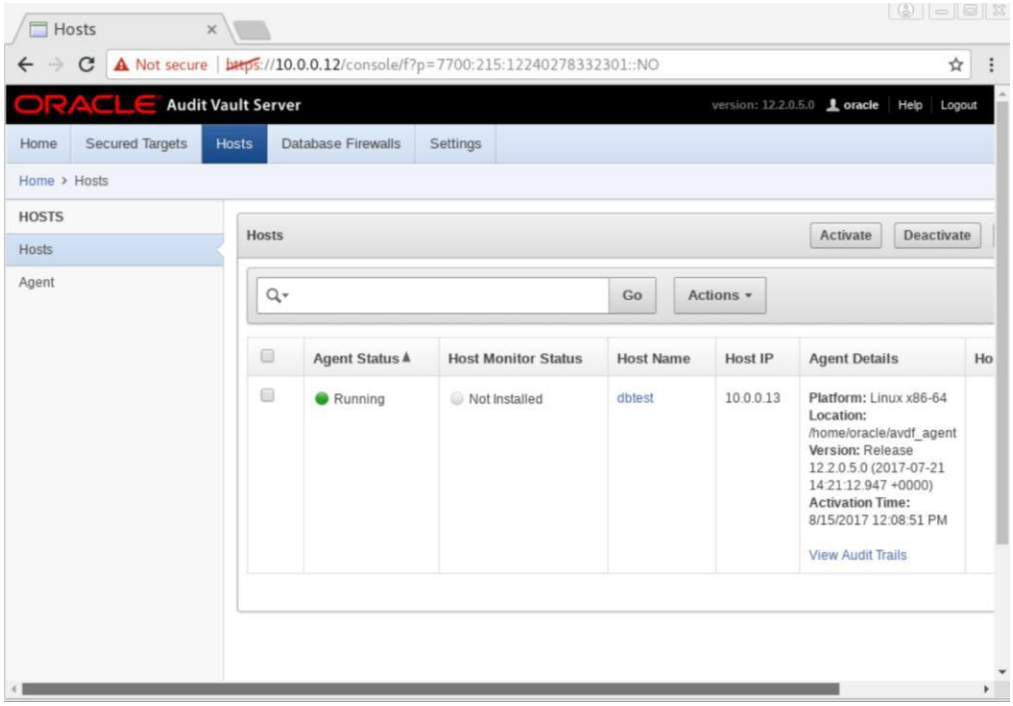
1. DBaaSインスタンスで、$AVDF_AGENT_HOMEディレクトリに移動し、次のコマンドを実行します。

```
./agentctl start -k
```

2. エージェント・アクティブ化キーの入力を求められたら、Oracle AVDFコンソールからコピーしたアクティブ化キーを入力します。アクティブ化キーは、コンソールに管理者としてログインしたときに「ホスト」タブに表示されます。

3. Audit Vault Agentが正常にアクティブ化され、実行されていることを確認するには、(管

理者としてログインした後に) Oracle AVDFコンソールの**「ホスト」**タブで**エージェント・ステータス**をチェックします。ステータスは、緑色の丸が付いた**「実行中」**になっているはずです。
また、`DB_NAME`と`DB_IP`の値が**「ホスト名」**列と**「ホストIP」**列に表示されているはずです。次の図は、エージェントのステータス、DBaaSのホスト名(dbtest)およびIPアドレス(10.0.0.13)を示しています。



DBaaSインスタンス・データベースをOracle AVDFのセキュア・ターゲットとして構成する

1. DBaaSインスタンスで、`$ORACLE_HOME/network/admin/tnsnames.ora`ファイルに移動し、`SERVICE_NAME`パラメータの値をコピーします。

2. Oracle AVDFコンソールに管理者としてログインします。

3. **「セキュア・ターゲット」**タブで**「登録」**をクリックします。

4. 次の値をフィールドに入力して**「保存」**をクリックします。

   - **新しいセキュア・ターゲット名:** ORACLE_SID (監査対象のDBaaSインスタンス・データベースのSID)

- **セキュア・ターゲット・タイプ:** Oracle Database
- **ホスト名/IPアドレス:** DB_IP
- **プロトコル:** TCP
- **ポート:** 1521
- **サービス名:** ステップ1の`SERVICE_NAME`パラメータの値
- **ユーザー名:** `audituser`
- **パスワード:** <audituser_password> (前のステップでaudituser用に作成したパスワード)

注意: NTPサーバーを使用して、Audit Vault Serverとセキュア・ターゲット(この場合はDBaaSインスタンス)の時間の同期を取ることが重要です。時間の同期が取れていないと、監査証跡の収集に悪影響を及ぼします。

Oracle AVDFで監査証跡を構成する

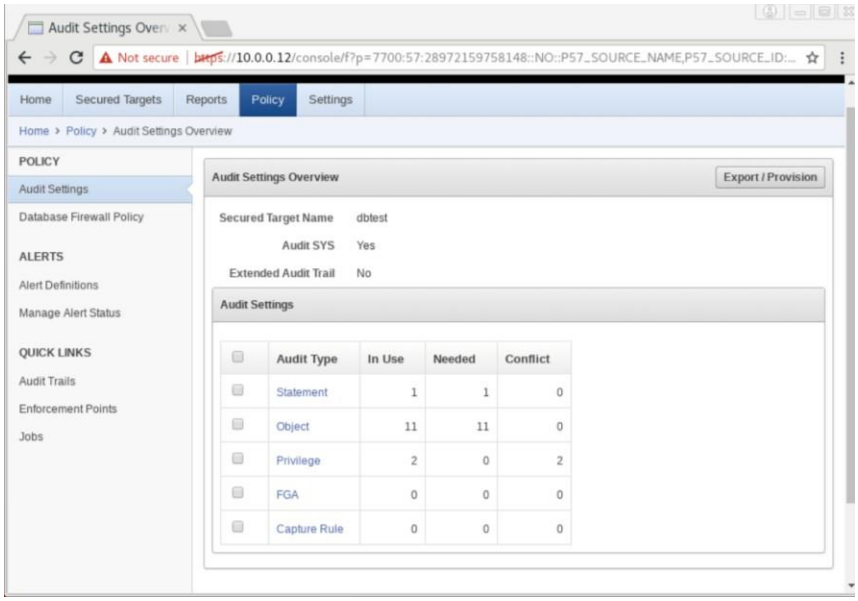
1. Oracle AVDFコンソールに管理者としてログインします。
2. **「セキュア・ターゲット」**タブで、左ペインの**「モニタリング」**の下にある**「監査証跡」**をクリックし、**「追加」**をクリックします。
3. 次の値をフィールドに入力して**「保存」**をクリックします。
   - **監査証跡のタイプ:** TABLE
   - **収集ホスト:** DB_NAME
   - **セキュア・ターゲット:** ORACLE_SID (セキュア・ターゲットの構成中に指定したもの)
   - **証跡の場所:** sys.aud$

データベース監査ポリシーをプロビジョニングする

Audit Vault Serverからデータベースに監査ポリシーをプロビジョニングできます。新しいポリシーのプロビジョニングや既存のポリシーの変更を行うには、監査者ユーザー権限が必要です。

1. Oracle AVDFコンソールに監査者としてログインします。

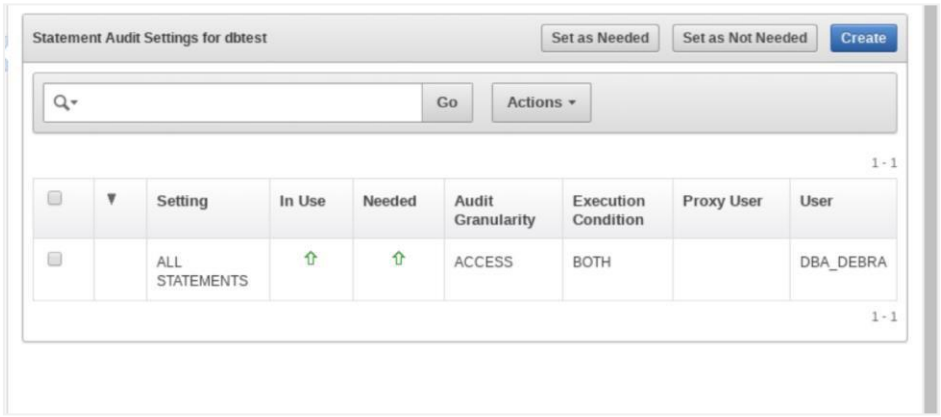
2. **「ポリシー」**タブで、ポリシーを作成するセキュア・ターゲットを選択します。コンソールにはすべての監査ポリシーが表示されます。次の図は、dbtestセキュア・ターゲットの監査ポリシーを示しています。



注意: 次の手順は文監査ポリシーを追加する例を示していますが、この手順は一般的なものであり、どのような監査ポリシーにも利用可能です。

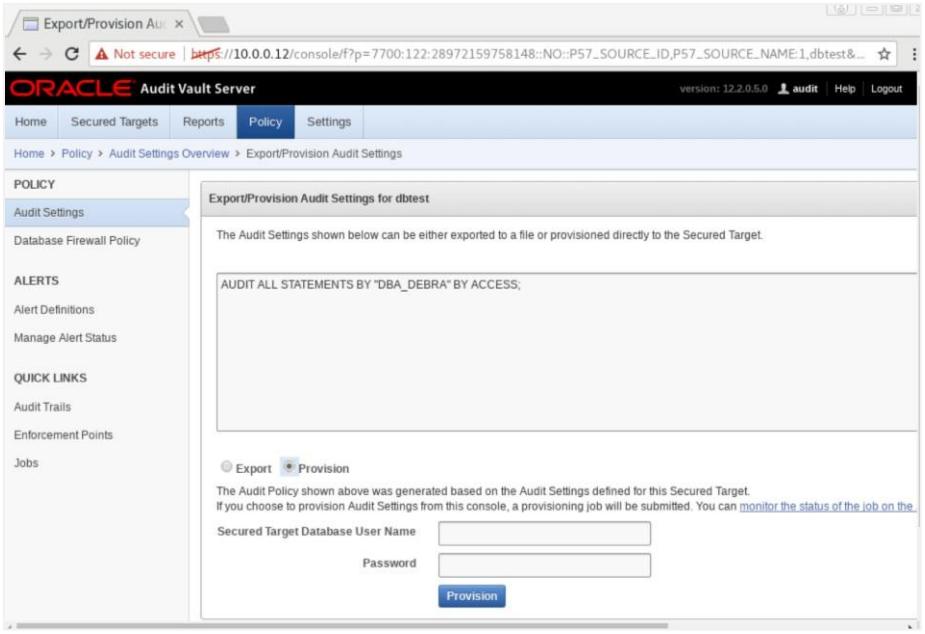
3. 文の監査ポリシーを追加するには、**「監査タイプ」**列で**「文」**をクリックし、**「作成」**をクリックします。監査ポリシーを定義します。

次の図は、セキュア・ターゲットdbtestのサンプル監査ポリシーAUDIT ALL STATEMENTS BY DBA_DEBRA BY ACCESSを示しています。



4. **「セキュア・ターゲット」**ペインに移動し、**「文」**を選択して**「プロビジョニング」**をクリックします。

5. **「プロビジョニング」**オプションを選択して、セキュア・ターゲットの**データベース・ユーザー名**(audituser)と**パスワード**(<audituser_password>)を指定します。次に**「プロビジョニング」**をクリックします。

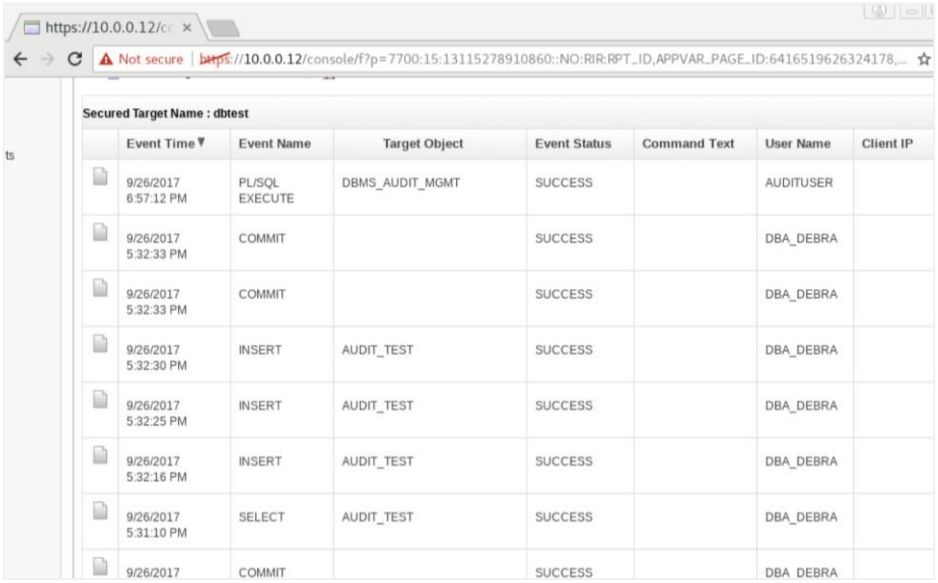


Oracle AVDFでデータベース・アクティビティをモニタリングする

前の例から引き続き、DBaaSインスタンスで実行されているdbtestセキュア・ターゲットでのユーザーDBA_DEBRAによるすべてのSQL文がAudit Vault Serverによって監査されます。すべてのアクティビティをOracle AVDFコンソールで確認できます。

1. Oracle AVDFコンソールに監査者としてログインします。

2. **「レポート」**タブで、**「すべてのアクティビティ」**をクリックします。
次の図は、dbtestセキュア・ターゲットでDBA_DEBRAユーザーが発行したすべての文を示しています。各アクティビティのタイムスタンプ、ステータス、ユーザー、SQLコマンド、その他の情報が表示されています。



Oracle Databaseの監査とOracle AVDFのベスト・プラクティス

Oracle AVDFを使用してOracle Databaseのセキュリティおよびコンプライアンス監査を行う際には、次のベスト・プラクティスに従ってください。

VCNセキュリティ・リストを使用してOracle AVDF VMのファイアウォールを構成する

VCNセキュリティ・リストを使用すると、Oracle AVDF VMへのネットワーク接続がVCN内の認可データベース・インスタンスから行われた場合にのみ許可することができます。

監査がDBaaSインスタンスのパフォーマンスに及ぼす影響を理解する

Audit Vault AgentはDBaaSインスタンスで実行され、Oracle Database監査証跡を読み取ってAudit Vault Serverにレコードをコピーします。Oracle AVDFは次のコレクタを利用しています。

- DBAUD (データベース監査表からの読取り)
- OSAUD (OSファイルからの読取り)
- REDO (REDOログの読取り)

エージェントによって収集されるイベントが多ければ多いほど、DBaaSインスタンスにかかる負

荷も大きくなります。一般に、1秒当たり100件の監査レコードを収集する場合、DBAUDとOSAUDには約2～3%のCPUオーバーヘッドがかかり、REDOには約6%のオーバーヘッドがかかります。このコレクタのオーバーヘッドは、標準監査とFGAによるパフォーマンス・オーバーヘッドを含んでいません。

1秒当たりの監査対象イベント数が多ければ多いほど、パフォーマンス・オーバーヘッドも大きくなります。そのため、どのイベントを監査するかを決める際には注意してください。

Audit Vault Serverのストレージ要件を理解する

監査レコードはAudit Vault Serverの領域を消費します。平均で、100万件の監査レコードには約900MBのディスク領域が必要です。1日に生成される監査レコードの数とその保存期間に応じて、十分なディスク領域(ブロック・ボリュームとOracle AVDF仮想ディスク・サイズの両方)を割り当てる必要があります。適切なサイズのディスクをプロビジョニングしないと、Oracle AVDF VMがクラッシュして、収集した監査レコードがすべて失われる可能性があります。

監査レコードをOracle Cloud Infrastructure Object Storageにアーカイブする

Oracle AVDFの監査レコードをOracle Cloud Infrastructure Object Storageバケットに定期的にアーカイブするよう設定することをお薦めします。Oracle AVDFでは、SCP (セキュア・コピー)を使用してIPアドレス対応ホストにアーカイブすることができます(NFSなどの他のオプションもあります)。Oracle AVDFの監査レコードをBYOH BMホストでアーカイブし、スクリプトを使用してBMホストからObject Storageバケットに監査レコードを転送することをお薦めします。定期的なアーカイブの設定の詳細は、Oracle AVDFのドキュメントを参照してください。

高可用性が得られるように構成する

Audit Vault Serverのペアを構成し、一方をプライマリ、もう一方をセカンダリにすることができます。プライマリの監査レコードは自動的にセカンダリに同期されます。このホワイト・ペーパーで説明したシナリオでは、プライマリとセカンダリのOracle AVDF VMを2つの異なるBYOH BMインスタンスにインストールして、最大限の可用性を得ることをお薦めします。高可用性(HA)設定については、Oracle AVDFのドキュメントを参照してください。

Audit Vault ServerへのSSHアクセスを有効にする

SSHアクセスは、Oracle AVDF VMのトラブルシューティングを行ったり、運用業務を実施したりする際に便利であるため、VMへのSSHアクセスを有効にすることをお薦めします。Oracle AVDFコンソールで、「システム」設定に移動して、ホストBMインスタンスからOracle AVDF VMへのSSHアクセスを有効にします。このステップが完了すると、`ssh support@AVDF_VM_IP`を使用して、ホストBMインスタンスからOracle AVDF VMにログインすることができます。

結論

このホワイト・ペーパーでは、Oracle Audit Vault and Database FirewallをOracle Cloud Infrastructureにデプロイし、Oracle Cloud Infrastructure DBaaSインスタンスを監査することでセキュリティとコンプライアンスの向上を図るソリューションを示しています。Oracle Cloud Infrastructure DBaaS API監査ログに加えて、Oracle AVDF監査は、DBaaSインスタンスを対象とした包括的な監査ロギングおよびモニタリング機能を提供します。この顧客管理型ソリューションを使用する場合、お客様がBMインスタンスにBYOHをデプロイして、Oracle AVDFセキュリティ・アプライアンスを実行できるようにする必要があります。

FAQ

Oracle AVDFアプライアンスをOracle Cloud Infrastructureインスタンスで直接実行できないのはなぜですか。

Oracle AVDFは、Oracle Linuxオペレーティング・システムとともにパッケージ化された監査ソフトウェアを含むセキュリティ・アプライアンスとして開発されています。Oracle AVDFをインストールする場合、ブート・ディスクを消去して、Oracle AVDF ISOをインストールする必要があります。Oracle AVDFをOracle Cloud Infrastructureインスタンスに直接インストールするためには、Oracle Cloud Infrastructureインスタンスで起動するようにOracle AVDF ISOをカスタマイズしなければなりません。現在のところ、使用可能なOracle AVDF ISOイメージはありません。

これはマネージド型のOracle AVDFサービスですか。

このホワイト・ペーパーでは、顧客管理型のソリューションを示しています。これは、企業がオンプレミスで使用する実証済の製品を利用して、お客様の重要なセキュリティ要件やコンプライアンス要件を満たすものです。Oracle AVDFアプライアンスを自社のVCNにデプロイして管理する責任はお客様にあります。Oracle Cloud Infrastructureまでご連絡いただき、マネージド型のOracle AVDFサービスに興味がある旨をお知らせください。

付録

BMインスタンスでSR-IOVを有効にする

1. `/etc/default/grub`ファイルで、`GRUB_CMDLINE_LINUX`行に`intel_iommu=on`を追加しま

す。

2. 新しいgrub構成ファイルを生成します。

```
grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

3. BMサーバーを再起動します。

VFを有効にしてセカンダリVNICのMACアドレスで構成する

1. 仮想機能(VF)を有効にして、`vepa`ブリッジ・モードを設定します。Oracle Linuxでは、`ens2f0`は物理インタフェースです。

```
echo “16” > /sys/class/net/ens2f0/device/sriov_numvfs

bridge link set dev ens2f0 hwmode vepa
```

2. 使用可能なVFをリストします。使用可能なVFのVF番号(VF_NUM)を書き留めてください。

```
ip link show ens2f0
```

3. VNICのMACアドレス(VNIC_MAC)でVFを構成します。

```
ip link set ens2f0 vf VF_NUM mac VNIC_MAC spoofchk off
```

セカンダリVNICのVLANタグを使用してネットワーク・インタフェースを作成する

1. VFネットワーク・デバイス名(VF_DEVICE_NAME)を取得します。

   VFの番号がVF_NUMの場合、次のコマンドの出力で行番号(VF_NUM+1)を選択します。たとえば、VF_NUMが1の場合は、出力の2番目の行を選択します。ポート、スロットおよび機能の番号は、その行の最初のフィールドとして、16進数形式でリストされています。たとえば、13:10:2はポート番号19、スロット番号16、機能番号2を表しており、VF_DEVICE_NAMEはenp19s16f2です。

```
lspci -nn | grep -i virtual
```

2. VFネットワーク・デバイスを起動します。

```
ip link set VF_DEVICE_NAME down

ip link set VF_DEVICE_NAME up
```

3. VFネットワーク・デバイスをVNIC VLANに割り当てます。

```
ip link add link VF_DEVICE_NAME name VLAN_DEVICE_NAME type vlan id
VNIC_VLAN_TAG

ip link set VLAN_DEVICE_NAME up
```

attach.xmlファイル

```
<interface type='direct'>
    <mac address='<VNIC_MAC>'/>
    <source dev='<VLAN_DEVICE_NAME>' mode='passthrough'/>
    <model type='e1000'/>
</interface>
```

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

オラクルとつながる

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services

Deploying Oracle Audit Vault and Database Firewall in Oracle Cloud Infrastructure
2018年4月
著者: Nachiketh Potlapally、George Csaba
協力著者: Michael Mesoros