Oracle Database@AWS ユーザーガイド

Oracle Database@AWS

Oracle Database@AWS: Oracle Database@AWS ユーザーガイド

Table of Contents

Oracle Database@AWS とは

Oracle Database@AWS は、AWS データセンター内の Oracle Cloud Infrastructure (OCI) によって管理される Oracle Exadata インフラストラクチャにアクセスできるようにするサービスです。Oracle Exadata ワークロードを移行し、AWS で実行されているアプリケーションとの低レイテンシーの接続を確立し、AWS のサービスと統合できます。AWS Marketplace を通じて 1 つの請求書を取得します。この請求書は、AWS コミットメントと Oracle Support rewards の対象となります。

次の図は、Oracle Exadata インフラストラクチャをホストする AWS データセンターに関連付けられた OCI リージョンの概要を示しています。AWS アベイラビリティーゾーン (AZ) 内で、Amazon VPC をデータセンターに関連付けられたプライベートネットワークにピアリング接続できます。これらのネットワークをピアリングすることで、VPC 内のアプリケーションサーバーは Oracle Exadata インフラストラクチャで実行されている Oracle データベースにアクセスできます。

Oracle Database@AWS の機能

Oracle Database@AWS を使用すると、次の機能のメリットが得られます。

Oracle Exadata データベースワークロードの AWS への移行

Oracle Database@AWS を使用すると、Oracle Exadata ワークロードを AWS 内の Oracle Exadata Database Service on Dedicated Infrastructure または Oracle Autonomous Database on Dedicated Exadata Infrastructure に簡単に移行できます。移行により、最小限の変更、フル機能の可用性、アーキテクチャの互換性、オンプレミスの Exadata デプロイと同じパフォーマンスが提供されます。Recovery Manager (RMAN)、Oracle Data Guard、トランスポータブルテーブルスペース、Oracle Data Pump、Oracle GoldenGate、AWS Database Migration Service、Oracle Zero Downtime Migration などの標準の Oracle データベース移行ツールを使用できます。

アプリケーションのレイテンシーの削減

Oracle Exadata と AWS で実行されているアプリケーションとの間に低レイテンシーの接続を確立できます。AWS でホストされるアプリケーションに近接しているため、ネットワークの遅延が最小限に抑えられ、パフォーマンスが向上します。

データ統合によるイノベーション

ゼロ ETL 統合を使用して Oracle と AWS 間でデータを統合し、分析、機械学習、生成 AI に活用することで、より深いインサイトを生成し、新しいイノベーションを開発できます。Amazon

Redshift を使用したゼロ ETL 統合により、Oracle Database@AWS に保存されたトランザクションデータに対してほぼリアルタイムの分析と機械学習 (ML) を有効にできます。

管理と運用の簡素化

共同サポート、購入、管理、運用により、Oracle と AWS の統合エクスペリエンスのメリットを享受できます。Oracle データベースサービスの使用は、既存の AWS コミットメントや Oracle Support rewards などの Oracle ライセンス特典の対象となります。使い慣れた AWS ツールやインターフェイスを使用して、Oracle Database@AWS リソースを購入、プロビジョニング、管理できます。AWS API、CLI、または SDK を使用してリソースをプロビジョニングおよび管理できます。AWS API は、リソースのプロビジョニングと管理に必要な対応する OCI API を呼び出します。

AWS サービスとのシームレスな統合

同じ環境で実行されている他の AWS のサービスやアプリケーションと統合できます。例えば、Oracle Database@AWS は Amazon EC2、Amazon VPC、IAM と統合されます。また、モニタリング用の Amazon CloudWatch やイベント管理用の Amazon EventBridge などの AWS のサービスと Oracle Database@AWS を統合することもできます。データベースのバックアップには、イレブンナインを超える耐久性を実現するように設計された Amazon S3 を使用できます。

関連する AWS のサービス

Oracle Database@AWS は次のサービスと連携して、Oracle データベースアプリケーションの可用性とスケーラビリティを向上させます。

- Amazon EC2 – Oracle アプリケーションサーバーとして機能する仮想サーバーを提供します。EC2 アプリケーションサーバーにトラフィックをルーティングするように、ロードバランサーを設定できます。詳細については、「Amazon EC2 ユーザーガイド」を参照してください。
- Amazon Virtual Private Cloud (VPC) – 論理的に隔離されている定義済みの仮想ネットワーク内で AWS リソースを起動できます。Oracle Exadata インフラストラクチャは、VPC にピアリング接続できる ODB ネットワークと呼ばれる特別なネットワークに存在します。その後、VPC でアプリケーションサーバーを実行し、Exadata データベースにアクセスできます。詳細については、Amazon VPC ユーザーガイドを参照してください。
- Amazon VPC Lattice – ODB ネットワークから Amazon S3 や Oracle マネージドバックアップなどの AWS のサービスへのネイティブアクセスを提供します。詳細については、「Amazon VPC Lattice とは」を参照してください。

- Amazon CloudWatch – Oracle Database@AWS のモニタリングサービスを提供します。OCI は Oracle Exadata システムに関するメトリクスデータを収集し、CloudWatch に送信します。詳細については、「Amazon CloudWatch での Oracle Database@AWS のモニターリング」を参照してください。
- AWS Identity and Access Management (IAM) – ユーザーのために Oracle Database@AWS リソースへのアクセスを安全にコントロールする際に役立ちます。IAM を使用して、どのユーザーが AWS リソースを使用できるかを制御し (認証)、さらに、どのリソースをユーザーがどのように使用できるかを制御します (認可)。詳細については、「Oracle Database@AWS のためのアイデンティティおよびアクセス管理」を参照してください。
- AWS 分析サービス – Exadata データベースからより迅速にインサイトを得るのに役立つ、広範で費用対効果の高い分析サービスのセットを提供します。各サービスは、インタラクティブ分析、ビッグデータ処理、データウェアハウス、リアルタイム分析、運用分析、ダッシュボード、視覚化など、幅広い分析ユースケース向けに構築されています。詳細については、「AWS での分析」を参照してください。

Oracle Database@AWS へのアクセス

AWS マネジメントコンソールを使用して、Oracle Database@AWS を作成、アクセス、管理できます。Oracle Database@AWS へのアクセスに使用するウェブインターフェイスを提供します。

Oracle Database@AWS の料金

Oracle Database@AWS のサービスは AWS Marketplace から購入できます。最初に Oracle 販売担当者に連絡します。その後、Oracle はプライベート料金契約に基づいて、AWS Marketplace でオファーをお客様に提供します。AWS 請求書には、使用量に基づいて料金が表示されます。

Oracle アプリケーションと Oracle データベースが同じアベイラビリティーゾーン (AZ) でホストされている場合、データ転送料金はかかりません。AZ 間の通信には、標準のデータ転送料金が適用されます。

ゼロ ETL、Oracle マネージドバックアップ、Amazon S3 などの Oracle Database@AWS マネージド統合を使用する場合、VPC Lattice を介したリソースの共有およびアクセスに対して標準のデータ処理料金が適用されます。Oracle Database@AWS マネージド統合には時間単位の料金はかかりません。詳細については、「Amazon VPC Lattice の料金」を参照してください。

次のステップ

これで、Oracle Database@AWS リソースの作成を開始する準備ができました。

1. Oracle Database@AWS の仕組みについて説明します。詳細については、「Oracle Database@AWS の仕組み」を参照してください。

   > **Note**
   >
   > AWS と Oracle Exadata に精通していて、すぐに開始したい場合は、このステップをスキップしてください。

2. AWS マネジメントコンソールから Oracle Database@AWS のプライベートオファーをリクエストし、オファーを承諾します。詳細については、「Oracle Database@AWS のプライベートオファーをリクエストする」を参照してください。

   > **Note**
   >
   > このプレビューでプライベートオファーをリクエストするには、AWS に連絡して、AWS アカウントを許可リストに追加してもらう必要があります。

3. AWS コンソールを使用して、ODB ネットワーク、Oracle Exadata インフラストラクチャ、Exadata VM クラスターを作成します。OCI ツールを使用して Exadata データベースを作成します。詳細については、「Oracle Database@AWS の開始方法」を参照してください。
4. AWS Resource Access Manager (AWS RAM) を使用してアカウント間でリソースを共有します。詳細については、「信頼されたアカウントでの共有 Oracle Database@AWS リソースの使用」を参照してください。

Oracle Database@AWS の仕組み

Oracle Database@AWS は Oracle Cloud Infrastructure (OCI) を AWS クラウドと統合します。以下のセクションでは、このマルチクラウドアーキテクチャの主要なコンポーネントについて説明します。

Oracle Exadata Database Service on Dedicated Infrastructure は、Exadata Database Machine を提供する OCI サービスです。Oracle Exadata Database Machine は、エンタープライズデータセンターで使用するための統合、事前設定、および事前テスト済みのフルスタックプラットフォームです。AWS コンソール、CLI、または API を使用して、AWS アベイラビリティーゾーン (AZ) に Oracle Exadata インフラストラクチャと VM クラスターを作成できます。

AWS でリソースを作成したら、OCI API を使用して Oracle Exadata データベースを作成および管理します。Amazon VPC とピアリング接続する ODB ネットワークにより、Amazon EC2 アプリケーションサーバーは Exadata データベースにアクセスできます。このようにして、Oracle Exadata データベースは AWS 環境に統合されます。

Oracle Database@AWS アーキテクチャを次の図に示します。

OCI 子サイト

Oracle Cloud Infrastructure は OCI リージョンおよび可用性ドメインでホストされています。OCI リージョンは、OCI リージョン内の独立したデータセンタークラスターである OCI 可用性ドメイン (AD) で構成されます。OCI 子サイトは、OCI アベイラビリティードメインを AWS リージョンのアベイラビリティーゾーン (AZ) に拡張するデータセンターです。Exadata インフラストラクチャは論理的には OCI リージョンに存在し、物理的には AWS リージョンに存在します。

Oracle Database@AWS の OCI 子サイトは、物理的には AWS データセンターにあります。AWS は Exadata インフラストラクチャをホストし、OCI はデータセンター内で Exadata インフラストラクチャのハードウェアをプロビジョニングして維持します。AWS コンソール、CLI、または API を使用して、Exadata インフラストラクチャ、プライベートネットワーク、VM クラスターを設定できます。Amazon EC2 や Amazon VPC などの AWS のサービスを使用して、インフラストラクチャで実行されている Oracle Exadata データベースへのアプリケーションアクセスを許可できます。

Oracle Exadata インフラストラクチャ

Oracle Exadata インフラストラクチャは、Oracle Exadata データベースを実行するデータベースサーバーとストレージサーバーの基盤となるアーキテクチャです。インフラストラクチャは、AWS アベイラビリティーゾーン (AZ) にあります。Exadata インフラストラクチャ上に VM クラスターを作成するには、AWS コンソール、CLI、または API を使用します。

Oracle Exadata インフラストラクチャは、データベースサーバーと呼ばれる物理マシンに分散されます。これらのサーバーは、Amazon EC2 専有サーバーと同様に、コンピューティングリソースを提供します。各データベースサーバーは、ハイパーバイザーで実行されている 1 つ以上の仮想マシン (VM) をホストします。これらの関係を示すアーキテクチャ図については、「Exadata Database Service on Dedicated Infrastructure Technical Architecture」を参照してください。

Oracle Database@AWS で Exadata インフラストラクチャを作成するときは、次のような情報を指定します。

- データベースサーバーの総数
- ストレージサーバーの総数
- Exadata システムモデル (X11M)
- インフラストラクチャをホストする AZ (「のサポート対象 リージョンOracle Database@AWS」を参照)

Oracle Exadata インフラストラクチャを作成する方法については、「ステップ 2: Oracle Database@AWS で Oracle Exadata インフラストラクチャを作成する」を参照してください。

ODB ネットワーク

ODB ネットワークは、AWS アベイラビリティーゾーン (AZ) で OCI インフラストラクチャをホストするプライベートの分離されたネットワークです。ODB ネットワークは、IP アドレスの CIDR 範囲で構成されます。ODB ネットワークは、OCI 子サイト内に存在するネットワークに直接マッピングされるため、AWS と OCI 間の通信手段として機能します。Exadata VM クラスターを作成するときは、ODB ネットワークを指定する必要があります (「ステップ 3: Oracle Database@AWS で Exadata VM クラスターまたは Autonomous VM クラスターを作成する」を参照)。

Oracle Database@AWS API を使用して、ODB ネットワーク内のリソースをプロビジョニングします。ODB ネットワークは AWS によって管理されますが、ODB ピアリング接続を設定して Amazon

VPC を ODB ネットワークに接続できます。詳細については、「ODB ピアリング」を参照してください。

ODB ネットワークを作成するときは、以下のような情報を指定します。

- アベイラビリティーゾーン – ODB ネットワークは AZ に固有です。

  Oracle Database@AWS は次の AWS リージョンで使用できます。

  米国東部 (バージニア北部)

  物理 ID が use1-az4 および use1-az6 の AZ を使用できます。

  米国西部 (オレゴン)

  物理 ID が usw2-az3 および usw2-az4 の AZ を使用できます。

  アジアパシフィック (東京)

  物理 ID が apne1-az1 および apne1-az4 の AZ を使用できます。

  米国東部 (オハイオ)

  物理 ID が use2-az1 および use2-az2 の AZ を使用できます。

  欧州 (フランクフルト)

  物理 ID が euc1-az1 および euc1-az2 の AZ を使用できます。

  カナダ (中部)

  物理 ID が cac1-az4 の AZ を使用できます。

  アジアパシフィック (シドニー)

  物理 ID が apse2-az4 の AZ を使用できます。

  上記の物理 AZ ID にマッピングされるアカウント内の論理 AZ 名を検索するには、次のコマンドを実行します。

```
aws ec2 describe-availability-zones \
  --region us-east-1 \
  --query "AvailabilityZones[*].{ZoneName:ZoneName, ZoneId:ZoneId}" \
  --output table
```

- クライアント CIDR アドレス – ODB ネットワークには、Exadata VM クラスターと Autonomous VM クラスターのクライアントサブネット CIDR が必要です。

- バックアップ CIDR アドレス – ODB ネットワークでは、VM クラスターのマネージドデータベースバックアップ用のバックアップサブネット CIDR が必要です。バックアップサブネットは、Exadata VM クラスターではオプションです。
- AWS のサービス統合 – Amazon S3 や Amazon Redshift とのゼロ ETL などの AWS のサービス統合用のネットワークパスを設定できます。詳細については、「AWS のサービス統合」を参照してください。

詳細については、「ステップ 1: Oracle Database@AWS で ODB ネットワークを作成する」を参照してください。

Virtual Private Cloud (VPC)

仮想プライベートクラウド (VPC) は、AWS クラウド内で作成する仮想ネットワークです。AWS クラウド内の他の仮想ネットワークから論理的に分離されているため、独自の IP アドレス範囲の選択、サブネットの作成、ルートテーブルとネットワークゲートウェイの設定など、仮想ネットワーク環境を完全に制御できます。詳細については、「Amazon VPC とは」を参照してください。

Amazon VPC 内で Amazon EC2 インスタンスを起動できます。EC2 インスタンスは、Oracle Exadata データベースと通信するアプリケーションサーバーをホストできます。VPC 内の他の EC2 インスタンスと同様に、アプリケーションサーバーを管理および起動できます。詳細については、「Amazon EC2 とは」を参照してください。

デフォルトでは、ODB ネットワークは VPC に接続されません。ODB ネットワークを既存の AWS インフラストラクチャに接続するには、ODB ネットワークと 1 つの VPC の間にピアリング接続を作成します。ODB ネットワークを作成するときに VPC を指定できます。詳細については、「ステップ 1: Oracle Database@AWS で ODB ネットワークを作成する」を参照してください。

ODB ピアリング

ODB ピアリングは、Amazon VPC と ODB ネットワーク間でトラフィックをプライベートにルーティングできるようにする、ユーザー作成のネットワーク接続です。VPC と ODB ネットワークの間には 1 対 1 の関係があります。ピアリング接続後、VPC 内の Amazon EC2 インスタンスは、同じネットワーク内にあるかのように ODB ネットワーク内の Oracle Exadata データベースと通信できます。

> **Note**
>
> ODB ピアリングは VPC ピアリングとは異なります。VPC ピアリングは、2 つの VPC 間のトラフィックをルーティングするピアリング接続です。

AWS RAM を使用して、1 つのアカウントの ODB ネットワークと別のアカウントの VPC をピアリングできます。ODB ネットワークを別のアカウントと共有する場合、信頼アカウントはピアリングを直接開始できます。ODB ピアリング接続を開始するアカウントは、接続を所有および管理します。

ODB ピアリング接続を作成または更新するときに、ピアネットワーク CIDR を指定できます。このようにして、ピア VPC 内のどのサブネットが ODB ネットワークにアクセスできるかを制御します。VPC アカウントは、ODB ネットワークを所有しなくても CIDR 範囲を更新できます。詳細については、「Oracle Database@AWS での Amazon VPC への ODB ピアリングの設定」を参照してください。

VPC 内のリソースは、複数のアベイラビリティーゾーン (AZ) にまたがることができます。ODB ネットワークでは、リソースは単一の AZ にバインドされます。この AZ は、ODB ネットワークを作成するときに定義します。

ODB ピアリング接続の作成

ODB ピアリング接続は ODB ネットワークの特性ではありませんが、独自の ID (プレフィックスは `odbpcx-`) とライフサイクルを持つ独立したリソースです。専用の API セットを使用してピアリング接続を管理します。例えば、Oracle Database@AWS コンソールまたは `CreateOdbPeeringConnection` API を使用して、既存の ODB ネットワークへの ODB ピアリング接続を作成します。詳細については、「Oracle Database@AWS での ODB ピアリング接続の作成」を参照してください。

ODB ピアリング接続を作成すると、Oracle Database@AWS は次のアクションを自動的に実行します。

1. Oracle VCN CIDR との CIDR ブロックの重複チェックなど、ネットワーク設定を検証します
2. 基盤となるネットワークピアリングインフラストラクチャをセットアップします
3. VPC CIDR アドレスを使用して (VPC ではなく) ODB ネットワークのルートテーブルを設定します

ODB ピアリング接続を作成したら、Amazon EC2 `create-route` コマンドを使用して VPC ルートテーブルを手動で更新します。詳細については、「ODB ピアリング用の VPC ルートテーブルの設定」を参照してください。

AWS のサービス統合

Oracle データベースに強化された機能と接続オプションを提供するために、Oracle Database@AWS は Amazon VPC Lattice を使用して AWS のサービスと統合されます。追加の VPC や複雑なネットワーク設定を必要とせずに、ODB ネットワークから直接 AWS のサービスへのネットワークパスを設定できます。

Oracle Database@AWS は、以下の AWS マネージドサービス統合をサポートしています。

Amazon S3

次の方法で Amazon S3 を Oracle Database@AWS と統合できます。

- Oracle マネージド Amazon S3 への自動バックアップ – Oracle Database@AWS は、自動バックアップのためにネットワークアクセスを自動的に有効にします。この統合を無効にすることはできません。OCI コンソールで Amazon S3 をマネージドバックアップターゲットとして設定すると、OCI は自動バックアップを S3 バケットにアップロードします。
- ODB ネットワークから Amazon S3 への直接アクセス – S3 への直接 ODB ネットワークアクセスを有効にし、スクリプト、インポートおよびエクスポートファイル、および関連ファイルを S3 バケットに保存できます。このアクセスを無効にすることができます。この設定は、Oracle マネージド自動バックアップの自動ネットワークアクセスとは無関係です。

Amazon Redshift とのゼロ ETL 統合

ODB ネットワークと Amazon Redshift とのゼロ ETL 統合を有効にできます。この統合により、従来の抽出、変換、ロード (ETL) プロセスなしで、Oracle Database@AWS で実行されている Oracle データベースから Amazon Redshift にデータをレプリケートできます。この統合により、Oracle データを Amazon Redshift と自動的に同期することで、リアルタイム分析と AI ワークロードが可能になります。

AWS のサービスのマネージド統合に加えて、VPC Lattice を使用して、他の VPC でホストされているサービスやリソースにアクセスしたり、VPC から ODB ネットワークインスタンスにアクセスしたりすることもできます。VPC Lattice コンソール、CLI、および API を使用して、アクセスとリソースを管理できます。詳細については、以下のリソースを参照してください。

- Oracle Database@AWS でのバックアップ

- Oracle Database@AWS の Amazon Redshift とのゼロ ETL 統合
- 「Amazon VPC Lattice とは」および「Oracle Database@AWS 用の VPC Lattice」

複数の VPC からのトラフィックルーティング

複数の VPC が 1 つの ODB ネットワークの Oracle Database@AWS リソースにアクセスできるようにするには、AWS Transit Gateway または AWS Cloud WAN を使用できます。

AWS Transit Gateway

Amazon VPC Transit Gateway は、VPC とオンプレミスネットワークを相互接続するために使用されるネットワークの中継ハブです。ODB ネットワークは、ODB ネットワークと単一の VPC 間の 1 対 1 の直接ピアリング接続のみをサポートします。ODB ネットワークを VPC にピアリング接続し、この VPC をトランジットゲートウェイにアタッチできます。ゲートウェイは複数の VPC に接続できます。このトランジットゲートウェイ設定では、複数の VPC サブネット間のトラフィックを単一の ODB ネットワークにルーティングできます。

詳細については、「Oracle Database@AWS の Amazon VPC Transit Gateway の設定」を参照してください。

AWS クラウド WAN

AWS クラウド WAN は、クラウド環境とオンプレミス環境全体のリソースを接続する統合グローバルネットワークを構築、管理、モニタリングできるマネージド型ワイドエリアネットワーク (WAN) サービスです。中央ダッシュボードを使用すると、AWS グローバルネットワーク全体にまたがるオンプレミスのブランチオフィス、データセンター、VPC を接続できます。

ODB ネットワークを VPC にピアリング接続し、この VPC をクラウド WAN コアネットワークにアタッチできます。この設定では、クラウド WAN を使用して、複数の VPC またはオンプレミスネットワークと ODB ネットワーク間でトラフィックをルーティングできます。詳細については、「Oracle Database@AWS の AWS Cloud WAN の設定」を参照してください。

Exadata VM クラスター

Exadata VM クラスターは、緊密に結合された一連の Exadata VM のセットです。各 VM には、Oracle Real Application Clusters (Oracle RAC) や Oracle Grid Infrastructure など、Oracle

Enterprise Edition のすべての機能を備えた完全な Oracle データベースインストールが含まれています。VM クラスターに 1 つ以上の Oracle Exadata データベースを作成できます。VM および VM クラスターのアーキテクチャを示す図については、「Exadata Database Service on Dedicated Infrastructure Technical Architecture」を参照してください。

VM クラスターを作成するときは、以下を含む情報を指定します。

- ODB ネットワーク
- Oracle Exadata インフラストラクチャ
- クラスター内の VM を配置するデータベースサーバー
- 使用可能な Exadata ストレージの合計量

VM クラスター内の各 VM の CPU コア、メモリ、ローカルストレージを設定できます。詳細については、「ステップ 3: Oracle Database@AWS で Exadata VM クラスターまたは Autonomous VM クラスターを作成する」を参照してください。

Autonomous VM クラスター

Autonomous VM クラスターは、機械学習と AI を使用して主要な管理タスクを自動化するフルマネージド型データベースです。従来のデータベースとは異なり、Autonomous データベースは、人間の介入を必要とせずに、データベースのプロビジョニング、保護、更新、バックアップ、チューニングを自動的に行います。

VM あたりの ECPU コア数、CPU あたりのデータベースメモリ、データベースストレージ、Autonomous コンテナデータベースの最大数を設定できます。詳細については、「ステップ 3: Oracle Database@AWS で Exadata VM クラスターまたは Autonomous VM クラスターを作成する」を参照してください。

Oracle Exadata データベース

Oracle Exadata は、Oracle データベースを実行するための高性能プラットフォームを提供するエンジニアリングシステムです。Oracle Database@AWS では、AWS コンソールを使用して、Exadata データベースをホストする Oracle Exadata インフラストラクチャと VM クラスターを作成します。次に、OCI API を使用して Oracle データベースを作成および管理します。詳細については、「ステップ 4: Oracle クラウドインフラストラクチャで Oracle Exadata データベースを作成する」を参照してください。

Oracle Database@AWS へのオンボーディング

Oracle Database@AWS の使用を開始する前に、AWS にサインアップし、必要なユーザーを作成してください。その後、Oracle からのプライベートオファーを受け入れることで、AWS Marketplace から Oracle Database@AWS を購入できます。

AWS アカウントへのサインアップ

AWS アカウント がない場合は、以下のステップを実行して作成します。

AWS アカウント にサインアップするには

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

   AWS アカウントにサインアップすると、AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

サインアップ処理が完了すると、AWS からユーザーに確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

AWS アカウントにサインアップしたら、AWS アカウントのルートユーザーをセキュリティで保護し、AWS IAM アイデンティティセンター を有効にして、管理ユーザーを作成します。これにより、日常的なタスクにルートユーザーを使用しないようにします。

AWS アカウントのルートユーザー をセキュリティで保護する

1. [ルートユーザー] を選択し、AWS アカウント のメールアドレスを入力して、アカウント所有者として AWS マネジメントコンソール にサインインします。次のページでパスワードを入力します。

ルートユーザーを使用してサインインする方法については、「AWS サインイン ユーザーガイド」の「ルートユーザーとしてサインインする」を参照してください。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」の「AWS アカウント ルートユーザーの仮想 MFA デバイスを有効にする (コンソール)」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「AWS IAM アイデンティティセンター の有効化」を参照してください。

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   IAM アイデンティティセンターディレクトリ をアイデンティティソースとして使用するチュートリアルについては、「AWS IAM アイデンティティセンター ユーザーガイド」の「デフォルトの IAM アイデンティティセンターディレクトリ を使用してユーザーアクセスを設定する」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM アイデンティティセンターユーザーを使用してサインインする方法については、「AWS サインイン ユーザーガイド」の「AWS アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「アクセス許可セットを作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「グループを追加する」を参照してください。

Oracle Database@AWS のプライベートオファーをリクエストする

AWS Marketplace 販売者のプライベートオファー機能を使用すると、Oracle Database@AWS の料金と EULA 条件を Oracle にリクエストして受け取ることができます。Oracle と価格設定と条件を交渉すると、Oracle は指定した AWS アカウントのプライベートオファーを作成します。プライベートオファーを承諾し、交渉価格と利用規約を受け取ります。このとき、Oracle Database@AWS ダッシュボードを使用できます。プライベートオファー契約の有効期限に達すると、製品のパブリック料金に自動的に移行されるか、Oracle Database@AWS のサブスクリプションが解除されます。プライベートオファーの詳細については、「AWS Marketplace のプライベートオファー」を参照してください。

Oracle Database@AWS のプライベートオファーをリクエストして承諾するには

1. AWS マネジメントコンソール にサインインします。
2. Oracle Database@AWS を検索して選択します。
3. [プライベートオファーをリクエストする] を選択します。

   > **Note**
   >
   > Oracle Database@AWS ダッシュボードは、プライベートオファーを承諾するまで使用できません。

4. Oracle Cloud Infrastructure (OCI) サイトで、リージョンや連絡先情報などの詳細を指定します。
5. OCI 担当者からお客様に連絡があり、プライベートオファーが利用可能になるまで待ちます。
6. AWS マネジメントコンソール で、[プライベートオファーを表示] を選択します。
7. オファーを選択し、[オファーを表示] を選択します。
8. [契約書を作成] を選択し、その後のプロンプトに応答してプライベートオファーを承諾します。

9. プライベートオファーを承諾したら、OCI アカウントをアクティブ化する必要があります。Oracle アクティベーションリンクには、AWS マネジメントコンソールから直接アクセスできます。

    1. コンソールで、[使用を開始する] セクションに移動します。
    2. コンソールにある Oracle アクティベーションリンクをクリックします。または、E メールで送信されたアクティベーションリンクを使用することもできます。
    3. Oracle アクティベーションページで、新しい Oracle クラウドアカウントを作成するか、既存のアカウントに追加するかを選択します。
    4. 画面の指示に従ってアクティベーションプロセスを完了します。
    5. アクティベーションリクエストを送信すると、AWS マネジメントコンソールに [アクティベーションが進行中] ステータスが表示され、ダッシュボードは一時的に無効になり、理由が表示されます。
    6. アクティベーションが完了すると、Oracle Database@AWS ダッシュボードが利用可能になり、リソースを管理できるようになります。
10. AWS マネジメントコンソールで、[ダッシュボード] を選択します。

複数のリージョンで Oracle Database@AWS をサブスクライブする

AWS Marketplace を通じて Oracle Database@AWS にサブスクライブしてオンボーディングを完了すると、AWS アカウントが OCI テナンシーにリンクされます。このリンクは、関連リソースとともに、Oracle Database@AWS が利用可能なすべての AWS リージョンに自動的にレプリケートされます。各リージョンごとにプロセスを繰り返すのではなく、サブスクライブとオンボードを 1 回だけ実行します。

複数のリージョンで Oracle Database@AWS を使用するには、次の手順を実行します。

1. AWS Marketplace を通じて Oracle Database@AWS にサブスクライブし、オンボーディングプロセスを完了します。

    Oracle Database@AWS を初めてサブスクライブすると、アカウントはホームリージョンでアクティブ化されます。Oracle Cloud Infrastructure (OCI) でホームリージョンを指定します。
2. OCI コンソールを使用して任意のリージョンを有効にします。

OCI でリージョンを有効にせず、Oracle Database@AWS コンソールでこのリージョンに切り替えると、サブスクライブしていないことを示すエラーが表示されます。この場合、このリージョンで Oracle Database@AWS ダッシュボードを使用する前に、OCI でこのリージョンを有効にする必要があります。

3. サブスクリプションプロセスを繰り返すことなく、サポートされている任意の AWS リージョンの Oracle Database@AWS にアクセスできます。

Oracle Database@AWS の開始方法

Oracle Database@AWS の使用を開始するには、Oracle Database@AWS コンソール、CLI、または API を使用して次のリソースを作成できます。

1. ODB ネットワーク
2. Oracle Exadata インフラストラクチャ
3. Exadata VM クラスターまたは Autonomous VM クラスター
4. ODB ピアリング接続

インフラストラクチャに Oracle Exadata データベースを作成するには、Oracle Database@AWS ダッシュボードではなく Oracle Cloud Infrastructure (OCI) コンソールまたは API を使用する必要があります。したがって、2 つのクラウド環境にリソースをデプロイします。ネットワークリソースとインフラストラクチャリソースは AWS にあり、データベース管理コントロールプレーンは OCI にあります。詳細については、Oracle Cloud Infrastructure ドキュメントの「Oracle Database@AWS」を参照してください。

Oracle Database@AWS のセットアップの前提条件

Oracle Exadata インフラストラクチャを設定する前に、以下を実行してください。

- 「Oracle Database@AWS へのオンボーディング」の手順を実行します。Oracle Database@AWS を使用するには、プライベートオファーを受け入れている必要があります。
- IAM プリンシパルに、ユーザーに Oracle Database@AWS リソースのプロビジョニングを許可する に一覧表示されているポリシーのアクセス許可を付与します。これらのアクセス許可は、Oracle Database@AWS を使用するのに必要です。

Oracle Database@AWS でサポートされている OCI サービス

Oracle Database@AWS は、次の Oracle Cloud Infrastructure (OCI) サービスをサポートしています。

- 専用インフラストラクチャ上の Oracle Exadata Database Service – AWS 内でアクセス可能なフルマネージド型の専用 Exadata 環境を提供します。詳細については、OCI ドキュメントの「専用インフラストラクチャ上の Oracle Exadata Database Service」を参照してください。

- 専用 Exadata インフラストラクチャ上の Autonomous データベース – OCI で実行されている高度に自動化されたフルマネージド型のデータベース環境を、ハードウェアおよびソフトウェアリソースをコミットして提供します。詳細については、OCI ドキュメントの「専用 Exadata インフラストラクチャ上の Autonomous データベースについて」を参照してください。

のサポート対象 リージョンOracle Database@AWS

Oracle Database@AWS は次の AWS リージョンで使用できます。

米国東部 (バージニア北部)

物理 ID が use1-az4 および use1-az6 の AZ を使用できます。

米国西部 (オレゴン)

物理 ID が usw2-az3 および usw2-az4 の AZ を使用できます。

アジアパシフィック (東京)

物理 ID が apne1-az1 および apne1-az4 の AZ を使用できます。

米国東部 (オハイオ)

物理 ID が use2-az1 および use2-az2 の AZ を使用できます。

欧州 (フランクフルト)

物理 ID が euc1-az1 および euc1-az2 の AZ を使用できます。

カナダ (中部)

物理 ID が cac1-az4 の AZ を使用できます。

アジアパシフィック (シドニー)

物理 ID が apse2-az4 の AZ を使用できます。

上記の物理 AZ ID にマッピングされるアカウント内の論理 AZ 名を検索するには、次のコマンドを実行します。

```
aws ec2 describe-availability-zones \
  --region us-east-1 \
```

```
  --query "AvailabilityZones[*].{ZoneName:ZoneName, ZoneId:ZoneId}" \
  --output table
```

Oracle Database@AWS の IP アドレス空間の計画

Oracle Database@AWS の IP アドレス空間を慎重に計画します。ODB ネットワークにプロビジョニングできるクラスターあたりの VM の数など、VM クラスターの数に基づいて IP アドレスの消費量を検討してください。詳細については、「Oracle Cloud Infrastructure ドキュメント」の「ODB ネットワーク設計」を参照してください。

トピック

- ODB ネットワーク内の IP アドレスの制限
- ODB ネットワークのクライアントサブネット CIDR 要件
- ODB ネットワークのバックアップサブネット CIDR 要件
- ODB ネットワークの IP 消費シナリオ

ODB ネットワーク内の IP アドレスの制限

ODB ネットワークの CIDR 範囲に関する以下の制限に注意してください。

- ODB ネットワークのクライアントまたはバックアップサブネット CIDR 範囲は、作成後に変更することはできません。
- IPv4 CIDR ブロックの関連付け制限のテーブルの制限された関連付け列で VPC CIDR 範囲を使用することはできません。
- Exadata X9M の場合、IP アドレス 100.106.0.0/16 および 100.107.0.0/16 は、OCI オートメーションによるクラスター相互接続用に予約されているため、次を実行することはできません。
  - これらの範囲を ODB ネットワークのクライアントまたはバックアップ CIDR 範囲に割り当てます。
  - ODB ネットワークへの接続に使用される VPC CIDR には、これらの範囲を使用します。
- 次の CIDR 範囲は Oracle Cloud Infrastructure 用に予約されており、ODB ネットワークには使用できません。
  - Oracle Cloud の予約済みの範囲 CIDR 169.254.0.0/16
  - リザーブドクラス D 224.0.0.0 - 239.255.255.255
  - リザーブドクラス E 240.0.0.0 - 255.255.255.255

- クライアントサブネットとバックアップサブネットの IP アドレス CIDR 範囲を重複させることはできません。
- クライアントサブネットとバックアップサブネットに割り当てられた IP アドレス CIDR 範囲と、ODB ネットワークへの接続に使用される VPC CIDR 範囲が重複することはできません。
- VM クラスター内の VM を別の ODB ネットワークにプロビジョニングすることはできません。ネットワークは VM クラスターのプロパティです。つまり、VM クラスター内の VM は同じ ODB ネットワークにのみプロビジョニングできます。

ODB ネットワークのクライアントサブネット CIDR 要件

次の表で、クライアントサブネット CIDR のサービスおよびインフラストラクチャによって消費される IP アドレスの数を示します。クライアントサブネットの最小 CIDR サイズは /27 で、最大サイズは /16 です。

IP アドレス番号	消費元	注意事項
6	Oracle Database@AWS	これらの IP アドレスは、ODB ネットワークでプロビジョニングする VM クラスターの数に関係なく予約されます。Oracle Database@AWS は以下を消費します。 • AWS の ODB ネットワークリソース用に予約された 3 つの IP アドレス • OCI ネットワークサービス用に予約された 3 つの IP アドレス
3	各 VM クラスター	これらの IP アドレスは、各 VM クラスターに存在する VM の数に関係なく、単一クライアントアクセス名 (SCAN) 用に予約されています。
4	各 VM	これらの IP アドレスは、インフラストラクチャの VM の数にのみ依存します。

ODB ネットワークのバックアップサブネット CIDR 要件

次の表で、バックアップサブネット CIDR のサービスおよびインフラストラクチャによって消費される IP アドレスの数を示します。バックアップサブネットの最小 CIDR サイズは /28 で、最大サイズは /16 です。

IP アドレス番号	消費元	注意事項
3	Oracle Database@AWS	これらの IP アドレスは、ODB ネットワークでプロビジョニングする VM クラスターの数に関係なく予約されます。Oracle Database@AWS は以下を消費します。 • CIDR 範囲の最初にある 2 つの IP アドレス • CIDR 範囲の最後にある 1 つの IP アドレス
3	各 VM	これらの IP アドレスは、インフラストラクチャの VM の数にのみ依存します。

ODB ネットワークの IP 消費シナリオ

次の表に、VM クラスターのさまざまな設定で ODB ネットワークで消費されている IP アドレスを示します。/28 はクライアントサブネット CIDR が 2 つの VM を持つ 1 つの VM クラスターをデプロイするための技術的な最小 CIDR 範囲ですが、少なくとも /27 CIDR 範囲を使用することをお勧めします。この場合、IP 範囲は VM クラスターによって完全に消費されず、追加の IP アドレスの割り当てを許可します。

設定	消費されたクライアント IP	クライアント IP の最小値	消費されたバックアップ IP	バックアップ IP の最小値
2 つの VM を持つ 1 つの VM クラスター	17 (6 サービス + 3 クラスター + 4*2)	32 (/27 CIDR 範囲)	9 (3 サービス + 3*2)	16 (/28 CIDR 範囲)
3 つの VM を持つ 1 つの VM クラスター	21 (6 サービス + 3 クラスター + 4*3)	32 (/27 CIDR 範囲)	12 (3 サービス + 3*3)	16 (/28 CIDR 範囲)

設定	消費されたクライアント IP	クライアント IP の最小値	消費されたバックアップ IP	バックアップ IP の最小値
4 つの VM を持つ 1 つの VM クラスター	25 (6 サービス + 3 クラスター + 4*4)	32 (/27 CIDR 範囲)	15 (3 サービス + 3*4)	16 (/28 CIDR 範囲)
8 つの VM を持つ 1 つの VM クラスター	41 (6 サービス + 3 クラスター + 4*8)	64 (/26 CIDR 範囲)	27 (3 サービス + 3*8)	32 (/27 CIDR 範囲)

次の表は、特定のクライアント CIDR 範囲に与えることが可能な各設定のインスタンス数を示しています。例えば、4 つの VM を持つ 1 つの VM クラスターは、クライアントサブネットで 24 個の IP アドレスを消費します。CIDR 範囲が /25 の場合、128 個の IP アドレスを使用できます。したがって、サブネットに 5 つの VM クラスターをプロビジョニングできます。

VM クラスターの設定	/27 で使用できる数 (32 IP)	/26 で使用できる数 (64 IP)	/25 で使用できる数 (128 IP)	/24 で使用できる数 (256 IP)	/23 で使用できる数 (512 IP)	/22 で使用できる数 (1024 IP)
2 つの VM を持つ 1 つの VM クラスター (16 IP)	1	3	7	15	30	60
3 つの VM を持つ 1 つの VM クラスター (20 IP)	1	3	6	12	24	48
4 つの VM を持つ 1 つの VM クラスター (24 IP)	1	2	5	10	20	40
2 つの VM を持つ 2 つの VM クラスターそれぞれ (27 IP)	1	2	4	9	18	36

VM クラスターの設定	/27 で使用できる数 (32 IP)	/26 で使用できる数 (64 IP)	/25 で使用できる数 (128 IP)	/24 で使用できる数 (256 IP)	/23 で使用できる数 (512 IP)	/22 で使用できる数 (1024 IP)
3 つの VM を持つ 2 つの VM クラスターそれぞれ (35 IP)	0	1	3	7	14	28
4 つの VM を持つ 2 つの VM クラスターそれぞれ (43 IP)	0	1	2	5	11	23

ステップ 1: Oracle Database@AWS で ODB ネットワークを作成する

ODB ネットワークは、 アベイラビリティーゾーン (AZ) で OCI インフラストラクチャをホストするプライベートの分離されたネットワークです。ODB ネットワークと Oracle Exadata インフラストラクチャは、VM クラスターをプロビジョニングし、Exadata データベースを作成するための前提条件です。ODB ネットワークと Oracle Exadata インフラストラクチャは、どちらの順序でも作成できます。詳細については、「ODB ネットワーク」および「ODB ピアリング」を参照してください。

このタスクは、Oracle Database@AWS の IP アドレス空間の計画 を読んだことを前提としています。後で ODB ネットワークを変更または削除するには、「Oracle Database@AWS の管理」を参照してください。

ODB ネットワークを作成するには

1. AWS マネジメントコンソールにサインインして、Oracle Database@AWS コンソール (https://console.aws.amazon.com/odb/) を開きます。
2. 右上で AWS リージョンを選択します。詳細については、「のサポート対象 リージョンOracle Database@AWS」を参照してください。
3. 左側のペインから、[ODB ネットワーク] を選択します。
4. [ODB ネットワークを作成する] を選択します。
5. [ODB ネットワーク名] で、ネットワーク名を入力します。名前は 1～255 文字で、英字またはアンダースコアで始まる必要があります。連続したハイフンを含めることはできません。

6. [アベイラビリティーゾーン] で、AZ 名を選択します。サポートされている AZ については、「のサポート対象 リージョンOracle Database@AWS」を参照してください。
7. [クライアントサブネット CIDR] で、クライアント接続の CIDR 範囲を指定します。詳細については、「ODB ネットワークのクライアントサブネット CIDR 要件」を参照してください。
8. [Backup サブネット CIDR] で、バックアップ接続の CIDR 範囲を指定します。バックアップトラフィックを分離して回復性を向上させるには、バックアップ CIDR とクライアント CIDR を重複させないことをお勧めします。詳細については、「ODB ネットワークのバックアップサブネット CIDR 要件」を参照してください。
9. [DNS 設定] で、次のいずれかのオプションを選択します。

   デフォルト

   [ドメイン名プレフィックス] には、ドメインのプレフィックスとして使用する名前を入力します。ドメイン名は oraclevcn.com に固定されています。例えば、**myhost** と入力した場合、完全修飾ドメイン名は myhost.oraclevcn.com です。

   カスタムドメイン名

   [ドメイン名] には、完全なドメイン名を入力します。例えば、myhost.myodb.com と入力します。
10. (オプション) [サービスの統合] では、VPC Lattice を使用してネットワークと統合するサービスを選択します。Oracle データベースに強化された機能と接続オプションを提供するために、Oracle Database@AWS は、さまざまな AWS のサービスと統合されます。次の統合のいずれかを選択します。

    Amazon S3

    Amazon S3 への直接 ODB ネットワークアクセスを有効にします。データベースは、データのインポート/エクスポートまたはカスタムバックアップのために S3 にアクセスできます。JSON ポリシーを入力できます。詳細については、「Oracle Database@AWS での Amazon S3 へのユーザー管理のバックアップ」を参照してください。

    ゼロ ETL

    Amazon Redshift を使用し、トランザクションデータでリアルタイム分析と機械学習を有効にします。詳細については、「Oracle Database@AWS の Amazon Redshift とのゼロ ETL 統合」を参照してください。

> **Note**
>
> ODB ネットワークを作成すると、Oracle Database@AWS は Oracle マネージド型バックアップのネットワークアクセスを Amazon S3 に自動的に事前設定します。この統合を有効または無効にすることはできません。詳細については、「AWS のサービス統合」を参照してください。

11. (オプション) [タグ] には、ネットワークのタグを最大 50 個入力します。タグは、リソースの整理と追跡に使用できるキーと値のペアです。
12. [ODB ネットワークを作成する] を選択します。

ODB ネットワークを作成した後、VPC にピア接続できます。ODB ピアリングは、Amazon VPC と ODB ネットワーク間でトラフィックをプライベートにルーティングできるようにする、ユーザー作成のネットワーク接続です。ピア接続後、VPC 内の Amazon EC2 インスタンスは、同じネットワーク内にあるかのように ODB ネットワーク内のリソースと通信できます。詳細については、「Oracle Database@AWS で Amazon VPC への ODB ピアリングを設定する」を参照してください。

ステップ 2: Oracle Database@AWS で Oracle Exadata インフラストラクチャを作成する

Oracle Exadata インフラストラクチャは、Oracle Exadata データベースを実行するデータベースサーバー、ストレージサーバー、およびネットワークの基盤となるアーキテクチャです。システムモデルとして Exadata X9M または X11M を選択します。それから、AWS コンソールを使用して、Exadata インフラストラクチャ上に VM クラスターを作成することができます。

Oracle Exadata インフラストラクチャと ODB ネットワークは、どちらの順序でも作成できます。インフラストラクチャの作成時にネットワーク情報を指定する必要はありません。

作成後に Oracle Exadata インフラストラクチャを変更することはできません。Exadata インフラストラクチャを削除するには、「Oracle Database@AWS での Oracle Exadata インフラストラクチャの削除」を参照してください。

Exadata インフラストラクチャを作成するには

1. AWS マネジメントコンソールにサインインして、Oracle Database@AWS コンソール (https://console.aws.amazon.com/odb/) を開きます。

2. 左側のペインで、[Exadata インフラストラクチャ] を選択します。
3. [Exadata インフラストラクチャを作成する] を選択します。
4. [Exadata インフラストラクチャー名] には、名前を入力します。名前は 1～255 文字で、英字またはアンダースコアで始まる必要があります。連続したハイフンを含めることはできません。
5. [アベイラビリティーゾーン] には、サポートされている AZ の 1 つを選択します。次に、[次へ] を選択します。
6. [Exadata システムモデル] で、[Exadata.X9M] または [Exadata.X11M] のいずれかを選択します。[Exadata.X11M] の場合は、次のサーバータイプも選択します。

   - [データベースサーバータイプ] で、Exadata インフラストラクチャのデータベースサーバーモデルタイプを選択します。現在、唯一の選択肢は [X11M] です。
   - [ストレージサーバータイプ] で、Exadata インフラストラクチャのストレージサーバーモデルタイプを選択します。現在、唯一の選択肢は [X11M-HC] です。
7. [データベースサーバー] の場合、デフォルトの 2 のままにするか、スライダーを移動して最大 32 台のサーバーを選択します。2 つ以上を指定するには、OCI の制限の引き上げをリクエストします。

   各 Exadata X9M データベースサーバーは、126 OCPU をサポートしています。各 Exadata X11M データベースサーバーは、760 ECPU をサポートしています。サーバーの数を変更すると、合計コンピューティング数が変わります。OCPU と ECPU の詳細については、Oracle ドキュメントの「Autonomous データベースのコンピューティングモデル」を参照してください。
8. [ストレージサーバー] の場合、デフォルトの 3 のままにするか、スライダーを移動して最大 64 台のサーバーを選択します。3 つ以上を指定するには、OCI の制限の引き上げをリクエストします。各 X9M ストレージサーバーは、64 TB を提供します。各 X11m ストレージサーバーは、80 TB を提供します。サーバーの数を変更すると、ストレージ合計の TB が変わります。続いて、次へを選択します。
9. [メンテナンスウィンドウ] で、システムメンテナンスをいつ実行するかを設定します。

   a. [スケジューリング設定] で、次のいずれかのオプションを選択します。

      - [Oracle が管理するスケジュール] - Oracle がメンテナンスアクティビティに最適な時間を決定します。
      - [カスタマーが管理するスケジュール] - メンテナンスアクティビティをいつ実行できるかをユーザーが指定します。

   b. [パッチ適用モード] では、以下のいずれかのオプションを選択します。

- [ローリング] - 更新は一度に 1 つのノードに適用され、パッチ適用中はデータベースを引き続き使用できます。
- [非ローリング] - 更新はすべてのノードに同時に適用され、ダウンタイムが必要になる場合があります。

c. [カスタマーが管理するスケジュール] を選択した場合、次の追加設定を行います。

- [メンテナンス月数] では、メンテナンスを実行できる月を選択します。
- [その月の週] で、メンテナンスを実行できるその月の週を選択します (第 1 週、第 2 週、第 3 週、第 4 週、または最後の週)。
- [曜日] には、メンテナンスを実行できる日 (月曜日から日曜日) を選択します。
- [開始時間] で、メンテナンスウィンドウが開始される時間を選択します。時間は UTC で表記されます。
- [通知リードタイム] で、今後のメンテナンスについての通知を受け取る日数を選択します。

> **Note**
>
> Oracle Cloud Infrastructure は、このウィンドウ中にシステムメンテナンスを実行します。メンテナンス中、Exadata インフラストラクチャは引き続き使用できますが、短時間、レイテンシーが増大することがあります。

10. (オプション) [OCI メンテナンス通知連絡先] には、最大 10 個の E メールアドレスを入力します。AWS はこれらの E メールアドレスを OCI に転送します。更新が発生すると、OCI は一覧表示されたアドレスに通知を送信します。
11. (オプション) [タグ] には、インフラストラクチャのタグを最大 50 個入力します。タグは、リソースの整理と追跡に使用できるキーと値のペアです。
12. [次へ] を選択し、インフラストラクチャ設定を確認します。
13. [Exadata インフラストラクチャを作成する] を選択します。

ステップ 3: Oracle Database@AWS で Exadata VM クラスターまたは Autonomous VM クラスターを作成する

Exadata VM クラスターは、Oracle Exadata データベースを作成できる一連の VM です。Exadata インフラストラクチャ上に VM クラスターを作成することができます。異なる Oracle Exadata インフラストラクチャを持つ複数の VM クラスターを同じ ODB ネットワークにデプロイできます。Exadata VM クラスターで作成するデータベースに完全な管理制御ができます。

Autonomous VM クラスターは、Oracle Exadata コンピューティングリソースとストレージリソースの事前割り当て済みプールであり、VM レベルで仮想化され、Autonomous データベース (ADB) を実行します。Exadata VM クラスターで作成するユーザー管理型データベースとは異なり、Autonomous データベースは、データベース管理者ではなく Oracle によってセルフチューニング、パッチの適用、管理が行われます。

VM クラスターを作成するときは、次の制限事項を考慮してください。

- VM クラスターは、ODB ネットワークと Oracle Exadata インフラストラクチャを作成した AZ にのみデプロイできます。
- VM クラスターをアカウント間で共有しない場合、Oracle Exadata インフラストラクチャと同じ AWS アカウントにある必要があります。AWS RAM を使用して ODB ネットワークと Oracle Exadata インフラストラクチャを 1 つの AWS アカウントから信頼されたアカウントと共有する場合、信頼されたアカウントは自分のアカウントに VM クラスターを作成できます。
- ODB ネットワークには VM クラスターのみをデプロイできます。他のリソースは許可されていません。
- VM クラスターの作成後は、ストレージ割り当てを変更できません。

> **Important**
>
> VM クラスターのサイズによっては、作成プロセスに 6 時間以上かかる場合があります。

Exadata VM cluster

Exadata VM クラスターを作成するには

1. AWS マネジメントコンソールにサインインして、Oracle Database@AWS コンソール (https://console.aws.amazon.com/odb/) を開きます。

2. 左のペインで、[Exadata VM クラスター] を選択します。
3. [VM クラスターを作成する] を選択します。
4. [VM クラスター名] で、名前を入力します。名前は 1～255 文字で、英字またはアンダースコアで始まる必要があります。連続したハイフンを含めることはできません。
5. (オプション) [グリッドインフラストラクチャクラスター名] には、使用している Oracle Database のバージョンと一致する VM クラスターの Grid インフラストラクチャのバージョンを入力します。名前は 1～11 文字で、ハイフンを含めることはできません。
6. [タイムゾーン] に、タイムゾーンを入力します。
7. [ライセンスオプション] で、[Bring-Your-Own-License (BYOL)] または [ライセンス付属] を選択し、[次へ] を選択します。このライセンスは Oracle が提供する OCI ライセンスであり、AWS が提供するライセンスではありません。
8. Exadata インフラストラクチャ設定を次のように設定します。

   a. [インフラストラクチャ] で、以下を選択します。

      - [Exadata インフラストラクチャー名] で、この VM クラスターに使用するインフラストラクチャを選択します。
      - [グリッド・インフラストラクチャー・バージョン] で、この VM クラスターに使用するバージョンを選択します。
      - [Exadata イメージ バージョン] で、この VM クラスターに使用するバージョンを選択します。表示されている利用可能な最も高いバージョンを選択することをお勧めします。

   b. [データベースサーバー] で、VM クラスターをホストするデータベースサーバーを 1 つ以上選択します。

   c. [設定] で、次を行います。

      - 各 VM に [CPU コア数]、[メモリ]、[ローカルストレージ] を選択するか、デフォルトを受け入れます。
      - VM クラスターの [Exadata ストレージ] の合計量を選択するか、デフォルトを受け入れます。

   d. (オプション) [ストレージ割り当て] で、次のいずれかのオプションを選択します。

      - [Exadata スパーススナップショット用ストレージの割り当てを有効にする]
      - [ローカルバックアップのストレージ割り当てを有効にする]

オプションを選択すると、使用可能なストレージ割り当てが変更されます。このストレージ割り当ては、後で変更することはできません。選択を確認して、[次へ] を選択します。

9. 接続を次のように設定します。

   a. [ODB ネットワーク] で、既存の ODB ネットワークを選択します。

   b. [ホスト名プレフィックス] で、VM クラスターのプレフィックスを入力します。ドメイン名を含んでいないことを確認します。プレフィックスは、Oracle Exadata VM クラスターホスト名の最初の部分になります。

   > **Note**
   >
   > [ホストドメイン名] は [oraclevcn.com] に固定されています。

   c. [リスナーポートをスキャン (TCP/IP)] の場合、単一のクライアントのアクセスネーム (SCAN) リスナーへの TCP アクセス用のポート番号を入力します。デフォルトのポート番号は 15。または、2484、6100、6200、7060、7070、7085、および 7879 を除いた、1024 ~ 8999 の範囲のカスタムポートスキャンを入力します。次に、[次へ] を選択します。

   d. [SSH キーペア] で、VM クラスターへの SSH アクセスに使用される 1 つ以上のキーペアのパブリックキー部分を入力します。次に、[次へ] を選択します。

10. (オプション) 次のように診断とタグを選択します。

    a. [診断イベント]、[ヘルスモニター]、[インシデントログとトレース収集] の診断コレクションを有効にするかどうかを選択します。Oracle はこの診断情報を使用して、問題の特定、追跡、解決を行います。

    b. [タグ] には、VM クラスターに最大 50 個のタグを入力します。タグは、リソースの整理と追跡に使用できるキーと値のペアです。続いて、[Next (次へ)] を選択します。

11. 設定を確認します。次に、[VM クラスターを作成する] を選択します。

Autonomous VM cluster

Autonomous VM クラスターを作成するには

1. AWS マネジメントコンソールにサインインして、Oracle Database@AWS コンソール (https://console.aws.amazon.com/odb/) を開きます。
2. 左のペインで、[Autonomous VM クラスター] を選択します。
3. [Autonomous VM クラスタを作成する] を選択します。
4. [VM クラスター名] で、名前を入力します。名前は 1 ~ 255 文字で、英字またはアンダースコアで始まる必要があります。連続したハイフンを含めることはできません。
5. [タイムゾーン] に、タイムゾーンを入力します。
6. [ライセンスオプション] で、[Bring-Your-Own-License (BYOL)] または [ライセンス付属] を選択し、[次へ] を選択します。このライセンスは Oracle が提供する OCI ライセンスであり、AWS が提供するライセンスではありません。
7. Exadata インフラストラクチャ設定を次のように設定します。
   a. [Exadata インフラストラクチャー名] で、この Autonomous VM クラスターに使用するインフラストラクチャを選択します。
   b. [データベースサーバー] で、Autonomous VM クラスターをホストするデータベースサーバーを 1 つ以上選択します。
   c. [設定] で、次を行います。
      - [VM あたりの ECPU コア数]、[CPU あたりのデータベースメモリ]、[データベースストレージ]、[Autonomous コンテナデータベースの最大数] を選択するか、デフォルトを受け入れます。
      - Autonomous VM クラスターの [Exadata ストレージ] の合計量を選択するか、デフォルトを受け入れます。
8. 接続を次のように設定します。
   a. [ODB ネットワーク] で、既存の ODB ネットワークを選択します。
   b. [リスナーポートをスキャン (TCP/IP)] で、Port のポート番号を入力します (TLS 以外)。デフォルトのポート番号は 15。または、2484、6100、6200、7060、7070、7085、および 7879 を除いた、1024 ~ 8999 の範囲の Port (TLS) を入力します。次に、[次へ] を選択します。

      [相互 TLS (mTLS) 認証を有効化] を選択して、相互 TLS 認証を許可します。

9. (オプション) 次のように診断とタグを選択します。

    a. [Oracle が管理するスケジュール]、または [カスタマーが管理するスケジュール] に変更設定をスケジュールするかどうかを選択します。[カスタマーが管理するスケジュール] を選択した場合、[メンテナンス月数]、[その月の週]、[曜日]、[開始時間 (UTC)] を設定します。

    b. [タグ] には、Autonomous VM クラスターに最大 50 個のタグを入力します。タグは、リソースの整理と追跡に使用できるキーと値のペアです。続いて、[Next (次へ)] を選択します。

10. 設定を確認します。それから、[Autonomous VM クラスタを作成する] を選択します。

ステップ 4: Oracle クラウドインフラストラクチャで Oracle Exadata データベースを作成する

Oracle Database@AWS で、AWS コンソール、CLI、または API を使用して次のリソースを作成し、管理できます。

- ODB ネットワーク
- Oracle Exadata インフラストラクチャ
- Exadata VM クラスターと Autonomous VM クラスター
- ODB ピアリング接続

作成したインフラストラクチャで Oracle Exadata データベースを作成し、管理するには、Oracle Database@AWS ダッシュボードではなく Oracle Cloud Infrastructure コンソールを使用する必要があります。ユーザー管理の Exadata データベースを Exadata VM クラスターに作成し、Autonomous Database を Autonomous Exadata VM クラスターに作成できます。OCI で Oracle データベースを作成する方法については、Oracle Cloud Infrastructure ドキュメントの「Exadata Database」を参照してください。

Oracle Exadata データベースを作成するには

1. AWS マネジメントコンソールにサインインして、Oracle Database@AWS コンソール (https://console.aws.amazon.com/odb/) を開きます。
2. 左側のペインから、[Exadata VM クラスター] または [Autonomous VM クラスター] を選択します。

3. 詳細ページを表示する VM クラスターを選択します。
4. [OCI で管理] を選択し、Oracle Cloud Infrastructure コンソールにリダイレクトされるようにします。
5. OCI でユーザー管理の Exadata データベースまたは Autonomous Database を作成します。

Oracle Database@AWS で Amazon VPC への ODB ピアリングを設定する

ODB ピアリングは、Amazon VPC と ODB ネットワーク間でトラフィックをプライベートにルーティングできるようにする、ユーザー作成のネットワーク接続です。VPC と ODB ネットワークの間には 1 対 1 の関係があります。コンソール、CLI、または API を使用してピアリング接続を作成したら、VPC ルートテーブルを更新し、DNS 解決を設定してください。ODB ピアリングの概念の概要については、「ODB ピアリング」を参照してください。

Oracle Database@AWS での ODB ピアリング接続の作成

ODB ピアリング接続を使用して、Oracle Exadata インフラストラクチャと Amazon VPC で実行されているアプリケーション間のプライベートネットワーク接続を確立できます。各 ODB ピアリング接続は、ODB ネットワークとは別に作成、表示、削除できる個別のリソースです。

ODB ピアリング接続を作成するときに、ピアネットワークの CIDR 範囲を指定できます。この手法により、必要なサブネットへのネットワークアクセスを制限し、攻撃の潜在的なターゲットを減らし、コンプライアンス要件に対して、より詳細なネットワークセグメンテーションができるようになります。

次のタイプの ODB ピアリング接続を作成できます。

同一アカウントの ODB ピアリング

ODB ネットワークと Amazon VPC 間の ODB ピアリング接続は、同じ AWS アカウントで作成できます。

クロスアカウント ODB ピアリング

AWS RAM を使用して ODB ネットワークを共有した後、あるアカウントの ODB ネットワークと別のアカウントの Amazon VPC の間に ODB ピアリング接続を作成できます。VPC 所有者アカウントは、ODB ネットワークを所有することなく、ピアリング接続で指定された CIDR 範囲を管理できます。

VPC と ODB ネットワークの間には 1 対 1 の関係があります。VPC と複数の ODB ネットワーク間、または ODB ネットワークと複数の VPC 間で ODB ピアリング接続を作成することはできません。

コンソール

1. AWS マネジメントコンソールにサインインして、Oracle Database@AWS コンソール (https://console.aws.amazon.com/odb/) を開きます。
2. ナビゲーションペインで、[ODB ピアリング接続] を選択します。
3. [ピアリング接続の作成] を選択します。
4. (オプション) [ODB ピアリング名] には、接続の一意の名前を入力します。
5. [ODB ネットワーク] で、ピアリングする ODB ネットワークを選択します。
6. [ピアネットワーク] で、ODB ネットワークとピア接続する Amazon VPC を選択します。
7. (オプション) [ピアネットワーク CIDR] で、ODB ネットワークにアクセスできるピア VPC から追加の CIDR ブロックを指定します。CIDR を指定しない場合、ピア VPC からのすべての CIDR へのアクセスが許可されます。
8. (オプション) [タグ] で、キーと値のペアを追加します。
9. [ピアリング接続の作成] を選択します。

ODB ピアリング接続を作成した後、ピアリングされた ODB ネットワークにトラフィックをルーティングするように Amazon VPC ルートテーブルを設定します。詳細については、「ODB ピアリング用の VPC ルートテーブルの設定」を参照してください。Oracle Database@AWS は ODB ネットワークルートテーブルを自動的に設定することに注意してください。

AWS CLI

ODB ピアリング接続を作成するには、`create-odb-peering-connection` コマンドを使用します。

```
aws odb create-odb-peering-connection \
    --odb-network-id odbnet-1234567890abcdef \
    --peer-network-id vpc-abcdef1234567890
```

ODB ネットワークへのアクセスを特定の CIDR 範囲に制限するには、`--peer-network-cidrs-to-be-added` パラメータを使用します。CIDR 範囲を指定しない場合、すべての範囲にアクセスできます。

```
aws odb create-odb-peering-connection \
    --odb-network-id odbnet-1234567890abcdef \
    --peer-network-id vpc-abcdef1234567890 \
```

```
    --peer-network-cidrs-to-be-added "10.0.1.0/24,10.0.2.0/24"
```

ODB ピアリング接続を一覧表示するには、list-odb-peering-connections コマンドを使用します。

```
aws odb list-odb-peering-connections
```

特定の ODB ピアリング接続に関する詳細を取得するには、get-odb-peering-connection コマンドを使用します。

```
aws odb get-odb-peering-connection \
    --odb-peering-connection-id odbpcx-1234567890abcdef
```

ODB ピアリング接続の更新

既存の ODB ピアリング接続を更新し、ピアネットワーク CIDR を追加または削除できます。ピア VPC 内のどのサブネットが ODB ネットワークにアクセスできるかを制御します。

コンソール

1. AWS マネジメントコンソールにサインインして、Oracle Database@AWS コンソール (https://console.aws.amazon.com/odb/) を開きます。
2. ナビゲーションペインで、[ODB ピアリング接続] を選択します。
3. 更新する ODB ピアリング接続を選択します。
4. [アクション] を選択し、[ピアリング接続を更新] をクリックします。
5. [ピアネットワーク CIDR] セクションで、必要に応じて CIDR ブロックを追加または削除します。
   - CIDR を追加するには、[CIDR を追加] を選択し、CIDR ブロックを入力します。
   - CIDR を削除するには、削除する CIDR ブロックの横にある [X] を選択します。
6. [ピアリング接続を更新] を選択します。

AWS CLI

ODB ピアリング接続にピアネットワーク CIDR を追加するには、update-odb-peering-connection コマンドで --peer-network-cidrs-to-be-added パラメータを指定します。

```
aws odb update-odb-peering-connection \
```

```
    --odb-peering-connection-id odbpcx-1234567890abcdef \
    --peer-network-cidrs-to-be-added "10.0.1.0/24,10.0.3.0/24"
```

ODB ピアリング接続からピアネットワーク CIDR を削除するには、update-odb-peering-connection コマンドで --peer-network-cidrs-to-be-removed パラメータを指定します。

```
aws odb update-odb-peering-connection \
    --odb-peering-connection-id odbpcx-1234567890abcdef \
    --peer-network-cidrs-to-be-removed "10.0.1.0/24,10.0.3.0/24"
```

ODB ピアリング用の VPC ルートテーブルの設定

ルートテーブルには、サブネットまたはゲートウェイからのネットワークトラフィックの経路を判断する、ルートと呼ばれる一連のルールが含まれます。ルートテーブルの送信先 CIDR は、トラフィックの送信先となる IP アドレスの範囲です。ODB ネットワークへの ODB ピアリング用に VPC を指定した場合、ODB ネットワークの宛先 IP 範囲を使用して VPC ルートテーブルを更新します。ODB ピアリングの詳細については、「ODB ピアリング」を参照してください。

ルートテーブルを更新するには、AWS CLI ec2 create-route コマンドを使用します。次の例では、Amazon VPC ルートテーブルを更新します。詳細については、「ODB ピアリング用の VPC ルートテーブルの設定」を参照してください。

```
aws ec2 create-route \
    --route-table-id rtb-1234567890abcdef \
    --destination-cidr-block 10.0.0.0/16 \
    --odb-network-arn arn:aws:odb:us-east-1:111111111111:odb-network/
odbnet_1234567890abcdef
```

ODB ネットワークのルートテーブルは、VPC CIDR で自動的に更新されます。VPC 内のすべての CIDR ではなく、特定のサブネット CIDR に対してのみ ODB ネットワークへのアクセスを許可するには、ODB ピアリング接続を作成するときにピアネットワーク CIDR を指定するか、既存の ODB ピアリング接続を更新してピアリング CIDR 範囲を追加または削除できます。詳細については、「Oracle Database@AWS での ODB ピアリング接続の作成」および「ODB ピアリング接続の更新」を参照してください。

VPC ルートテーブルの詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「サブネットルートテーブル」および「AWS CLI コマンドリファレンス」の「ec2 create-route」を参照してください。

Oracle Database@AWS の DNS の設定

Amazon Route 53 は、DNS ルーティングに使用できる可用性と拡張性に優れたドメインネームシステム (DNS) のウェブサービスです。ODB ネットワークと VPC の間に ODB ピアリング接続を作成する場合、VPC 内から ODB ネットワークリソースの DNS クエリを解決するメカニズムが必要です。Amazon Route 53 を使用して、以下のリソースを設定できます。

- アウトバウンドエンドポイント

  ODB ネットワークに DNS クエリを送信するのに、エンドポイントが必要です。
- リゾルバールール

  このルールは、Route 53 Resolver が ODB ネットワークの DNS に転送する DNS クエリのドメイン名を指定します。

Oracle Database@AWS での DNS の仕組み

Oracle Database@AWS は、ODB ネットワークのドメインネームシステム (DNS) 設定を自動的に管理します。ドメイン名には、デフォルトのドメイン名 `oraclevcn.com` にカスタムプレフィックスを指定するか、完全なカスタムドメイン名を指定できます。詳細については、「ステップ 1: Oracle Database@AWS で ODB ネットワークを作成する」を参照してください

Oracle Database@AWS が ODB ネットワークをプロビジョニングすると、次のリソースが作成されます。

- ODB ネットワークと同じ CIDR ブロックを持つ Oracle Cloud Infrastructure (OCI) 仮想クラウドネットワーク (VCN)

  この VCN は、お客様のリンクされた OCI テナンシーにあります。ODB ネットワークと OCI VCN の間には 1:1 のマッピングがあります。すべての ODB ネットワークは OCI VCN に関連付けられています。
- OCI VCN 内のプライベート DNS リゾルバー

  この DNS リゾルバーは、OCI VCN 内の DNS クエリを処理します。OCI オートメーションは VM クラスターのレコードを作成します。スキャンは、`*.oraclevcn.com` の完全修飾ドメイン名 (FQDN) を使用します。
- プライベート DNS リゾルバーの OCI VCN 内の DNS リスニングエンドポイント

DNS リスニングエンドポイントは、Oracle Database@AWS コンソールの ODB ネットワークの詳細ページで確認できます。

Oracle Database@AWS の ODB ネットワークでのアウトバウンドエンドポイントの設定

アウトバウンドエンドポイントを使用すると、DNS クエリを VPC からネットワークまたは IP アドレスに送信できます。エンドポイントは、クエリの送信元の IP アドレスを指定します。DNS クエリを VPC から ODB ネットワークに転送するには、Route 53 コンソールを使用してアウトバウンドエンドポイントを作成します。詳細については、「アウトバウンド DNS クエリのネットワークへの転送」を参照してください。

ODB ネットワークのアウトバウンドエンドポイントを設定するには

1. AWS マネジメントコンソール にサインインし、Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. 左のペインで、[アウトバウンドエンドポイント] を選択します。
3. ナビゲーションバーで、アウトバウンドエンドポイントを作成する VPC の [リージョン] を選択します。
4. [Create outbound endpoint (アウトバウンドエンドポイントの作成)] を選択します。
5. [アウトバウンドエンドポイントの全般設定] セクションに、次のように入力します。
   a. 以下へのアウトバウンド TCP および UDP 接続を許可する [セキュリティグループ] を選択します。
      - リゾルバーが ODB ネットワークの DNS クエリに使用する IP アドレス
      - リゾルバーが ODB ネットワークの DNS クエリに使用するポート
   b. [エンドポイントタイプ] で、[IPv4] を選択します。
   c. [このエンドポイントのプロトコル] で、[Do53] を選択します。
6. [IP アドレス] で以下の情報を提供してください。
   - IP アドレスを指定するか、Route 53 Resolver がサブネット内の使用可能なアドレスから IP アドレスを選択できるようにします。DNS クエリには、最小 2 つから最大 6 つの IP アドレスを選択します。少なくとも 2 つの異なるアベイラビリティーゾーンで IP アドレスを選択することをお勧めします。

- [サブネット] で、以下を含むサブネットを選択します。
  - ODB ネットワーク上の DNS リスナーの IP アドレスへのルートを含むルートテーブル
  - IP アドレスとリゾルバーが ODB ネットワークの DNS クエリに使用するポートへの UDP および TCP トラフィックを許可するネットワークアクセスコントロールリスト (ACL)
  - 送信先ポート範囲 1024 ~ 65535 のリゾルバーからのトラフィックを許可するネットワーク ACL

7. (オプション) [タグ] で、エンドポイントのタグを指定します。
8. [Submit] を選択してください。

Oracle Database@AWS でのリゾルバールールの設定

リゾルバールールは、DNS クエリをルーティングする方法を決定する一連の基準です。リゾルバーが ODB ネットワークの DNS に転送する DNS クエリのドメイン名を指定するルールを再利用または作成します。

既存のリゾルバールールの使用

既存のリゾルバールールを使用するのに、アクションはルールのタイプによって異なります。

AWS アカウント の VPC と同じ AWS リージョンにある同じドメインのルール

新しいルールを作成する代わりに、ルールを VPC に関連付けます。ルールダッシュボードからルールを選択し、AWS リージョン内の該当する VPC に関連付けます。

VPC と同じリージョンにあるが、別のアカウントにある同じドメインのルール

AWS Resource Access Manager を使用して、リモートアカウントからアカウントにルールを共有します。ルールを共有するときは、対応するアウトバウンドエンドポイントも共有します。ルールをアカウントと共有した後、ルールダッシュボードからルールを選択し、アカウントの VPC に関連付けます。詳細については、「転送ルールの管理」を参照してください。

新しいリゾルバールールの作成

既存のリゾルバールールを再利用できない場合、Amazon Route 53 コンソールを使用して新しいルールを作成します。

新しいリゾルバールールを作成するには

1. AWS マネジメントコンソール にサインインし、Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. 左のペインで、[ルール] を選択します。
3. ナビゲーションバーで、アウトバウンドエンドポイントが存在する VPC の [リージョン] を選択します。
4. [Create rule] を選択してください。
5. [アウトバウンドトラフィックのルール] セクションを次のように入力します。
   a. [ルールタイプ] で、[転送ルール] を選択します。
   b. [ドメイン名] には、ODB ネットワークから完全なドメイン名を指定します。
   c. [このルールを使用する VPC] で、DNS クエリが ODB ネットワークに転送される VPC に関連付けます。
   d. [アウトバウンドエンドポイント] で、Oracle Database@AWS の ODB ネットワークでのアウトバウンドエンドポイントの設定 で作成したアウトバウンドエンドポイントを選択します。

   > **Note**
   > このルールに関連付けられた VPC は、アウトバウンドエンドポイントを作成したのと同じ VPC である必要はありません。

6. [ターゲット IP アドレス] セクションを次のように入力します。
   a. [IP アドレス] には、ODB ネットワーク上の DNS リスナー IP の IP アドレスを指定します。
   b. [ポート] で、[53] を指定します。これは、リゾルバーが DNS クエリに使用するポートです。

   > **Note**
   > Route 53 Resolver は、このルールに一致する DNS クエリを、このルールに関連付けられた VPC から参照されるアウトバウンドエンドポイントに転送します。これらのクエリは、[ターゲット IP アドレス] で指定したターゲット IP アドレスに転送されます。

c. [伝送プロトコル] で、[Do53] を選択します。

7. (オプション) [タグ] で、ルールのタグを指定します。
8. [Submit] を選択してください。

Oracle Database@AWS の DNS 設定をテストする

アウトバウンドエンドポイントとリゾルバールールを作成した後、DNS が正しく解決することをテストします。アプリケーション VPC で Amazon EC2 インスタンスを使用して、次のように DNS 解決を実行します。

Linux または MacOS の場合

`dig` *`record-name record-type`* の形式のコマンドを使用します。

Windows の場合 –

`nslookup -type=`*`record-name record-type`* の形式のコマンドを使用します。

Oracle Database@AWS の Amazon VPC Transit Gateway の設定

Amazon VPC Transit Gateway は、仮想プライベートクラウド (VPC) とオンプレミスネットワークを相互接続するネットワークの中継ハブです。ハブアンドスポークアーキテクチャの各 VPC は、トランジットゲートウェイに接続して、他の接続VPC にアクセスできます。AWS Transit Gateway は、IPv4 と IPv6 の両方のトラフィックをサポートしています。

Oracle Database@AWS では、ODB ネットワークは 1 つの VPC へのピア接続のみをサポートします。ODB ネットワークにピア接続されている VPC に Transit Gateway を接続する場合は、複数の VPC をこのゲートウェイに接続できます。これら異なる VPC で実行されているアプリケーションは、ODB ネットワークで実行されている Exadata VM クラスターにアクセスできます。

次の図は、2 つの VPC と 1 つのオンプレミスネットワークに接続されているトランジットゲートウェイを示しています。

前述の図では、1 つの VPC が ODB ネットワークにピア接続されています。この設定では、ODB ネットワークはトランジットゲートウェイにアタッチされたすべての VPC にトラフィックをルーティングできます。VPC のそれぞれのルートテーブルには、ローカルルートと、ODB ネットワークを宛先とするトラフィックをトランジットゲートウェイに送信するルートの両方が含まれます。

AWS Transit Gateway では、トランジットゲートウェイへの 1 時間あたりの接続数と、AWS Transit Gateway を経由するトラフィック量に対して課金されます。コストに関する情報については、「AWS Transit Gateway 料金表」を参照してください。

要件

Oracle Database@AWS 環境が以下の要件を満たしていることを確認します。

- ODB ネットワークにピア接続されている VPC は、同じ AWS アカウントにある必要があります。ピア接続された VPC が ODB ネットワークとは異なるアカウントにある場合、Transit Gateway アタッチメントは共有設定に関係なく失敗します。
- ODB ネットワークにピア接続されている VPC には、Transit Gateway アタッチメントが必要です。

> **Note**
>
> トランジットゲートウェイが共有用に設定されている場合、任意のアカウントに存在することができます。したがって、ゲートウェイ自体が VPC および ODB ネットワークと同じアカウントに存在している必要はありません。

- Transit Gateway アタッチメントは、ODB ネットワークと同じアベイラビリティーゾーン (AZ) にある必要があります。

制限

Oracle Database@AWS の Amazon VPC Transit Gateway には以下の制限があることに注意してください。

- Amazon VPC Transit Gateway は、ODB ネットワークをアタッチメントとして使用するネイティブ統合は提供しません。したがって、次のような VPC 機能は利用できません。
  - パブリック DNS ホスト名のプライベート IP アドレスへの解決
  - ODB ネットワークトポロジ、ルーティング、接続ステータスの変更に関するイベント通知
- ODB ネットワークへのマルチキャストトラフィックはサポートされていません。

トランジットゲートウェイのセットアップと設定

Amazon VPC コンソールまたは `aws ec2` コマンドを使用して、トランジットゲートウェイを作成し、設定します。次の手順では、ODB ネットワークが AWS アカウントの VPC にピア接続されていないことを前提としています。ODB ネットワークと VPC がアカウントで既にピアリングされている場合、ステップ 1～3 をスキップします。

> **Note**
>
> VPC のアタッチメントをアタッチまたは再アタッチする場合、必ず CIDR 範囲を ODB ODB ネットワークに再入力します。

Oracle Database@AWS のトランジットゲートウェイをセットアップし設定するには

1. ODB ネットワークを作成します。詳細については、「ステップ 1: Oracle Database@AWS で ODB ネットワークを作成する」を参照してください。
2. ODB ネットワークを含むのと同じアカウントを使用して VPC を作成します。詳細については、「Amazon VPC ユーザーガイド」の「VPC を作成する」を参照してください。
3. ODB ネットワークと VPC の間に ODB ピアリング接続を作成します。詳細については、「Oracle Database@AWS で Amazon VPC への ODB ピアリングを設定する」を参照してください。
4. 「Amazon VPC Transit Gateways の使用を開始する」の手順に従って、トランジットゲートウェイを設定します。ゲートウェイは、ODB ネットワークおよび VPC と同じ AWS アカウントにあるか、別のアカウントによって共有されている必要があります。

   > **Important**
   >
   > ODB ネットワークと同じ AZ に Transit Gateway アタッチメントを作成します。

5. コアネットワークにアタッチする VPC およびオンプレミスネットワークの ODB ネットワークに CIDR 範囲を追加します。詳細については、「Oracle Database@AWS での ODB ネットワークの更新」を参照してください。

   CLI を使用している場合、`--peered-cidrs-to-be-added` と `--peered-cidrs-to-be-removed` と使用して `update-odb-network` コマンドを実行します。詳細については、「AWS CLI Command Reference」を参照してください。

Oracle Database@AWS の AWS Cloud WAN の設定

AWS Cloud WAN は、マネージド型ワイドエリアネットワーク (WAN) サービスです。AWS Cloud WAN を使用して、クラウド環境とオンプレミス環境全体で実行されているリソースを接続する統合グローバルネットワークを構築、管理、モニタリングできます。

AWS Cloud WAN で、グローバルネットワークは、ネットワークオブジェクトの高レベルコンテナとして機能する単一のプライベートネットワークです。コアネットワークは、AWS によって管理されるグローバルネットワークの一部です。

AWS Cloud WAN には、以下のような主な利点があります。

- 複数のリージョンでセキュリティを維持しながら運用を簡素化する一元化されたネットワーク管理
- 複数のルーティングドメインを介してトラフィックを分離するセグメンテーションが組み込まれたコアネットワーク
- ネットワーク管理を自動化し、グローバルネットワーク全体で一貫した設定を定義するポリシーのサポート

Oracle Database@AWS では、ODB ネットワークは 1 つの VPC へのピア接続のみをサポートします。AWS Cloud WAN コアネットワークをピア接続された VPC に接続すると、グローバルトラフィックルーティングが有効になります。複数のリージョンにまたがってアタッチされた VPC 内のアプリケーションは、ODB ネットワーク内の Exadata VM クラスターにアクセスできます。ODB ネットワークトラフィックを独自のセグメントに分離したり、他のセグメントへのアクセスを有効にしたりできます。

次の図は、3 つの VPC と 1 つのオンプレミスネットワークに接続されている AWS Cloud WAN コアネットワークを示しています。

AWS Cloud WAN は、ODB ネットワークをアタッチメントとして使用するネイティブ統合は提供しません。したがって、次のような VPC 機能は利用できません。

- パブリック DNS ホスト名のプライベート IP アドレスへの解決
- ODB ネットワークトポロジ、ルーティング、接続ステータスの変更に関するイベント通知

AWS Cloud WAN では、以下に対して時間単位で課金されます。

- リージョンの数 (コアネットワークエッジ)

- コアネットワークアタッチメントの数
- アタッチメントを介してコアネットワークを経由するトラフィックの量

料金の詳細については、「AWS Cloud WAN の料金表」を参照してください。

Oracle Database@AWS のコアネットワークを設定するには

1. コアネットワークにアタッチする VPC およびオンプレミスネットワークの ODB ネットワークに CIDR 範囲を追加します。詳細については、「Oracle Database@AWS での ODB ネットワークの更新」を参照してください。

   > **Note**
   >
   > VPC のアタッチメントをアタッチまたは再アタッチする場合、必ず CIDR 範囲を ODB ODB ネットワークに再入力します。

2. 「AWS Cloud WAN グローバルネットワークとコアネットワークを作成する」の手順に従います。

Oracle Database@AWS での使用権限の共有

Oracle Database@AWS を使用すると、同じ AWS 組織内の AWS アカウント間で Oracle Database@AWS の AWS Marketplace 使用権限を共有できます。これにより、他のアカウントはサブスクリプションを使用して独自の Oracle Exadata インフラストラクチャと ODB ネットワークリソースをプロビジョニングできます。

共有メソッド

Oracle Database@AWS は、次の 2 つの共有方法をサポートしています。

AWS License Manager による使用権限の共有

- 他のアカウントに独自の Oracle Exadata インフラストラクチャと ODB ネットワークリソースをプロビジョニングする機能を付与します
- 各アカウントは独立して動作し、リソースライフサイクルを完全に制御します
- チームまたはビジネスユニット間でセルフサービスプロビジョニングを有効にするのに最適です

AWS Resource Access Manager (AWS RAM) とのリソース共有

- 既にプロビジョニングされた Oracle Exadata インフラストラクチャと ODB ネットワークリソースを共有します
- 受取人アカウントが VM クラスターを作成できるようにしながら、インフラストラクチャ管理を一元化します
- 複数のアカウントで同じインフラストラクチャを使用することでコストを最適化します

組織のニーズに基づいて、両方の共有方法を同時に使用できます。

Oracle Database@AWS 使用権限共有の制限

Oracle Database@AWS の使用権限を共有するときは、次の制限に注意してください。

- AWS 組織内の AWS アカウントとのみ共有できます。
- 組織単位 (OU) 全体または組織全体と共有することはできません

- アカウントは 1 つの購入者アカウント (1 つのプライベートオファーから) からのみ使用権限を受け取ることができます
- 購入者アカウントは別の購入者アカウントと使用権限を共有することはできません
- 受信者アカウントは、共有使用権限を使用する前に Oracle Database@AWS のサービスを初期化する必要があります
- 使用権限付与オペレーションは、米国東部 (バージニア北部) リージョンからのみ実行できます

アカウント間で Oracle Database@AWS の使用権限を共有する

コストを最適化しながらコラボレーションを有効にするには、Oracle Database@AWS の使用権限を同じ AWS 組織内の他の AWS アカウントと共有します。このトピックでは、AWS License Manager を使用して使用権限を共有する方法について説明します。

使用権限を共有するための前提条件

Oracle Database@AWS の使用権限を共有する前に、以下があることを確認してください。

- アクティブな Oracle Database@AWS サブスクリプション (AWS Marketplace を通じてプライベートオファーを承諾した購入者アカウントである必要があります)
- 使用権限を共有する組織内の AWS アカウントの ID
- AWS License Manager のリソースとオペレーションを使用するために必要なアクセス許可 (詳細については、「AWS License Manager ユーザーガイド」の「License Manager の Identity and Access Management」を参照してください)
- ユーザー (付与者) と使用権限の受取人 (被付与者) に対する以下のアクセス許可

使用権限の共有に必要なアクセス許可

AWS License Manager のアクセス許可に加えて、Oracle Database@AWS には次のアクセス許可が必要です。

付与者のアクセス許可

- `odb:CreateGrantShare`
- `odb:UpdateGrantShare`
- `odb:DeleteGrantShare`

被付与者アクセス許可

- `odb:UpdateGrantShare`
- `odb:DeleteGrantShare`

AWS License Manager を使用して Oracle Database@AWS の使用権限を別のアカウントと共有する

使用権限を別の AWS アカウントと共有するには、AWS License Manager を使用して権限を作成します。詳細については、「AWS License Manager ユーザーガイド」の「License Manager 使用権限の配布」を参照してください。

権限を作成した後、受取人 (被付与者) は以下を行う必要があります。

- 許可を受け入れてアクティブ化します。詳細については、「AWS License Manager ユーザーガイド」の「License Manager での権限の受理とアクティベーション」を参照してください。
- Oracle Database@AWS の初期化手順に従います。

初期化が完了すると、被付与者は共有権限を使用して Oracle Database@AWS リソースをプロビジョニングできます。

Oracle Database@AWS でのリソース共有

Oracle Database@AWS を使用すると、Exadata インフラストラクチャと ODB ネットワークを同じ AWS 組織内の複数の AWS アカウント間で共有できます。これにより、インフラストラクチャを一度プロビジョニングすれば信頼できるアカウント間で再利用できるため、責任を分離しながらコストを削減できます。

リソースを共有する場合:

- リソースを所有するアカウント (所有者アカウント) は、リソースのライフサイクルの制御を維持します。
- 共有リソースへのアクセスを受け取るアカウント (信頼されたアカウント) は、付与されたアクセス許可に基づいて、これらのリソースを表示して使用できます。
- 信頼されたアカウントは、共有インフラストラクチャに独自のリソースを作成できますが、基盤となる共有リソースを削除することはできません。

Oracle Database@AWS と AWS RAM の統合

Oracle Database@AWS は AWS Resource Access Manager (AWS RAM) を使用して、アカウント間でのリソースの安全かつ制御された共有を可能にします。AWS RAM を使用すると、同じ AWS 組織内の複数の AWS アカウント間で Oracle Database@AWS リソースを安全に共有できます。AWS RAM はリソース共有を簡素化し、運用オーバーヘッドを削減し、共有された Oracle Database@AWS リソースのセキュリティと可視性を提供します。

AWS RAM を使用したリソース共有。これにより、自身が所有するリソースを共有できます。リソース共有は、共有するリソースと、それらを共有する AWS アカウントを指定します。

Oracle Database@AWS でのリソース共有の利点

アカウント間で Oracle Database@AWS リソースを共有すると、次の利点があります。

- コスト最適化 – 管理アカウントを通じて高価な Exadata インフラストラクチャを一度プロビジョニングし、複数のアカウントと共有することで、全体的なコストを削減します。
- 責任の分離 – コラボレーションを可能にしながら、インフラストラクチャ管理者とデータベースユーザーの間の明確な境界を維持します。

- 管理の簡素化 – 分散データベースオペレーションを有効にしながら、インフラストラクチャのプロビジョニングと管理を一元化します。
- 一貫したガバナンス – 共有リソース全体に一貫したポリシーとコントロールを適用します。

例えば、管理者は AWS アカウントで Oracle Exadata インフラストラクチャと ODB ネットワークをプロビジョニングし、開発者アカウントと共有できます。開発者は、独自の高価なハードウェアをプロビジョニングすることなく、この共有インフラストラクチャに VM クラスターを作成できます。このアプローチにより、アカウント間の責任の適切な分離を維持しながら、コストを大幅に削減できます。

Oracle Database@AWS でのリソース共有の仕組み

以下の Oracle Database@AWS リソースを共有できます。

- Oracle Exadata インフラストラクチャ
- ODB ネットワーク

Oracle Database@AWS は、次のプロセスを通じて前述のリソースを共有します。

1. 購入者アカウント (AWS Marketplace 経由で Oracle Database@AWS プライベートオファーを受け入れるアカウント) は、Exadata インフラストラクチャや ODB ネットワークなどの Oracle Database@AWS リソースをプロビジョニングします。
2. 購入者アカウントは、AWS RAM を使用してリソース共有を作成し、共有するリソースとそれらを共有する信頼されたアカウントを指定します。
3. 同じ組織内の信頼されたアカウントのリソース共有は自動的に受け入れられます。
4. 共有リソースを使用する前に、信頼されたアカウントは、`aws odb initialize-service` コマンドを使用するか、Oracle Database@AWS コンソールで [アカウントを有効化] を選択して、アカウントの Oracle Database@AWS のサービスを初期化する必要があります。
5. 初期化後、信頼されたアカウントは、共有 Exadata インフラストラクチャ上の VM クラスターや ODB ネットワークなど、共有インフラストラクチャ上に独自のリソースを作成できます。

信頼されたアカウントの共有リソースに対するアクセス許可

リソースを共有すると、Oracle Database@AWS はリソースタイプごとに特定のアクション (管理アクセス許可) を自動的に選択します。

Exadata インフラストラクチャの場合

Oracle Database@AWS は、信頼されたアカウントに次のアクセス許可を付与します。

- odb:CreateCloudVmCluster
- odb:CreateCloudAutonomousVmCluster
- odb:GetCloudExadataInfrastructure
- odb:ListCloudExadataInfrastructures
- odb:GetCloudExadataInfrastructureUnallocatedResources
- odb:ListDbServers
- odb:GetDbServer
- odb:ListCloudVmClusters
- odb:ListCloudAutonomousVmClusters

ODB ネットワークの場合

信頼されたアカウントには、次のアクセス許可が付与されます。

- odb:CreateCloudVmCluster
- odb:CreateCloudAutonomousVmCluster
- odb:GetOdbNetwork
- odb:ListOdbNetworks
- odb:CreateOdbPeeringConnection
- odb:ListOdbPeeringConnections

リソース共有では、Oracle Database@AWS リソースの階層的な性質が尊重されます。例えば、Exadata インフラストラクチャを共有する場合、信頼されたアカウントはこのインフラストラクチャに VM クラスターを作成できますが、Exadata インフラストラクチャ自体を変更または削除することはできません。

リソースが共有解除されると、信頼されたアカウントは共有インフラストラクチャに新しいリソースを作成できなくなります。ただし、作成済みのリソースは引き続きアクセス可能で機能します。

Oracle Database@AWS リソース共有の制限

リソースを共有する前に、次の制限事項に注意してください。

リソース共有に関する制限事項

Oracle Database@AWS リソースを共有するときは、次の制限に注意してください。

- リソースは AWS アカウント ID でのみ共有できます。
- リソースを共有できるのは、同じ AWS 組織内の AWS アカウントのみです。
- 特定の AWS リージョン内でリソースを共有します。リージョン間でリソースを共有するには、リージョンごとに個別のリソース共有を作成する必要があります。
- リソース共有を作成すると、各リソースタイプのアクション (管理アクセス許可) が自動的に選択され、変更することはできません。
- Oracle Database@AWS をリソースとして使用して、他の AWS アカウントと共有することはできません。
- 信頼されたアカウントは、1 つの購入者アカウント (1 つのプライベートオファー) からの共有リソースのみを使用できます。したがって、2 つの購入者アカウントが同じ信頼されたアカウントとリソースを共有することはできません。
- 購入者アカウントは、別の購入者アカウントとリソースを共有できません。
- 信頼されたアカウントと共有されるリソースは、最初に購入者のホームリージョンの購入者アカウントによって共有される必要があります。
- リソースの共有を解除する場合は、同じ信頼できるアカウントで同じリソースを再共有する前に、約 15 分間待つことをお勧めします。

共有リソースの作成と使用に関する制限

Oracle Database@AWS リソースを作成または使用する場合は、次の制限に注意してください。

- 購入者アカウントのみが Exadata インフラストラクチャと ODB ネットワークリソースを作成できます。購入者アカウントは、Oracle Database@AWS プライベートオファーを受け入れるアカウントです。
- 信頼できるアカウントは、購入者アカウントによって共有されている Exadata インフラストラクチャでのみリソースを作成できます。
- 信頼されたアカウントは、共有リソースを使用する前に、アカウントで Oracle Database@AWS のサービスを初期化する必要があります。

共有リソースの削除に関する制限

- 信頼できるアカウントによって作成された VM クラスターを持つ Exadata インフラストラクチャは、それらの VM クラスターが削除されるまで削除できません。
- ODB ピアリング接続が削除されるまで、信頼されたアカウントによって作成された ODB ピアリング接続を持つ ODB ネットワークを削除することはできません。
- 購入者アカウントは、信頼されたアカウントによって作成された Oracle Database@AWS リソースを削除することはできません。
- 信頼されたアカウントは共有リソースを表示できますが、購入者アカウントが所有する Oracle Database@AWS リソースを変更または削除することはできません。

アカウント間で Oracle Database@AWS リソースを共有する

コストを最適化しながらコラボレーションを有効にするには、Oracle Database@AWS リソースを同じ AWS 組織内の他の AWS アカウントと共有します。このトピックでは、AWS Resource Access Manager (AWS RAM) を使用してリソースを共有する方法について説明します。

トピック

リソースを共有するための前提条件

Oracle Database@AWS リソースを共有する前に、以下があることを確認してください。

- アクティブな Oracle Database@AWS サブスクリプション (AWS Marketplace を通じてプライベートオファーを承諾した購入者アカウントである必要があります)
- Exadata インフラストラクチャや ODB ネットワークなど、共有するリソースの ID または名前
- リソースを共有する組織内の AWS アカウントの ID
- AWS RAM でリソース共有を作成するために必要なアクセス許可

- AWS RAM を使用して AWS Organizations とリソースを共有する機能 (詳細については、「AWS Resource Access Manager ユーザーガイド」の「AWS Organizations 内でリソース共有を有効にする」を参照してください)

AWS RAM を使用して Oracle Database@AWS リソースを別のアカウントと共有する

Exadata インフラストラクチャまたは ODB ネットワークを別の AWS アカウントと共有するには、AWS RAM を使用してリソース共有を作成します。これにより、信頼されたアカウントは Exadata インフラストラクチャに VM クラスターを作成できます。

コンソール

1. AWS RAM コンソール (https://console.aws.amazon.com/ram/) を開きます。
2. [リソースの共有の作成] を選択します。
3. [名前] に、リソース共有のわかりやすい名前を入力します。
4. [リソースタイプの選択] で、次のいずれかのリソースを選択します。
   - [Oracle Database@AWS ODB ネットワーク]
   - [Oracle Database@AWS Exadata インフラストラクチャ]
5. 共有する Exadata インフラストラクチャリソースを選択します。[プリンシパルにアクセス権限を付与する] まで、[次へ] を選択します。
6. [プリンシパル] で [AWS アカウント] を選択し、共有する AWS アカウント ID を入力します。
7. [マネージド型アクセス許可] で、次のアクセス許可を選択して、信頼されたアカウントが共有 Exadata インフラストラクチャに VM クラスターを作成できるようにします。
   - AWSRAMDefaultPermissionODBNetwork
   - AWSRAMDefaultPermissionODBCloudExadataInfrastructure
8. [リソースの共有の作成] を選択します。

AWS CLI

AWS CLI を使用してリソースを共有するには、`aws ram create-resource-share` コマンドを使用します。次の例では、指定された Exadata インフラストラクチャをアカウント 222222222222 と共有する `ExadataInfraShare` という名前のリソース共有を作成し、このアカウントが共有インフラストラクチャに VM クラスターを作成できるようにします。

```
aws ram create-resource-share --region us-east-1 \
    --name "ExadataInfraShare" \
    --resource-arns arn:aws:odb:us-east-1:111111111111:cloud-exadata-infrastructure/
exa_infra_1 \
    --principals 222222222222
```

リソース共有の表示

共有したリソースと共有したアカウントを表示するには:

コンソール

1. AWS RAM コンソール (https://console.aws.amazon.com/ram/) を開きます。
2. [共有リソース] を選択して、他のアカウントと共有したリソースを表示します。
3. リソース共有を選択すると、共有されているリソースや共有先のプリンシパルなどの詳細が表示されます。

AWS CLI

AWS CLI を使用してリソース共有を表示するには、get-resource-shares コマンドを使用します。

```
aws ram get-resource-shares --resource-owner SELF
```

特定のリソース共有のリソースを表示するには、list-resources コマンドを使用します。

```
aws ram list-resources \
    --resource-owner SELF \
    --resource-share-arns arn:aws:ram:us-east-1:111111111111:resource-share/12345678-
abcd-1234-efgh-111111111111
```

リソース共有が共有されているプリンシパル (アカウント) を表示するには、list-principals コマンドを使用します。

```
aws ram list-principals \
    --resource-owner SELF \
    --resource-share-arns arn:aws:ram:us-east-1:111111111111:resource-share/12345678-
abcd-1234-efgh-111111111111
```

AWS RAM を使用したリソース共有の更新または削除

AWS RAM を使用して信頼できるアカウントとのリソースの共有を停止するには、次のいずれかのアクションを実行します。

- リソース共有からリソースを削除します。
- リソース共有から信頼されたアカウントを削除します。
- リソース共有を削除します。

共有リソースへのアクセスを取り消したり、共有リソースを削除する前に、次の影響を考慮してください。

- 信頼されたアカウントは、共有されていないインフラストラクチャに新しいリソースを作成できなくなります。
- 共有 Exadata インフラストラクチャで信頼されたアカウントによって作成された既存のリソースは引き続き機能し、それらの AWS アカウントから引き続きアクセスできます。
- 信頼できるアカウントによって作成された VM クラスターを持つ Exadata インフラストラクチャは、それらの VM クラスターが削除されるまで削除できません。

リソースの共有を解除する前に、スムーズに移行できるように信頼されたアカウントと調整することをお勧めします。

詳細については、「AWS Resource Access Manager ユーザーガイド」の「AWS RAM 内でのリソース共有の更新」および「AWS RAM 内のリソース共有の削除」を参照してください。

信頼されたアカウントでの Oracle Database@AWS の初期化

信頼されたアカウントとは、リソース共有を受け取る資格があると指定した AWS アカウントです。AWS 組織内の別の個人の AWS アカウントである必要があります。信頼できるアカウントで共有 Oracle Database@AWS リソースを使用する前に、サービスを初期化する必要があります。初期化により、必要なメタデータが作成され、AWS アカウントと Oracle Cloud Infrastructure 間の接続が確立されます。

トピック

- Oracle Database@AWS 初期化とは
- 次のステップ

Oracle Database@AWS 初期化とは

リソースがアカウントと共有されたら、共有リソースにアクセスしたり使用する前に Oracle Database@AWS のサービスを初期化する必要があります。最初にサービスを初期化せずに Oracle Database@AWS API を使用しようとすると、エラーが発生します。

初期化は 1 回限りのプロセスです。必要なメタデータを作成し、AWS アカウントと Oracle Cloud Infrastructure 間の接続を確立します。

AWS マネジメントコンソールまたは AWS CLI を使用してサービスを初期化できます。

コンソール

1. https://console.aws.amazon.com/odb/ で Oracle Database@AWS コンソールを開きます。
2. このアカウントで Oracle Database@AWS コンソールに初めてアクセスする場合は、ウェルカムページが表示されます。
3. [アカウントを有効化] を選択します。
4. サービス初期化プロセスが開始されます。このプロセスは完了までに数分かかることがあります。
5. [アカウントを有効化] ボタンが [ダッシュボード] ボタンに変わるまで、ウェルカムページを定期的に更新します。
6. [ダッシュボード] を選択して Oracle Database@AWS の使用を開始します。

AWS CLI

AWS CLI を使用して信頼されたアカウントで Oracle Database@AWS を初期化するには、`initialize-service` コマンドを使用します。

```
aws odb initialize-service
```

初期化ステータスを確認するには、`get-oci-onboarding-status` コマンドを使用します。

```
aws odb get-oci-onboarding-status
```

初期化が完了すると、出力に `ACTIVE_LIMITED` のステータスが表示されます。これは、アカウントが共有リソースにアクセスできるものの、新しい Exadata インフラストラクチャまたは ODB ネットワークを作成できないことを示します。

次のステップ

信頼されたアカウントで Oracle Database@AWS を初期化した後、以下を実行できます。

- `list` および `get` コマンドを使用するか、AWS コンソールで共有リソースを表示します。
- 共有 Exadata インフラストラクチャと ODB ネットワーク上に VM クラスターと Autonomous VM クラスターを作成します。
- 共有 ODB ネットワークで ODB ピアリング接続を作成します。

共有リソースの操作の詳細については、「信頼されたアカウントでの共有 Oracle Database@AWS リソースの使用」を参照してください。

信頼されたアカウントでの共有 Oracle Database@AWS リソースの使用

リソースが信頼されたアカウントと共有され、Oracle Database@AWS のサービスを初期化したら、共有リソースを表示して使用できます。このトピックでは、信頼されたアカウントで共有リソースを使用する方法について説明します。

トピック

信頼されたアカウントの共有リソースの制限

共有 Oracle Database@AWS リソースを使用する場合は、次の制限に注意してください。

- リソース共有は、同じ AWS 組織内でのみサポートされます。
- 購入者アカウント (Oracle Database@AWS プライベートオファーを承諾したアカウント) のみが、Exadata インフラストラクチャと ODB ネットワークリソースを作成できます。
- リソースは、必要なアクセス許可がある場合にのみ、共有インフラストラクチャ上でのみ作成できます。

- 各リソースタイプに対する特定のアクション (マネージドアクセス許可) は、リソース共有の作成時に自動的に選択され、変更することはできません。
- 別のアカウントが所有するリソースを変更または削除することはできません。
- 共有インフラストラクチャで作成するリソースは、アカウントによって所有され、OCI クォータにカウントされます。親リソースにも同じことが当てはまります。
- 所有者アカウントがリソースの共有を解除すると、この共有インフラストラクチャ上に新しいリソースを作成できなくなります。ただし、既存のリソースは引き続き機能します。
- クロスリージョンのリソース共有はサポートされていません。リソースは同じ AWS リージョン内でのみ共有できます。
- 信頼されたアカウントのリソースは、Oracle Database@AWS サブスクリプションの購入者に請求されます。
- 共有されているリソースを使用する場合は、Amazon リソースネーム (ARN) を指定する必要があります。

共有 Exadata インフラストラクチャ上に VM クラスターを作成する

信頼されたアカウントが共有 Exadata インフラストラクチャと ODB ネットワークにアクセスできる場合は、このインフラストラクチャ上に Exadata VM クラスター、Autonomous VM クラスター、または ODB ピアリングを作成できます。

> **Note**
>
> 共有されているリソースを使用する場合は、リソース ID のみを指定するのではなく、Amazon リソースネーム (ARN) を指定する必要があります。

コンソール

1. https://console.aws.amazon.com/odb/ で Oracle Database@AWS コンソールを開きます。
2. ナビゲーションペインで、[Exadata VM クラスター] または [Autonomous VM クラスター] を選択します。
3. [VM クラスターを作成する] または [Autonomous VM クラスターを作成する] を選択します。
4. [Exadata インフラストラクチャ] の場合は、VM クラスターを作成する共有 Exadata インフラストラクチャを選択します。
5. VM クラスターの設定に応じて、残りのフィールドに入力します。

6. [VM クラスターを作成する] または [Autonomous VM クラスターを作成する] を選択します。

AWS CLI

AWS CLI を使用して共有 Exadata インフラストラクチャに VM クラスターを作成するには、`create-cloud-vm-cluster` コマンドを使用します。

```
aws odb create-cloud-vm-cluster --region us-east-1 \
    --cloud-exadata-infrastructure-id arn:aws:odb:us-east-1:111111111111:cloud-exadata-infrastructure/exa_aaaaaaaaaa \
    --odb-network-id arn:aws:odb:us-east-1:111111111111:odb-network/odbnet_aaaaaaaaaa \
    --cpu-core-count 4 \
    --display-name "Shared-VMC-1" \
    --gi-version "19.0.0.0" \
    --hostname "vmchost" \
    --ssh-public-keys "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQ..." \
```

AWS CLI を使用して共有 Exadata インフラストラクチャに Autonomous VM クラスターを作成するには、`create-cloud-vm-cluster` コマンドを使用します。

```
aws odb create-cloud-autonomous-vm-cluster --region us-east-1  \
    --cloud-exadata-infrastructure-id arn:aws:odb:us-east-1:111111111111:cloud-exadata-infrastructure/exa_aaaaaaaaaa \
    --odb-network-id arn:aws:odb:us-east-1:111111111111:odb-network/odbnet_aaaaaaaaaa\
    --display-name "Shared-AVMC-1" \
    --autonomous-data-storage-size-in-tbs 8 \
    --cpu-core-count-per-node 16
```

VM クラスターは、指定された共有 Exadata インフラストラクチャ上に作成され、信頼されたアカウントによって所有されます。

信頼されたアカウントの共有リソースの表示

アカウントと共有されているリソースは、AWS マネジメントコンソールまたは AWS CLI を使用して表示できます。

コンソール

1. https://console.aws.amazon.com/odb/ で Oracle Database@AWS コンソールを開きます。

2. ナビゲーションペインで、表示するリソースタイプを選択します。[Exadata インフラストラクチャ] または [ODB ネットワーク]。
3. コンソールには、共有されているリソースが表示されます。
4. 共有リソースを選択すると、その詳細が表示されます。

AWS CLI

AWS CLI を使用して共有リソースを表示するには、リソースタイプに適した `list` コマンドを使用します。例えば、Exadata インフラストラクチャを一覧表示するには、次のようにします。

```
aws odb list-cloud-exadata-infrastructures
```

レスポンスには、共有されているリソースが表示されます。

特定の共有リソースに関する詳細情報を取得するには、リソース ID を指定した適切な `get` コマンドを使用します。

```
aws odb get-cloud-exadata-infrastructure --cloud-exadata-infrastructure-id exa_infra_1
```

共有 ODB ネットワークでの ODB ピアリングの設定

共有 ODB ネットワーク上のアプリケーションとデータベース間の通信を有効にするには、VPC と共有 ODB ネットワーク間に ODB ピアリングを設定します。ODB ピアリングの詳細については、「Oracle Database@AWS での ODB ピアリング接続の作成」を参照してください。

コンソール

1. https://console.aws.amazon.com/odb/ で Oracle Database@AWS コンソールを開きます。
2. ナビゲーションペインで、[ODB ピアリング] を選択します。
3. [ODB ネットワークピアリングの作成] を選択します。
4. [ODB ネットワーク] の場合は、ピアリングする共有 ODB ネットワークを選択します。
5. [ピアネットワーク] で、VPC を選択します。
6. [ODB ネットワークピアリングの作成] を選択します。

AWS CLI

AWS CLI を使用して VPC と共有 ODB ネットワーク間にネットワークピアリング接続を作成するには、`create-odb-peering-connection` コマンドを使用します。

```
aws odb create-odb-peering-connection \
    --odb-network-id odbnet_1234567890abcdef \
    --peer-network-id vpc-abcdef1234567890
```

ピアリング接続を作成したら、ルートテーブルを更新してピアリングネットワーク間のトラフィックを有効にします。

```
aws ec2 create-route \
    --route-table-id rtb-1234567890abcdef \
    --destination-cidr-block 10.0.0.0/16 \
    --odb-network-arn arn:aws:odb:us-east-1:111111111111:odb-network/
odbnet_1234567890abcdef
```

Oracle Database@AWS の管理

一部の Oracle Database@AWS リソースは、作成後に変更および削除できます。

Oracle Database@AWS での ODB ネットワークの更新

次の ODB ネットワークリソースを更新できます。

- ODB ネットワーク名
- ODB ネットワークへの ODB ピアリング接続を確立するために使用する Amazon VPC
- ODB ネットワーク内の Exadata リソースにアクセスできる VPC CIDR 範囲

> **Note**
>
> CIDR 範囲を指定することで、VPC 全体を ODB ネットワークで使用できるようにするのではなく、必要な VPC サブネットへの接続を制限できます。

このセクションでは、ステップ 1: Oracle Database@AWS で ODB ネットワークを作成する で既に ODB ネットワークを作成していることを前提としています。

ODB ネットワークを更新するには

1. AWS マネジメントコンソールにサインインして、Oracle Database@AWS コンソール (https://console.aws.amazon.com/odb/) を開きます。
2. 左側のペインから、[ODB ネットワーク] を選択します。
3. 変更するネットワークを選択します。
4. [Modify] (変更) を選択します。
5. (オプション) [ODB ネットワーク名] に新しいネットワーク名を入力します。名前は 1～255 文字で、英字またはアンダースコアで始まる必要があります。連続したハイフンを含めることはできません。
6. (オプション) [ピアード CIDR] の場合、ODB ネットワークへの接続を必要とするピアリング接続された VPC からの CIDR 範囲を指定します。アクセスを制限するには、必要最小限の CIDR 範囲を指定することをお勧めします。
7. (オプション) [サービス統合を設定] では、[Amazon S3] または [ゼロ ETL] を選択または選択解除します。

8. [続行] を選択し、[修正] を選択します。

Oracle Database@AWS での ODB ネットワークの削除

ODB ネットワークを削除できます。このセクションでは、ステップ 1: Oracle Database@AWS で ODB ネットワークを作成する で既に ODB ネットワークを作成していることを前提としています。VM クラスターで現在使用されている ODB ネットワークを削除することはできません。

ODB ネットワークを削除するには

1. AWS マネジメントコンソールにサインインして、Oracle Database@AWS コンソール (https://console.aws.amazon.com/odb/) を開きます。
2. 左側のペインから、[ODB ネットワーク] を選択します。
3. 削除するネットワークを選択します。
4. [削除] を選択します。
5. (オプション) [関連する OCI リソースを削除] を選択して、ODB ネットワークとともに作成された OCI リソースを削除します。
6. テキストボックスに「**`delete me`**」と入力します。
7. [削除] を選択します。

Oracle Database@AWS での VM クラスターの削除

Exadata VM クラスターまたは Autonomous VM クラスターを削除できます。このセクションでは、ステップ 3: Oracle Database@AWS で Exadata VM クラスターまたは Autonomous VM クラスターを作成する で VM クラスターが既に作成されていることを前提としています。

VM クラスターを削除するには

1. AWS マネジメントコンソールにサインインして、Oracle Database@AWS コンソール (https://console.aws.amazon.com/odb/) を開きます。
2. 左側のペインから、[Exadata VM クラスター] または [Autonomous VM クラスター] を選択します。
3. 削除する VM クラスターを選択します。
4. [削除] を選択します。
5. 確認を求めるメッセージが表示されたら、**`delete me`** と入力し、[削除] を選択してください。

Oracle Database@AWS での Oracle Exadata インフラストラクチャの削除

Oracle Exadata インフラストラクチャを削除できます。このセクションでは、ステップ 2: Oracle Database@AWS で Oracle Exadata インフラストラクチャを作成する で Oracle Exadata インフラストラクチャを既に作成していることを前提としています。VM クラスターで現在使用されている Exadata インフラストラクチャは削除できません。

Oracle Exadata インフラストラクチャを削除するには

1. AWS マネジメントコンソールにサインインして、Oracle Database@AWS コンソール (https://console.aws.amazon.com/odb/) を開きます。
2. 左側のペインで、[Exadata インフラストラクチャ] を選択します。
3. 削除する Exadata インフラストラクチャを選択します。
4. [削除] を選択します。
5. 確認を求めるメッセージが表示されたら、**`delete me`** と入力し、[削除] を選択してください。

ODB ピアリング接続の削除

ODB ピアリング接続が不要になった場合には、それを削除することができます。ODB ネットワークを削除する前に、すべての ODB ピアリング接続を削除する必要があります。

コンソール

1. AWS マネジメントコンソールにサインインして、Oracle Database@AWS コンソール (https://console.aws.amazon.com/odb/) を開きます。
2. ナビゲーションペインで、[ODB ピアリング接続] を選択します。
3. 削除する ODB ピアリング接続を選択します。
4. [削除] を選択します。
5. 削除を確認するには **`delete me`** と入力して、[削除] を選択します。

AWS CLI

ODB ピアリング接続を削除するには、`delete-odb-peering-connection` コマンドを使用します。

```
aws odb delete-odb-peering-connection \
    --odb-peering-connection-id odbpcx-1234567890abcdef
```

Oracle Database@AWS でのバックアップ

Oracle Database@AWS には、Oracle データベースを保護するための複数のバックアップオプションが用意されています。Amazon S3 とシームレスに統合する Oracle マネージドバックアップを使用するか、Oracle Recovery Manager (RMAN) を使用して独自のユーザー管理のバックアップを作成できます。

Amazon S3 への Oracle マネージドバックアップ

ODB ネットワークを作成すると、Oracle Database@AWS は Amazon S3 への Oracle マネージドバックアップのネットワークアクセスを自動的に設定します。OCI は、必要な DNS エントリとセキュリティリストを設定します。これらの設定により、OCI Virtual Cloud Network (VCN) と Amazon S3 間のトラフィックが許可されます。ODB ネットワークでは自動バックアップは有効化も制御もされません。

Oracle マネージドバックアップは OCI によって完全に管理されます。Oracle Exadata データベースを作成するときは、OCI コンソールで [自動バックアップの有効化] を選択して、自動バックアップを有効にできます。以下のいずれかのバックアップ先を選択します。

- Amazon S3
- OCI Object Storage
- Autonomous Recovery Service

詳細については、OCI ドキュメントの「Backup Exadata Database」を参照してください。

Oracle Database@AWS での Amazon S3 へのユーザー管理のバックアップ

Oracle Database@AWS では、専用インフラストラクチャ上の Exadata Database Service を使用して、データベースのユーザー管理のバックアップを作成できます。Oracle Recovery Manager (RMAN) を使用してデータをバックアップし、Amazon S3 バケットに保存します。Oracle Database@AWS のマネージドサービスの利点を維持しながら、バックアップのスケジュール、保持ポリシー、ストレージコストを完全に制御できます。

> **Note**
>
> Oracle Database@AWS は、専用インフラストラクチャ上の Autonomous データベースのユーザー管理のバックアップをサポートしていません。

ユーザー管理のバックアップは、Oracle Database@AWS が提供する AWS マネージドバックアップソリューションを補完します。コンプライアンス要件、クロスリージョンディザスタリカバリ、または既存のバックアップ管理ワークフローとの統合のために手動バックアップを使用できます。

次のユーザー管理のバックアップ手法を使用できます。

Oracle Secure Backup

最適なパフォーマンスで Amazon S3 に直接バックアップをストリーミングします。

Storage Gateway

Storage Gateway は、NFS 共有を使用するファイルベースのバックアップに使用します。

S3 マウントポイント

ファイルクライアントを使用して、Amazon S3 バケットをローカルファイルシステムとしてマウントします。

Oracle Database@AWS の Amazon S3 へのユーザー管理のバックアップの前提条件

Oracle Exadata データベースを Amazon S3 にバックアップする前に、次の操作を行います。

1. ODB ネットワークから Amazon S3 への直接アクセスを有効にします。
2. Oracle Database@AWS と Amazon S3 間のネットワーク接続とルーティングを設定します。

ODB ネットワークから Amazon S3 へのアクセスを有効にする

データベースを手動で Amazon S3 にバックアップするには、ODB ネットワークから S3 への直接アクセスを有効にします。この手法により、データベースはデータのインポート/エクスポートやユーザー管理のバックアップなどのビジネスニーズに合わせて Amazon S3 にアクセスできます。バックアップストレージのターゲット先を完全に制御でき、ポリシーを使用して VPC Lattice を使用した Amazon S3 へのアクセスを制限できます。

ODB ネットワークからの Amazon S3 への直接アクセスは、デフォルトでは有効になっていません。ODB ネットワークを作成または変更するときに S3 アクセスを有効にできます。

コンソール

ODB ネットワークから Amazon S3 への直接アクセスを有効にするには

1. https://console.aws.amazon.com/odb/ で Oracle Database@AWS コンソールを開きます。
2. ナビゲーションペインで [ODB ネットワーク] を選択します。
3. Amazon S3 アクセスを有効にする ODB ネットワークを選択します。
4. [Modify] (変更) を選択します。
5. [Amazon S3] を選択します。
6. (オプション) Amazon S3 ポリシードキュメントを設定してAmazon S3へのアクセスを制御します。ポリシーを指定しない場合、デフォルトのポリシーによってフルアクセスが付与されます。
7. [続行] を選択してから、[修正] を選択します。

AWS CLI

ODB ネットワークから Amazon S3 への直接アクセスを有効にするには、`s3-access` パラメータを指定して `update-odb-network` コマンドを使用します。

```
aws odb update-odb-network \
  --odb-network-id odb-network-id \
  --s3-access ENABLED
```

Amazon S3 ポリシードキュメントを設定するには、`--s3-policy-document` パラメータを使用します。

```
aws odb update-odb-network \
  --odb-network-id odb-network-id \
  --s3-policy-document file://s3-policy.json
```

Amazon S3 アクセスを有効にすると、リージョン DNS `s3.region.amazonaws.com` を使用して ODB ネットワークから Amazon S3 にアクセスできます。OCI はこの DNS 名をデフォルトに設定します。カスタム DNS 名を使用するには、カスタム DNS がサービスネットワークエンドポイントの IP アドレスに解決されるように VCN DNS を変更します。

Oracle Database@AWS と Amazon S3 間のネットワーク接続の設定

Amazon S3 へのユーザー管理のバックアップを許可するには、VM が S3 Amazon VPC エンドポイントにアクセスできる必要があります。OCI コンソールでは、ネットワークセキュリティグループ (NSG) のセキュリティルールを編集して、入出力トラフィックを制御できます。ユーザー管理のバックアップの場合、トラフィックはバックアップサブネットではなくクライアントサブネットを経由します。次の手順では、クライアントサブネットの NSG を更新して、VPC エンドポイント IP アドレスの出力ルールを追加します。

VM に Amazon S3 エンドポイントへのアクセスを許可するには

1. https://console.aws.amazon.com/odb/ で Oracle Database@AWS コンソールを開きます。
2. [ODB ネットワーク] を選択します。
3. ODB ネットワークの名前を選択します。
4. [OCIリソース] を選択します。
5. [サービスの統合] タブを選択します。
6. [Amazon S3] では、以下の情報をメモしておきます。
   - Amazon VPC S3 エンドポイントの IPv4 アドレス。この情報は後で必要になります。例えば、IP アドレスは `192.168.12.223` のようになります。
   - Amazon VPC S3 エンドポイントのドメイン名。この情報は後で必要になります。例えば、ドメイン名は `s3.us-east-1.amazonaws.com` のようになります。
7. 左側のナビゲーションペインで、[Exadata VM クラスター] を選択し、[VM クラスター名] を選択します。
8. ページの上部で、[概要] タブを選択します。
9. [仮想マシン] を選択し、VM の名前を選択します。
10. [DNS 名] の値をメモしておきます。これは、`ssh` を使用して VM に接続するときに指定するホスト名です。
11. 右上で、[OCI で管理] を選択します。これにより、OCI コンソールが開きます。
12. [仮想クラウドネットワーク] リストページで、ODB ネットワーククライアントサブネット (`exa_static_nsg`) のネットワークセキュリティグループ (NSG) を含む VCN を選択します。詳細については、OCI ドキュメントの「Managing Security Rules for an NSG」を参照してください。
13. 詳細ページで、表示されるオプションに応じて、次のいずれかのアクションを実行します。

- [セキュリティ] タブで、[ネットワークセキュリティグループ] に移動します。
- [リソース] で、[ネットワークセキュリティグループ] を選択します。

14. クライアントサブネットの NSG を選択します (exa_static_nsg)。
15. 前にメモした VPC エンドポイントアドレスの Egress ルールを追加します。

VM から S3 への接続をテストするには

1. ssh を使用して、以前に取得した DNS 名を持つ VM に root として接続します。接続するときに、SSH キーを含む .pem ファイルを指定します。
2. 次のコマンドを実行して、VM が Amazon S3 Amazon VPC エンドポイントにアクセスできることを確認します。前にメモしておいた S3 ドメイン名を使用します。

```
# nslookup s3.us-east-1.amazonaws.com
# curl -v https://s3.us-east-1.amazonaws.com/
# aws s3 ls --endpoint-url https://s3.us-east-1.amazonaws.com
```

Oracle Secure Backup を使用して Amazon S3 にバックアップする

Oracle Secure Backup は、Recovery Manager (RMAN) で使用する SBT インターフェイスとして機能します。RMAN と Oracle Secure Backup を使用して、Oracle Database@AWS データベースを Amazon S3 に直接バックアップできます。Oracle Secure Backup には次の利点があります。

- Oracle Secure Backup は、RMAN と S3 間のデータ転送を最適化します。
- 中間バックアップストレージは必要ありません。
- Oracle Secure Backup は、バックアップメディアのライフサイクルを管理します。

Oracle Secure Backup を使用して Amazon S3 にバックアップするには

1. Exadata VM サーバーに Oracle Secure Backup モジュールをインストールします。プレースホルダーの値を AWS アクセスキーとシークレットアクセスキーに置き換えます。詳細については、Oracle のドキュメントの「Backup to Cloud with Oracle Secure Backup Cloud Module」を参照してください。

```
cd $ORACLE_HOME/lib
```

```
java -jar osbws_install.jar -AWSID aws-access-key-id -AWSKey aws-secret-access-
key -walletDir $ORACLE_HOME/dbs/osbws_wallet -location us-west-2 -useHttps -
awsEndPoint s3.us-west-2.amazonaws.com
```

2. RMAN に接続し、バックアップチャネルとデフォルトのデバイスタイプを設定します。

```
RMAN target /
RMAN> CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' PARMS 'SBT_LIBRARY=/u02/app/oracle/
product/19.0.0.0/dbhome_2/lib/libosbws.so, ENV=(OSB_WS_PFILE=/u02/app/oracle/
product/19.0.0.0/dbhome_2/dbs/osbwssmalikdb1.ora)';
RMAN> CONFIGURE DEFAULT DEVICE TYPE TO 'SBT_TAPE';
```

3. 設定を確認します。

```
RMAN> SHOW ALL;
```

4. データベースをバックアップします。

```
RMAN> BACKUP DATABASE;
```

5. バックアップが正常に完了したことを確認します。

```
RMAN> LIST BACKUP OF DATABASE SUMMARY;
```

Amazon EC2 で AWS Storage Gateway を使用して Amazon S3 にバックアップする

AWS Storage Gateway は、オンプレミス環境を AWS クラウドストレージサービスに接続するハイブリッドサービスです。Oracle Database@AWS のバックアップの場合、Storage Gateway を使用して、Amazon S3 に直接書き込むファイルベースのバックアップワークフローを作成できます。Oracle Secure Backup 手法とは異なり、バックアップのライフサイクルを管理します。

このソリューションでは、Storage Gateway を設定するための個別の Amazon EC2 インスタンスを作成します。また、Amazon EBS ボリュームを追加して、Amazon S3 への読み取りと書き込みをキャッシュします。

この手法には次の利点があります:

- Oracle Secure Backup などのメディアマネージャーは必要ありません。
- 中間バックアップストレージは必要ありません。

Storage Gateway をデプロイしてファイル共有を作成するには

1. https://console.aws.amazon.com/storagegateway/home/ AWS マネジメントコンソールを開き、ゲートウェイを作成する AWS リージョンを選択します。
2. Amazon EC2 インスタンスをハブとして使用して、Amazon S3 ファイルゲートウェイをデプロイしてアクティブ化します。「Storage Gateway ユーザーガイド」の「S3 ファイルゲートウェイ用にカスタマイズされた Amazon EC2 ホストをデプロイする」の手順に従います。

   ファイルゲートウェイを設定するときは、以下を実行してください。

   - キャッシュストレージ用に、サイズが 150 GiB 以上の Amazon EBS ボリュームを少なくとも 1 つ追加します。
   - セキュリティグループの NFS アクセス用に TCP/UDP ポート 2049 を開きます。これにより、NFS ファイル共有を作成できます。
   - ゲートウェイのアクティブ化中に 1 回限りの HTTP アクセスを許可するために、インバウンドトラフィック用に TCP ポート 80 を開きます。このポートは、アクティブ化の後で閉じることができます。
3. ODB ネットワークと Storage Gateway 間のプライベート接続用の Amazon VPC エンドポイントを作成します。詳細については、「インターフェイス VPC エンドポイントを使用して AWS サービスにアクセスする」を参照してください。
4. Storage Gateway コンソールを使用して Amazon S3 バケットのファイル共有を作成します。詳細については、「ファイル共有の作成」を参照してください。

Storage Gateway を使用してデータベースを Amazon S3 にバックアップするには

1. ターミナルで、ssh を使用して Exadata VM の DNS 名に接続します。DNS 名を見つけるには、「Oracle Database@AWS の Amazon S3 へのユーザー管理のバックアップの前提条件」を参照してください。
2. NFS マウント用のディレクトリを Exadata VM クラスターサーバーに作成します。例えば、次の例では /home/oracle/sgw_mount/ ディレクトリを作成します。

   ```
   mkdir /home/oracle/sgw_mount/
   ```
3. 作成したディレクトリに NFS 共有をマウントします。次の例では、ディレクトリ /home/oracle/sgw_mount/ に共有を作成します。*SG-IP-address* を Storage Gateway の IP アドレスに置き換え、*your-bucket-name* を S3 バケットの名前に置き換えます。

```
sudo mount -t nfs -o nolock,hard SG-IP-address:/your-bucket-name /home/oracle/
sgw_mount/
```

4. RMAN に接続し、マウントされたディレクトリにデータベースをバックアップします。次の例では、チャネル rman_local_bkp を作成し、マウントポイントパスを使用してバックアップピースをフォーマットします。

```
$ rman TARGET /
RMAN> ALLOCATE CHANNEL rman_local_bkp DEVICE TYPE DISK;
RMAN> BACKUP FORMAT '/home/oracle/sgw_mount/%U' DATABASE;
```

5. バックアップファイルがマウントディレクトリに作成されていることを確認します。次の例は、2 つのバックアップピースを示しています。

```
$ ls -lart /home/oracle/sgw_mount/
total 8569632
-rw-r----- 1 oracle asmdba 1112223334 Jul 10 20:51 1a2b34cd_1234_1_1
drwxrwxrwx 1 nobody nobody 0 Jul 10 20:56 .
-rw-r----- 1 oracle asmdba 5556667778 Jul 10 20:56 1a2b34cd_1235_1_1
```

S3 マウントポイントを使用して Amazon S3 にバックアップする

Amazon S3 マウントポイントを使用して、最初にローカルにバックアップを作成し、次にそれを Amazon S3 にコピーできます。この手法では、ローカルストレージにバックアップを作成し、マウントポイントインターフェイスを使用して Amazon S3 に転送します。データを 2 回バックアップする必要があるため、バックアップ時間は他の手法よりも長くなります。

> **Note**
>
> ステージングなしでマウントポイントを使用して Amazon S3 に直接バックアップすることはサポートされていません。RMAN には、Amazon S3 マウントポイントインターフェイスと互換性のない特定のファイルシステムのアクセス許可が必要です。

この手法では、Oracle Secure Backup などのメディアマネージャーのライセンスを取得する必要はありません。バックアップのライフサイクルを管理します。

S3 マウントポイントを使用して Amazon S3 にバックアップするには

1. ターミナルで、ssh を使用して Exadata VM の DNS 名に接続します。DNS 名を見つけるには、「Oracle Database@AWS の Amazon S3 へのユーザー管理のバックアップの前提条件」を参照してください。
2. Exadata VM クラスターサーバーに Amazon S3 マウントポイントをインストールします。インストールと設定の詳細については、「Amazon S3 ユーザーガイド」の「Mountpoint for Amazon S3」を参照してください。

```
$ sudo yum install ./mount-s3.rpm
```

3. mount-s3 コマンドを実行してインストールを確認します。

```
$ mount-s3 --version
mount-s3 1.19.0
```

4. Exadata VM クラスターサーバーのローカルストレージに中間バックアップディレクトリを作成します。データベースをこのローカルディレクトリにバックアップし、バックアップを S3 バケットにコピーします。次の例では、ディレクトリ /u02/rman_bkp_local を作成します。

```
mkdir /u02/rman_bkp_local
```

5. Amazon S3 マウントポイント用のディレクトリを作成します。次の例では、ディレクトリ /home/oracle/s3mount を作成します。

```
$ mkdir /home/oracle/s3mount
```

6. マウントポイントを使用して Amazon S3 バケットをマウントします。次の例では、ディレクトリ /home/oracle/s3mount に S3 バケットをマウントします。*your-s3-bucket-name* を実際の Amazon S3 バケット名に置き換えます。

```
$ mount-s3 s3://your-s3-bucket-name /home/oracle/s3mount
```

7. Amazon S3 バケットの内容にアクセスできることを確認します。

```
$ ls -lart /home/oracle/s3mount
```

8. RMAN をターゲットデータベースに接続し、ローカルステージングディレクトリにバックアップします。次の例では、チャネル rman_local_bkp を作成し、パス /u02/rman_bkp_local/ を使用してバックアップピースをフォーマットします。

```
$ rman TARGET /

RMAN> ALLOCATE CHANNEL rman_local_bkp DEVICE TYPE DISK;
RMAN> BACKUP FORMAT '/u02/rman_bkp_local/%U' DATABASE;
```

9. バックアップがローカルディレクトリに作成されたことを確認します。

```
$ cd /u02/rman_bkp_local/
$ ls -lart
total 4252128
drwxr-xr-x 8 oracle oinstall 4096 Jul 10 02:13 ..
-rw-r----- 1 oracle asmdba 1112223334 Jul 10 02:13 abcd1234_1921_1_1
drwxr-xr-x 2 oracle oinstall 4096 Jul 10 02:13 .
-rw-r----- 1 oracle asmdba 5556667778 Jul 10 02:14 abcd1234_1922_1_1
```

10. バックアップファイルをローカルステージングディレクトリから Amazon S3 マウントポイントにコピーします。

```
cp /u02/rman_bkp_local/* /home/oracle/s3mount/
```

11. ファイルが Amazon S3 に正常にコピーされたことを確認します。

```
$ ls -lart /home/oracle/s3mount/
total 4252112
drwx------ 6 oracle oinstall 225 Jul 10 02:09 ..
drwxr-xr-x 2 oracle oinstall 0 Jul 10 02:24 .
-rw-r--r-- 1 oracle oinstall 1112223334 Jul 10 02:24 abcd1234_1921_1_1
-rw-r--r-- 1 oracle oinstall 5556667778 Jul 10 02:24 abcd1234_1922_1_1
```

Amazon S3 への直接アクセスの無効化

ODB ネットワークから Amazon S3 に直接アクセスする必要がなくなった場合は、無効にできます。S3 への直接ネットワークアクセスを有効または無効にしても、Amazon S3 への Oracle マネージドバックアップのネットワークアクセスには影響しません。

コンソール

Amazon S3 への直接アクセスを無効にするには

1. https://console.aws.amazon.com/odb/ で Oracle Database@AWS コンソールを開きます。

2. ナビゲーションペインで [ODB ネットワーク] を選択します。
3. Amazon S3 アクセスを無効にする ODB ネットワークを選択します。
4. [Modify] (変更) を選択します。
5. [S3 アクセスを有効にする] チェックボックスをオフにします。
6. [ODB ネットワークを変更する] を選択します。

AWS CLI

`s3-access` パラメータを指定して、`update-odb-network` コマンドを使用します。

```
aws odb update-odb-network \
  --odb-network-id odb-network-id \
  --s3-access DISABLED
```

Amazon S3 統合のトラブルシューティング

Amazon S3 への Oracle マネージドバックアップまたは Amazon S3 への直接アクセスで問題が発生した場合は、次のトラブルシューティング手順を検討してください。

データベースから Amazon S3 にアクセスできない

以下をチェックしてください:

- ODB ネットワークで Amazon S3 アクセスが有効になっていることを確認します。`GetOdbNetwork` アクションを使用して、`s3Access` ステータスが `Enabled` かどうかを確認します。
- 正しいリージョン DNS 名 (`s3.region.amazonaws.com`) を使用していることを確認します。
- Oracle データベースに Amazon S3 にアクセスするために必要なアクセス許可があることを確認します。

Oracle マネージドバックアップが失敗する

以下をチェックしてください:

- Amazon S3 への Oracle マネージドバックアップはデフォルトで有効になっており、無効にすることはできません。バックアップが失敗する場合は、Oracle データベースログで具体的なエラーメッセージを確認します。

- サービス統合リソースを表示して、Amazon VPC Lattice リソースが正しく設定されていることを確認します。
- Oracle マネージド自動バックアップの問題については、Oracle サポートにお問い合わせください。詳細については、「Oracle Database@AWS のサポートを取得する」を参照してください。

Oracle Database@AWS の Amazon Redshift とのゼロ ETL 統合

ゼロ ETL 統合は、複数のソースからのトランザクションデータと運用データを Amazon Redshift で利用できるようにするフルマネージドソリューションです。このソリューションを使用すると、Oracle Exadata または専有 Exadata インフラストラクチャ上の Autonomous データベースで実行されている Oracle データベースから Amazon Redshift にデータをレプリケートできます。自動同期により、従来の抽出、変換、ロード (ETL) プロセスを回避できます。また、リアルタイム分析と AI ワークロードも有効にします。詳細については、「Amazon Redshift 管理ガイド」の「ゼロ ETL 統合」を参照してください。

ゼロ ETL 統合には、次のような利点があります。

- リアルタイムデータレプリケーション – Oracle データベースから Amazon Redshift への継続的なデータ同期を最小限のレイテンシーで実現
- 複雑な ETL パイプラインの排除 – カスタムデータ統合ソリューションの構築と維持は不要
- 運用オーバーヘッドの削減 – AWS API による自動セットアップと管理
- データ統合アーキテクチャの簡素化 – Oracle Database@AWS と AWS 分析サービスのシームレスな統合
- セキュリティの強化 – 組み込みの暗号化と AWS IAM アクセスコントロール

Amazon Redshift では、Oracle Database@AWS とのゼロ ETL 統合には追加料金はかかりません。ゼロ ETL 統合の一部として作成した変更データの作成と処理に使用した既存の Amazon Redshift リソースの料金が発生します。詳細については、Amazon Redshift の料金を参照してください。

Oracle Database@AWS でのゼロ ETL 統合でサポートされるデータベースバージョン

ゼロ ETL 統合は、次の Oracle データベースバージョンをサポートしています。

- Oracle Exadata – Oracle Database 19c
- 専用インフラストラクチャ上の Autonomous データベース – Oracle Database 19c および 23ai

Oracle Database@AWS でのゼロ ETL 統合の仕組み

ゼロ ETL 統合により、Oracle Database@AWS はデータを Amazon Redshift にレプリケートできます。統合では、Amazon VPC Lattice を活用して安全なネットワーク接続を作成します。変更データキャプチャ (CDC) テクノロジーにより、リアルタイムのデータ同期が保証されます。AWS Glue API を使用して統合を管理します。

ゼロ ETL 統合アーキテクチャには以下が含まれます。

- 安全な接続 – データ転送に TLS ポート 2484 経由の SSL/TLS 暗号化を使用します
- AWS Secrets Manager – AWS Key Management Service を使用してデータベース認証情報と証明書を安全に保存します
- AWS Glue 統合 – ゼロ ETL 統合用の統合管理インターフェイスを提供します

レプリケーションは次のステップで進行します。

1. ポート 2484 で SSL を使用して Oracle データベースへの安全な接続を確立する
2. 選択したデータベース、スキーマ、テーブルの初期フルダンプを実行する
3. 継続的なリアルタイムレプリケーションのための変更データキャプチャ (CDC) を設定する
4. レプリケートされたデータをターゲットの Amazon Redshift クラスターに書き込む

> **Important**
>
> ゼロ ETL 統合はデフォルトでは有効になっていません。AWS Glue API を使用して設定する必要があります。Oracle Database@AWS API を使用してゼロ ETL 統合を直接設定することはできません。

Oracle Database@AWS でのゼロ ETL 統合の前提条件

ゼロ ETL 統合を設定する前に、次の前提条件を満たしていることを確認してください。

一般的な前提条件

- Oracle Database@AWS のセットアップ – 少なくとも 1 つの VM クラスターがプロビジョニングされ、実行されていることを確認します。

- ゼロ ETL が有効になっている統合 – VM クラスターまたは Autonomous VM クラスターが、ゼロ ETL が有効になっている ODB ネットワークに関連付けられていることを確認します。
- サポートされている Oracle Database バージョン – Oracle Database 19c (Oracle Exadata) または Oracle Database 19c/23ai (専用インフラストラクチャ上の Autonomous Database) を使用する必要があります。
- 同じ AWS リージョン – ソース Oracle データベースとターゲット Amazon Redshift クラスターは同じ AWS リージョンに存在する必要があります。

Oracle データベースの前提条件

Oracle データベースを次の設定で構成する必要があります。

レプリケーションユーザーのセットアップ

レプリケートする各プラガブルデータベース (PDB) に専用のレプリケーションユーザーを作成します。

- Oracle Exadata の場合 – 安全なパスワードでユーザー ODBZEROETLADMIN を作成します。
- 専用インフラストラクチャ上の Autonomous データベースの場合 – 既存の GGADMIN ユーザーを使用します。

レプリケーションユーザーに次のアクセス許可を付与します。

```
-- For Autonomous Database on Dedicated Infrastructure only
ALTER USER GGADMIN ACCOUNT UNLOCK;
ALTER USER GGADMIN IDENTIFIED BY ggadmin-password;

-- For Oracle Exadata only
GRANT SELECT ON any-replicated-table TO "ODBZEROETLADMIN";
GRANT LOGMINING to "ODBZEROETLADMIN";

-- Grant the following permissions to all services.
-- For Oracle Exadata, use the ODBZEROETLADMIN user. For Autonomous Database on
 Dedicated Infrastructure,
-- use the GGADMIN user.
GRANT CREATE SESSION TO "ODBZEROETLADMIN";
GRANT SELECT ANY TRANSACTION TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$ARCHIVED_LOG TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$LOG TO "ODBZEROETLADMIN";
```

```
GRANT SELECT ON V_$LOGFILE TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$LOGMNR_LOGS TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$LOGMNR_CONTENTS TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$DATABASE TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$THREAD TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$PARAMETER TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$NLS_PARAMETERS TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$TIMEZONE_NAMES TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$TRANSACTION TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$CONTAINERS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_INDEXES TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_OBJECTS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_TABLES TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_USERS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_CATALOG TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_CONSTRAINTS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_CONS_COLUMNS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_TAB_COLS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_IND_COLUMNS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_ENCRYPTED_COLUMNS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_LOG_GROUPS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_TAB_PARTITIONS TO "ODBZEROETLADMIN";
GRANT SELECT ON SYS.DBA_REGISTRY TO "ODBZEROETLADMIN";
GRANT SELECT ON SYS.OBJ$ TO "ODBZEROETLADMIN";
GRANT SELECT ON DBA_TABLESPACES TO "ODBZEROETLADMIN";
GRANT SELECT ON DBA_OBJECTS TO "ODBZEROETLADMIN";
GRANT SELECT ON SYS.ENC$ TO "ODBZEROETLADMIN";
GRANT SELECT ON GV_$TRANSACTION TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$DATAGUARD_STATS TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$DATABASE_INCARNATION TO "ODBZEROETLADMIN";
GRANT EXECUTE ON SYS.DBMS_CRYPTO TO "ODBZEROETLADMIN";
GRANT SELECT ON SYS.DBA_DIRECTORIES TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_VIEWS TO "ODBZEROETLADMIN";
GRANT SELECT ON DBA_SEGMENTS TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$TRANSPORTABLE_PLATFORM TO "ODBZEROETLADMIN";
GRANT CREATE ANY DIRECTORY TO "ODBZEROETLADMIN";
GRANT EXECUTE ON DBMS_FILE_TRANSFER TO "ODBZEROETLADMIN";
GRANT EXECUTE ON DBMS_FILE_GROUP TO "ODBZEROETLADMIN";
GRANT EXECUTE on DBMSLOGMNR to "ODBZEROETLADMIN";
GRANT SELECT on V_$LOGMNRLOGS to "ODBZEROETLADMIN";
GRANT SELECT on V_$LOGMNRCONTENTS to "ODBZEROETLADMIN";
GRANT LOGMINING to "ODBZEROETLADMIN";
GRANT SELECT ON GV_$CELL_STATE TO "ODBZEROETLADMIN";
```

サプリメンタルロギング

Oracle データベースでサプリメンタルロギングを有効にして、変更データをキャプチャします。

```
-- Check if supplemental logging is enabled
SELECT supplemental_log_data_min FROM v$database;

-- Enable supplemental logging if not already enabled.
-- For Oracle Exadata, enable supplemental logging on both the CDB and PDB.
-- For Autonomous Database on Dedicated Infrastructure, enable supplemental logging on
 the PDB only.
ALTER DATABASE ADD SUPPLEMENTAL LOG DATA;

-- For Autonomous Database on Dedicated Infrastructure only
ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;

-- Archive current online redo log
ALTER SYSTEM ARCHIVE LOG CURRENT;
```

Oracle Database@AWS と Amazon Redshift 間のゼロ ETL 統合を設定するには、SSL を設定する必要があります。

Oracle Exadata データベースの場合

ポート 2484 で SSL を手動で設定する必要があります。このタスクには以下が含まれます。

- `listener.ora` での `(PROTOCOL=tcps)(PORT=2484)` の設定
- `sqlnet.ora` を使用したウォレットの設定
- SSL 証明書の生成と設定 (My Oracle Support ドキュメントの How To Configure SSL/TCPS For Exadata Cloud Database (ExaCC/ExaCS) (Doc ID 2947301.1) を参照)

Autonomous データベースの場合

ポート 2484 の SSL はデフォルトで有効になっています。追加の設定は必要ありません。

> **Important**
>
> SSL ポートは 2484 に固定されています。

AWS のサービスの前提条件

ゼロ ETL 統合を設定する前に、AWS Secrets Manager をセットアップし、IAM アクセス許可を設定します。

AWS Secrets Manager のセットアップ

次のように、Oracle データベース認証情報を AWS Secrets Manager に保存します。

1. AWS Key Management Service でカスタマーマネージドキー (CMK) を作成します。
2. CMK を使用して、AWS Secrets Manager にデータベース認証情報を保存します。
3. Oracle Database@AWS アクセスを許可するようにリソースポリシーを設定します。

TDE キー ID とパスワードを取得するには、「AWS Database Migration Service のソースとして Oracle を使用するためにサポートされている暗号化方法」で説明されている方法を使用します。次のコマンドは、base64 ウォレットを生成します。

```
base64 -i cwallet.sso > wallet.b64
```

次の例は、Oracle Exadata のシークレットを示しています。*asm_service_name* の場合、*111.11.11.11* は VM ノードの仮想 IP を表します。ASM リスナーを SCAN に登録することもできます。

```
{
  "database_info": [
    {
      "name": "ODBDB_ZETLPDB",
      "service_name": "ODBDB_ZETLPDB.paas.oracle.com",
      "username": "ODBZEROETLADMIN",
      "password": "secure_password",
      "tde_key_id": "ORACLE.SECURITY.DB.ENCRYPTION.key_id",
      "tde_password": "tde_password",
      "certificateWallet": "base64_encoded_wallet_content"
    }
  ],
  "asm_info": {
    "asm_user": "odbzeroetlasm",
    "asm_password": "secure_password",
    "asm_service_name": "111.11.11.11:2484/+ASM"
  }
```

```
}
```

次の例は、専用インフラストラクチャ上の Autonomous データベースのシークレットを示しています。

```
{
  "database_info": [
    {
      "database_name": "ZETLACD_ZETLADBMORECPU",
      "service_name": "ZETLADBMORECPU_high.adw.oraclecloud.com",
      "username": "ggadmin",
      "password": "secure_password",
      "certificateWallet": "base64_encoded_wallet_content"
    }
  ]
}
```

IAM 許可を設定する

ゼロ ETL 統合オペレーションを許可する IAM ポリシーを作成します。次のポリシー例では、Exadata VM クラスターの記述、作成、更新、削除オペレーションを許可します。Autonomous VM クラスターの場合、リソース ARN に `cloud-vm-cluster` ではなく、`cloud-autonomous-vm-cluster` の値を使用します。

Oracle Database@AWS でのゼロ ETL 統合に関する考慮事項

Oracle Database@AWS と Amazon Redshift とのゼロ ETL 統合を設定するときは、次のガイドラインを考慮してください。

初期データロード時間

初期の完全ロード時間は、データベースのサイズによって異なります。大規模なデータベースでは、最初の同期が完了するまでに数時間または数日かかる場合があります。

Oracle データベースのパフォーマンス

特にトランザクション量が多い場合、変更データキャプチャは Oracle データベースのパフォーマンスに影響を与える可能性があります。ゼロ ETL 統合を有効にした後、データベースのパフォーマンスをモニタリングします。

スキーマの変更

ソース Oracle データベースのデータ定義言語 (DDL) が変更されると、手動で介入して統合を再作成する必要がある場合があります。スキーマの変更は慎重に計画してください。

一般的な考慮事項については、「Amazon Redshift とのゼロ ETL 統合を使用する場合の考慮事項」を参照してください。

Oracle Database@AWS でのゼロ ETL 統合の制限

以下の一般的な制限事項に注意してください。

統合ごとに 単一の PDB

各ゼロ ETL 統合では、1 つのプラガブルデータベース (PDB) からのみデータをレプリケートできます。`include: pdb1.*.*, include: pdb2.*.*` のようなデータフィルターはサポートされていません。

Autonomous データベースまたは Exadata インフラストラクチャごとに 1 つの統合

各ゼロ ETL 統合は、専有インフラストラクチャ上の 1 つの Autonomous データベースからのみデータをレプリケートできます。

固定 SSL ポート

SSL 接続では、ポート 2484 を使用する必要があります。

同じリージョンの要件

ソース Oracle Database@AWS VM クラスターとターゲット Amazon Redshift クラスターは、同じ AWS リージョンに存在する必要があります。クロスリージョンレプリケーションはサポートされていません。

mTLS サポートなし

相互 TLS (mTLS) はサポートされていません。OCI データベースで mTLS が有効になっている場合、ゼロ ETL 統合を使用するには無効にする必要があります。

イミュータブルな統合設定

統合に関連付けられたシークレット ARN または KMS キーを作成した後は、それを変更することはできません。これらの設定を変更するには、統合を削除して再作成する必要があります。

TDE 列レベルの暗号化

列レベルの透過的データ暗号化 (TDE) は、Oracle Exadata データベースではサポートされていません。テーブルスペースレベルの TDE のみがサポートされています。

サポートされるデータ型

一部の Oracle 固有のデータ型は完全にはサポートされていないか、レプリケーション中に変換が必要になる場合があります。データベースを本番環境にデプロイする前に、特定のデータ型を徹底的にテストしてください。

Oracle Database@AWS と Amazon Redshift の統合の設定

Oracle データベースと Amazon Redshift 間のゼロ ETL 統合を設定するには、次の手順を実行します。

1. ODB ネットワークでゼロ ETL を有効にします。
2. Oracle データベースの前提条件を設定します。
3. AWS Secrets Manager と AWS Key Management Service をセットアップします。
4. IAM 許可を設定します。
5. Amazon Redshift リソースポリシーを設定します。
6. ゼロ ETL 統合を作成します。
7. Amazon Redshift にターゲットデータベースを作成します。

ステップ 1: ODB ネットワークのゼロ ETL を有効にする

ソース VM クラスターに関連付けられた ODB ネットワークのゼロ ETL 統合を有効にできます。デフォルトでは、この統合は無効になっています。

コンソール

ゼロ ETL 統合を有効にするには

1. https://console.aws.amazon.com/odb/ で Oracle Database@AWS コンソールを開きます。
2. ナビゲーションペインで [ODB ネットワーク] を選択します。
3. ゼロ ETL 統合を有効にする ODB ネットワークを選択します。

4. [Modify] (変更) を選択します。
5. [ゼロ ETL] を選択します。
6. [続行] を選択してから、[修正] を選択します。

AWS CLI

ゼロ ETL 統合を有効にするには、`--zero-etl-access` パラメータを指定して `update-odb-network` コマンドを使用します。

```
aws odb update-odb-network \
  --odb-network-id odb-network-id \
  --zero-etl-access ENABLED
```

ソース VM クラスターに関連付けられた ODB ネットワークのゼロ ETL 統合を有効にするには、`update-odb-network` コマンドを使用します。このコマンドは、ゼロ ETL 統合に必要なネットワークインフラストラクチャを設定します。

```
aws odb update-odb-network \
  --odb-network-id your-odb-network-id \
  --zero-etl-access ENABLED
```

ステップ 2: Oracle データベースの設定

「前提条件」の説明に従って Oracle データベース設定を完了します。

- レプリケーションユーザーを作成し、必要なアクセス許可を付与します。
- アーカイブ REDO ログを有効にします。
- SSL を設定します (Oracle Exadata のみ)。
- 該当する場合、ASM ユーザーを設定します (Oracle Exadata のみ)。

ステップ 3: AWS Secrets Manager と AWS Key Management Service をセットアップする

カスタマーマネージドキー (CMK) を作成し、データベース認証情報を保存します。

1. `create-key` コマンドを使用して AWS Key Management Service で CMK を作成します。

```
aws kms create-key \
  --description "ODB Zero-ETL Integration Key" \
  --key-usage ENCRYPT_DECRYPT \
  --key-spec SYMMETRIC_DEFAULT
```

2. AWS Secrets Manager にデータベース認証情報を保存します。

```
aws secretsmanager create-secret \
  --name "ODBZeroETLCredentials" \
  --description "Credentials for Oracle Database@AWS Zero-ETL integration" \
  --kms-key-id your-cmk-key-arn \
  --secret-string file://secret-content.json
```

3. Oracle Database@AWS アクセスを許可するには、シークレットにリソースポリシーをアタッチします。

```
aws secretsmanager put-resource-policy \
  --secret-id "ODBZeroETLCredentials" \
  --resource-policy file://secret-resource-policy.json
```

上記のコマンドでは、`secret-resource-policy.json` に次の JSON が含まれています。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "zetl.odb.amazonaws.com"
      },
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": "*"
    }
  ]
}
```

4. CMK にリソースポリシーをアタッチします。暗号化されたゼロ ETL 統合をサポートするには、CMK リソースポリシーに Oracle Database@AWS サービスプリンシパルと Amazon Redshift サービスプリンシパルの両方のアクセス許可を含める必要があります。

```
aws kms put-key-policy \
  --key-id your-cmk-key-arn \
  --policy-name default \
  --policy file://cmk-resource-policy.json
```

cmk-resource-policy.json には次のポリシーステートメントを含める必要があります。最初のステートメントは Oracle Database@AWS サービスアクセスを許可し、2 番目のステートメントは Amazon Redshift が暗号化されたデータオペレーションの KMS キーに許可を作成できるようにします。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow ODB service access",
      "Effect": "Allow",
      "Principal": {
        "Service": "zetl.odb.amazonaws.com"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:CreateGrant"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Allows the Redshift service principal to add a grant to a KMS
 key",
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "kms:CreateGrant",
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "kms:EncryptionContext:{context-key}": "{context-value}"
        },
        "ForAllValues:StringEquals": {
          "kms:GrantOperations": [
            "Decrypt",
            "GenerateDataKey",
            "CreateGrant"
          ]
        }
      }
    }
  ]
}
```

ステップ 4: IAM のアクセス許可を設定する

ゼロ ETL 統合オペレーションを許可する IAM ポリシーを作成してアタッチします。

```
aws iam create-policy \
  --policy-name "ODBZeroETLIntegrationPolicy" \
  --policy-document file://odb-zetl-iam-policy.json

aws iam attach-user-policy \
  --user-name your-iam-username \
  --policy-arn policy-arn
```

次のポリシーは必要なアクセス許可を付与します。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ODBGlueIntegrationAccess",
      "Effect": "Allow",
      "Action": [
        "glue:CreateIntegration",
        "glue:ModifyIntegration",
```

```
        "glue:DeleteIntegration",
        "glue:DescribeIntegrations",
        "glue:DescribeInboundIntegrations"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ODBZetlOperations",
      "Effect": "Allow",
      "Action": "odb:CreateOutboundIntegration",
      "Resource": "*"
    },
    {
      "Sid": "ODBRedshiftFullAccess",
      "Effect": "Allow",
      "Action": [
        "redshift:*",
        "redshift-serverless:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
         "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DisableAlarmActions",
        "tag:GetResources",
        "tag:UntagResources",
        "tag:GetTagValues",
        "tag:GetTagKeys",
        "tag:TagResources"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ODBRedshiftDataAPI",
```

```
      "Effect": "Allow",
      "Action": [
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ODBKMSAccess",
      "Effect": "Allow",
      "Action": [
        "kms:CreateKey",
        "kms:DescribeKey",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:ListKeys",
        "kms:CreateAlias",
        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ODBSecretsManagerAccess",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:ValidateResourcePolicy"
      ],
```

```
      "Resource": "*"
    }
  ]
}
```

ステップ 5: Amazon Redshift リソースポリシーを設定する

Amazon Redshift クラスターにリソースポリシーを設定して、インバウンド統合を承認します。

```
aws redshift put-resource-policy \
  --no-verify-ssl \
  --resource-arn "your-redshift-cluster-arn" \
  --policy '{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "Service": "redshift.amazonaws.com"
        },
        "Action": [
          "redshift:AuthorizeInboundIntegration"
        ],
        "Condition": {
          "StringEquals": {
            "aws:SourceArn": "your-vm-cluster-arn"
          }
        }
      },
      {
        "Effect": "Allow",
        "Principal": {
          "AWS": "your-account-id"
        },
        "Action": [
          "redshift:CreateInboundIntegration"
        ]
      }
    ]
  }' \
  --region us-west-2
```

> **Tip**
>
> または、AWS コンソールで [私のために修正] オプションを使用することもできます。このオプションを使用すると、手動で設定する必要なく、必要な Amazon Redshift ポリシーが自動的に設定されます。

ステップ 6: AWS Glue を使用してゼロ ETL 統合を作成する

AWS Glue `create-integration` コマンドを使用してゼロ ETL 統合を作成します。このコマンドでは、ソース VM クラスターとターゲット Amazon Redshift 名前空間を指定します。

次の例では、Exadata VM クラスターで実行されている pdb1 という名前の PDB との統合を作成します。ソース ARN で `cloud-vm-cluster` を `cloud-autonomous-vm-cluster` に置き換えることで、Autonomous VM クラスターを作成することもできます。KMS キーの指定はオプションです。キーを指定する場合、ステップ 3: AWS Secrets Manager と AWS Key Management Service をセットアップする で作成したキーとは異なる場合があります。

```
aws glue create-integration \
  --integration-name "MyODBZeroETLIntegration" \
  --source-arn "arn:aws:odb:region:account:cloud-vm-cluster/cluster-id" \
  --target-arn "arn:aws:redshift:region:account:namespace/namespace-id" \
  --data-filter "include: pdb1.*.*" \
  --integration-config '{
      "RefreshInterval": "10",
      "IntegrationMode": "DEFAULT",
      "SourcePropertiesMap": {
        "secret-arn": "arn:aws:secretsmanager:region:account:secret:secret-name"
      }
    }' \
  --description "Zero-ETL integration for Oracle to Amazon Redshift" \
  --kms-key-id "arn:aws:kms:region:account:key/key-id"
```

コマンドは統合 ARN を返し、ステータスを `creating` に設定します。`describe-integrations` コマンドを使用して統合ステータスをモニタリングできます。

```
aws glue describe-integrations \
  --integration-identifier integration-id
```

> **Important**
>
> 統合ごとに 1 つの PDB のみがサポートされます。データフィルターでは、`include: pdb1.*.*` のように単一の PDB を指定する必要があります。ソースは、統合が作成される AWS リージョンおよびアカウントと同じリージョンおよびアカウントにある必要があります。

ステップ 7: Amazon Redshift でターゲットデータベースを作成する

統合がアクティブになったら、Amazon Redshift クラスターにターゲットデータベースを作成します。

```
-- Connect to your Amazon Redshift cluster
psql -h your-redshift-endpoint -U username -d database

-- Create database from integration
CREATE DATABASE target_database_name
FROM INTEGRATION 'integration-id'
DATABASE "source_pdb_name";
```

ターゲットデータベースを作成したら、レプリケートされたデータをクエリできます。

```
-- List databases to verify creation
\l

-- Connect to the new database
\c target_database_name

-- List tables to see replicated data
\dt
```

ゼロ ETL 統合を検証する

AWS Glue で統合ステータスをクエリし、Oracle の変更が Amazon Redshift にレプリケートされていることを確認することで、統合が機能していることを確認します。

ゼロ ETL 統合が正しく機能していることを確認するには

1. 統合ステータスを確認します。

```
aws glue describe-integrations \
  --integration-identifier integration-id
```

ステータスは ACTIVE または REPLICATING である必要があります。

2. Oracle データベースに変更を加え、Amazon Redshift に反映されるかどうかを確認して、データのレプリケーションを検証します。
3. Amazon CloudWatch でレプリケーションメトリクスをモニタリングします (利用可能な場合)。

Oracle Database@AWS でのゼロ ETL 統合でのデータフィルタリング

Oracle Database@AWS のゼロ ETL 統合は、データのフィルタリングをサポートします。これを使用して、ソース Oracle Exadata データベースがターゲットデータウェアハウスにレプリケートするデータを制御できます。データベース全体をレプリケートする代わりに、1 つ以上のフィルターを適用して、特定のテーブルを選択的に含めたり除外したりできます。これにより、関連するデータのみが転送されるようにすることで、ストレージとクエリのパフォーマンスを最適化できます。フィルタリングはデータベースレベルとテーブルレベルに制限されています。列レベルと行レベルのフィルタリングはサポートされていません。

Oracle Database と Amazon Redshift では、オブジェクト名の大文字と小文字の処理方法が異なり、これはデータフィルター設定とターゲットクエリの両方に影響します。次の点に注意してください。

- Oracle Database は、CREATE ステートメントで明示的に引用符で囲まれていない限り、データベース、スキーマ、およびオブジェクト名を大文字で保存します。例えば、mytable (引用符なし) を作成する場合、Oracle データディクショナリはテーブル名を MYTABLE として保存します。作成ステートメントでオブジェクト名を引用符で囲むと、Oracle データディクショナリは大文字と小文字を保持します。
- ゼロ ETL データフィルターでは大文字と小文字が区別され、Oracle データディクショナリに表示されるオブジェクト名の大文字と小文字が正確に一致する必要があります。例えば、Oracle ディクショナリにスキーマとテーブル名 REINVENT.MYTABLE が保存されている場合は、include: ORCL.REINVENT.MYTABLE を使用してフィルタを作成します。
- Amazon Redshift クエリは、明示的に引用符で囲まれていない限り、デフォルトで小文字のオブジェクト名になります。例えば、MYTABLE (引用符なし) のクエリは mytable を検索します。

Amazon Redshift フィルターを作成してデータをクエリするときは、大文字と小文字の違いに注意してください。Oracle Database@AWS のフィルタリングに関する考慮事項は、Amazon RDS for Oracle の場合と同じです。Oracle データベースで大文字と小文字がデータフィルターにどのように影響するかの例については、「Amazon Relational Database Service ユーザーガイド」の「RDS for Oracle の例」を参照してください。

ゼロ ETL 統合のモニタリング

ゼロ ETL 統合を定期的にモニタリングすることで、最適なパフォーマンスを確保し、問題を早期に特定できます。

統合ステータスのモニタリング

AWS Glue API を使用してゼロ ETL 統合のステータスをモニタリングします。

```
# Check status of a specific integration
aws glue describe-integrations \
  --integration-identifier integration-id

# List all integrations in your account
aws glue describe-integrations
```

統合ステータスには以下が含まれます。

- creating – 統合がセットアップ中です
- active – 統合が実行され、データがレプリケートされています
- modifying – 統合設定を更新中です
- needs_attention – 統合には手動による介入が必要です
- failed – 統合でエラーが発生しました
- deleting – 統合は削除中です

パフォーマンスのモニタリング

ゼロ ETL 統合パフォーマンスの以下の側面をモニタリングします。

- レプリケーションラグ – Oracle で変更が発生してから Amazon Redshift に反映されるまでの時間差
- データスループット – 時間単位あたりにレプリケートされるデータの量

- エラー率 – レプリケーションエラーまたは失敗の頻度
- リソース使用率 – ソースシステムとターゲットシステムの両方での CPU、メモリ、ネットワーク使用状況

Amazon CloudWatch を使用してこれらのメトリクスをモニタリングし、重要なしきい値のアラームを設定します。

Oracle Database@AWS でのゼロ ETL 統合の管理

ゼロ ETL 統合を作成した後、統合の変更や削除など、さまざまな管理オペレーションを実行できます。このセクションでは、ゼロ ETL 統合の継続的な管理について説明します。

ゼロ ETL 統合の変更

サポートされるデータウェアハウスとのゼロ ETL 統合では、名前、説明、データフィルタリングオプションのみを変更できます。統合の暗号化に使用される AWS Key Management Service キー、ソースデータベースまたはターゲットデータベースは変更できません。

統合を変更するための前提条件

ゼロ ETL 統合を変更する前に、以下があることを確認してください。

- 必要なアクセス許可 – IAM ユーザーまたはロールには、標準の `odb:UpdateOutboundIntegration` アクセス許可に加えて、AWS Glue アクセス許可が必要です。
- アクティブ状態の統合 – 統合は `CREATING`、`MODIFYING`、`DELETING` または `FAILED` ではなく、`ACTIVE` 状態である必要があります。
- 有効なデータフィルター構文 – 新しいデータフィルターは、サポートされている包含/除外パターン構文に従う必要があります。

データフィルターの変更

データフィルターを変更することで、レプリケートされるテーブルまたはスキーマを変更できます。これにより、統合全体を再作成することなく、レプリケーションからデータベースオブジェクトを追加または削除できます。

統合のデータフィルターを変更するには、`modify-integration` コマンドを使用します。

```
aws glue modify-integration \
  --integration-identifier integration-id \
  --data-filter "include: pdb1.new_schema.*"
```

統合名と説明を同時に変更することもできます。次の例では、pdb1 の 2 つのスキーマの統合名、説明、フィルターを変更します。

```
aws glue modify-integration \
  --integration-identifier integration-id \
  --data-filter "include: pdb1.schema1.*, pdb1.schema2.*" \
  --integration-name "Updated Integration Name" \
  --description "Updated integration description"
```

Important

データフィルターを変更すると、統合は modifying 状態になり、データの再同期を実行します。統合はレプリケーションを停止し、新しいフィルター設定を適用し、再ロードターゲットオペレーションでレプリケーションを再開します。統合ステータスをモニタリングして、変更が正常に完了したことを確認します。

ゼロ ETL 統合へのデータフィルターの変更に関する考慮事項

データフィルターを変更するときは、次の点を考慮してください。

- 単一の PDB の制限 – 統合ごとに指定できるプラガブルデータベース (PDB) は 1 つだけです。include: pdb1.*.*, include: pdb2.*.* のようなデータフィルターはサポートされていません
- レプリケーションの中断 – 変更プロセス中はデータレプリケーションが停止し、新しいフィルターが適用された後に再開されます。
- データの再ロード – 統合は、新しいフィルター条件に一致するデータの完全な再ロードを実行します。
- パフォーマンスへの影響 – データフィルターの変更が大きいと、完了までにかなりの時間がかかり、再ロード中にソースデータベースのパフォーマンスに影響を及ぼす可能性があります。

ゼロ ETL 統合設定の変更に関する制限事項

ゼロ ETL 統合を作成した後、次の設定を変更することはできません。

- シークレット ARN – データベース認証情報を含む AWS Secrets Manager シークレット
- KMS キー: 暗号化に使用されるカスタマーマネージドキー。
- ソース ARN – Oracle Database@AWS VM クラスター
- ターゲット ARN – Amazon Redshift クラスターまたは名前空間

これらの設定を変更するには、既存のゼロ ETL 統合を削除し、新しい統合を作成します。

ゼロ ETL 統合の削除

ゼロ ETL 統合が不要になった場合は、それを削除してレプリケーションを停止し、関連するリソースをクリーンアップできます。

AWS Glue を使用した削除

AWS Glue API を使用してゼロ ETL 統合を削除できます。

```
aws glue delete-integration \
  --integration-identifier integration-id
```

統合は、次の状態で削除できます。

- アクティブ
- needs_attention
- 「失敗」
- syncing

削除の影響

ゼロ ETL 統合を削除するときは、次の効果を考慮してください。

レプリケーションが停止します。

Oracle Database@AWS は、Amazon Redshift からの新しい変更をレプリケートしません。

既存のデータは保持されます。

Amazon Redshift に既にレプリケートされているデータは引き続き使用できます。

ターゲットデータベースは残ります。

統合から作成された Amazon Redshift データベースは自動的に削除されません。

> **Important**
>
> 削除は元に戻せません。削除後にレプリケーションを再開する必要がある場合は、完全な初期ロードを実行する新しい統合を作成します。

ゼロ ETL 管理のベストプラクティス

これらのベストプラクティスに従って、ゼロ ETL 統合のパフォーマンス、セキュリティ、コスト効率を最適化します。

運用のベストプラクティス

これらの運用プラクティスは、信頼性が高く効率的なゼロ ETL 統合を維持するのに役立ちます。

定期的なモニタリング

CloudWatch アラームを設定して、統合のヘルスメトリクスとパフォーマンスメトリクスをモニタリングします。

認証情報のローテーション

データベースパスワードを定期的に更新し、AWS Secrets Manager で更新します。

バックアップの検証

Oracle データベースのバックアップにディザスタリカバリに必要なコンポーネントが含まれていることを定期的に確認します。

パフォーマンステスト

特にピーク使用期間中に、ゼロ ETL 統合が Oracle データベースのパフォーマンスに与える影響をテストします。

スキーマ変更計画

スキーマの変更を本番環境に適用する前に、開発環境で計画およびテストします。

セキュリティのベストプラクティス

これらのセキュリティ対策を実装して、ゼロ ETL 統合とデータを保護します。

最小特権アクセス

レプリケーションユーザーと AWS IAM ロールに必要最小限のアクセス許可のみを付与します。

ネットワークセキュリティ

セキュリティグループと NACL を使用して、必要なポートとソースのみにネットワークアクセスを制限します。

保管中の暗号化

Oracle データベースと Amazon Redshift クラスターの両方が保管時の暗号化を使用していることを確認します。

監査ログ

Oracle と Amazon Redshift の両方で監査ログ記録を有効にして、データアクセスと変更を追跡します。

シークレットの管理

可能な場合は AWS Secrets Manager の自動ローテーション機能を使用します。

コスト最適化

これらの戦略を適用して、効果的なゼロ ETL 統合パフォーマンスを維持しながらコストを最適化します。

データのフィルタリング

正確なデータフィルターを使用して、必要なデータのみをレプリケートし、ストレージとコンピューティングのコストを削減します。

Amazon Redshift の最適化

適切な Amazon Redshift ノードタイプを使用し、データ圧縮を実装してコストを最適化します。

使用状況のモニタリング

AWS Cost Explorer を使用して、ゼロ ETL 統合の使用状況とコストを定期的に確認します。

未使用の統合をクリーンアップする

継続的な料金を回避するために不要になった統合を削除します。

ゼロ ETL 統合のトラブルシューティング

このセクションでは、ゼロ ETL 統合の一般的な問題を解決するためのガイダンスを提供します。

ゼロ ETL 統合セットアップの失敗

認証の失敗

- AWS Secrets Manager にレプリケーションユーザーが存在し、正しいパスワードが設定されていることを確認します。
- レプリケーションユーザーに必要なアクセス許可がすべて付与されていることを確認します。
- シークレット ARN が正しく、Oracle Database@AWS からアクセス可能であることを確認します。
- CMK リソースポリシーが Oracle Database@AWS サービスプリンシパルによるアクセスを許可していることを確認します。

ネットワーク接続の問題

- ODB ネットワークでゼロ ETL 統合が有効になっていることを確認します。
- ポート 2484 で SSL が正しく設定されていることを確認します(Exadata のみ)。
- Oracle データベースリスナーが実行中で、接続を受け入れていることを確認します。
- ネットワークセキュリティグループと NACL がポート 2484 のトラフィックを許可していることを確認します。
- シークレットのサービス名が実際の Oracle サービス名と一致していることを確認します。

アクセス許可エラー

- IAM ユーザーまたはロールに、AWS Glue 統合オペレーションに必要なアクセス許可があることを確認します。
- Amazon Redshift リソースポリシーで VM クラスターからのインバウンド統合が許可されていることを確認します。
- Oracle Database@AWS にシークレットと AWS Key Management Service キーへのアクセスが許可されていることを確認します。

レプリケーションの問題

初期ロードの失敗

- Oracle データベースに、全ロードオペレーションをサポートするのに十分なリソースがあることを確認します。
- ソースデータベースでの補足的なログ記録が有効になっていることを確認します。
- データ抽出を妨げる可能性のあるテーブルレベルのロックまたは制約がないか確認します。

変更データキャプチャの問題

- Oracle データベースに十分な REDO ログスペースと保存期間があることを確認します。
- レプリケーションユーザーがアーカイブされた REDO ログにアクセスできることを確認します。
- ASM 対応システムの場合は、ASM ユーザーが正しく設定されていることを確認します。
- Oracle データベースのパフォーマンスをモニタリングして、CDC がリソースの競合を引き起こしていないことを確認します。

レプリケーションの遅延が大きい

- CloudWatch でレプリケーション遅延メトリクスをモニタリングします。
- ソースデータベースでトランザクション量が多いか、トランザクションが大きいを確認します。
- Amazon Redshift クラスターに受信データを処理するための十分な容量があることを確認します。

データ整合性の問題

欠落または不完全なデータ

- データフィルターに必要なスキーマとテーブルがすべて含まれていることを確認します。
- レプリケーションの失敗の原因となっている可能性のあるサポートされていないデータ型を確認します。
- レプリケーションユーザーがすべての必要なテーブルに対して SELECT 許可を持っていることを確認します。

データ型変換エラー

- Oracle と Redshift の間でサポートされているデータ型のマッピングを確認します。
- カスタム処理が必要な可能性がある Oracle 固有のデータ型を確認します。

- より互換性のあるデータ型を使用するように Oracle スキーマを変更することを検討してください。

モニタリングとデバッグ

ゼロ ETL 統合の問題をモニタリングおよびデバッグするには、次のアプローチを使用します。

- 統合ステータスのモニタリング – `aws glue describe-integrations` を使用して統合ステータスを定期的に確認します。
- CloudWatch メトリクス – レプリケーションのパフォーマンスとエラーについて、使用可能な CloudWatch メトリクスをモニタリングします。
- Oracle データベースのモニタリング – Oracle データベースのパフォーマンスとリソース使用率をモニタリングします。
- Redshift モニタリング – Amazon Redshift クラスターのパフォーマンスとストレージ使用率をモニタリングします。

このトラブルシューティングガイドを使用しても解決できない複雑な問題については、次の情報を AWS サポート に連絡してください。

- 統合 ARN と現在のステータス。
- 統合からのエラーメッセージにはオペレーションが記述されています。
- Oracle データベースと Amazon Redshift クラスターの設定。
- 問題が発生した時刻のタイムライン。

Oracle Database@AWS でのセキュリティ

AWS でのクラウドセキュリティは最優先事項です。AWS のユーザーは、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを利用できます。

セキュリティは AWS、OCI、およびお客様の間の共有責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ — AWS は、AWS クラウド で AWS のサービス を実行するインフラストラクチャを保護する責任を負います。また AWS は、お客様が使用するサービスを安全に提供します。サードパーティーの監査人は、AWS コンプライアンスプログラム の一環として、セキュリティの有効性を定期的にテストおよび検証します。
- クラウド内のセキュリティ - ユーザーの責任は、使用する AWS のサービスに応じて異なります。ユーザーは、ユーザーのデータの機密性、組織の要件、および適用法と規制などのその他要因に対する責任も担います。

このドキュメントは、Oracle Database@AWS の使用時に責任共有モデルを適用する方法を理解するために役立ちます。また、Oracle Database@AWS リソースのモニタリングや保護に役立つ、その他 AWS サービスの使用方法についても説明します。

Oracle Database@AWS リソースへのアクセスを管理できます。アクセスの管理に使用する方法は、お客様が Oracle Database@AWS で実行する必要のあるタスクのタイプによって異なります。

- AWS Identity and Access Management (IAM) ポリシーを使用して、どのユーザーが Oracle Database@AWS リソースの管理を許可されるかを決定するアクセス許可を割り当てます。例えば、IAM を使用して、Exadata インフラストラクチャ、VM クラスター、またはタグリソースの作成、説明、変更、削除を実行できるユーザーを決定できます。
- Oracle データベースエンジンのセキュリティ機能を使用して、DB インスタンス上のデータベースにログインできるユーザーを制御します。これらの機能は、データベースがローカルネットワーク上にあるかのように動作します。
- Exadata データベースでは、Secure Socket Layer (SSL) または Transport Layer Security (TLS) 接続を使用します。詳細については、「Prepare for TLS Walletless Connections」を参照してください。
- Oracle Database@AWS はインターネットから直接アクセスすることはできず、AWS 内のプライベートサブネットにのみデプロイされます。

- Oracle Database@AWS は、さまざまなオペレーションに多くのデフォルトの Transmission Control Protocol (TCP) ポートを使用します。ポートの完全なリストについては、「デフォルトのポート割り当て」を参照してください。
- デフォルトで有効になっている透過的なデータ暗号化 (TDE) を使用してキーを保存および管理するに、Oracle Database@AWS は OCI ボールトまたは Oracle Key Vault を使用します。Oracle Database@AWS は AWS Key Management Service をサポートしていません。
- デフォルトでは、データベースは Oracle 管理の暗号化キーを使用して設定されます。データベースは、カスタマーマネージドキーもサポートしています。
- データ保護を強化するには、Oracle Database@AWS で Oracle Data Safe を使用します。

以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Oracle Database@AWS を設定する方法を示します。

トピック

Oracle Database@AWS でのデータ保護

データを保護するため、「AWS アカウント」認証情報を保護し、AWS IAM アイデンティティセンター または AWS Identity and Access Management (IAM) を使用して個々のユーザーをセットアップすることをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- AWS CloudTrail で API とユーザーアクティビティロギングを設定します。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「AWS CloudTrail ユーザーガイド」の「CloudTrail 証跡の使用」を参照してください。

- AWS のサービス内のすべてのデフォルトセキュリティコントロールに加え、AWS 暗号化ソリューションを使用します。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API を使用して AWS にアクセスする際に FIPS 140-3 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これには、コンソール、API、AWS CLI、または AWS SDK を使用して Oracle Database@AWS またはその他の AWS のサービスで作業する場合が含まれます。タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

データ暗号化

Exadata データベースは、Oracle Transparent Data Encryption (TDE) を使用してデータを暗号化します。データは、一時テーブルスペース、UNDO セグメント、REDO ログ、JOIN や SORT などの内部データベースオペレーション中にも保護されます。詳細については、「Data Security」を参照してください。

転送中の暗号化

Exadata データベースは、Oracle Net Services のネイティブ暗号化と整合性機能を使用して、データベースへの接続を保護します。詳細については、「Security of data in transit」を参照してください。

キー管理

透過的なデータ暗号化には、マスター暗号化キーを安全に保存するためのキーストアと、キーストアを安全かつ効率的に管理し、キーメンテナンスオペレーションを実行するための管理フレームワークが含まれています。詳細については、「To administer Vault encryption keys」を参照してください。

Oracle Database@AWS のためのアイデンティティおよびアクセス管理

AWS Identity and Access Management IAMは、管理者が AWS リソースへのアクセスを安全にコントロールするために役立つ AWS のサービスです。IAM 管理者は、誰を認証 (サインイン) し、誰に Oracle Database@AWS リソースの使用を認可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる「AWS」のサービスです。

トピック

対象者

AWS Identity and Access Management (IAM) の使用方法は、ロールによって異なります。

- サービスユーザー - 機能にアクセスできない場合は、管理者にアクセス許可をリクエストします (「Oracle Database@AWS ID とアクセスのトラブルシューティング」を参照)。
- サービス管理者 - ユーザーアクセスを決定し、アクセス許可リクエストを送信します (「Oracle Database@AWS と IAM の連携方法」を参照)
- IAM 管理者 - アクセスを管理するためのポリシーを作成します (「Oracle Database@AWS のアイデンティティベースのポリシー」を参照)

アイデンティティによる認証

認証とは、アイデンティティ認証情報を使用して AWS にサインインする方法です。ユーザーは、IAM ユーザー の AWS アカウントのルートユーザー として、または IAM ロールを引き受けることによって、認証される 必要があります。

AWS IAM アイデンティティセンター (IAM アイデンティティセンター)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーテッドアイデンティティとしてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、AWS はリクエストに暗号で署名するための SDK と CLI を提供します。詳細については、「IAM ユーザーガイド」の「API リクエストに対する AWS 署名バージョン 4」を参照してください。

AWS アカウント のルートユーザー

AWS アカウントを作成すると、すべての AWS のサービスとリソースに対する完全なアクセス権を持つ AWS アカウント ルートユーザーと呼ばれる 1 つのサインイン ID を使用して開始します。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザー認証情報を必要とするタスクについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーテッドアイデンティティ

ベストプラクティスでは、人間のユーザーが一時的な認証情報を使用して AWS のサービス にアクセスする際、アイデンティティプロバイダーとのフェデレーションを使用することが求められます。

フェデレーテッドアイデンティティは、エンタープライズディレクトリ、ウェブ ID プロバイダー、Directory Service のユーザーであり、ID ソースからの認証情報を使用して AWS のサービスにアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、AWS IAM アイデンティティセンター をお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「IAM アイデンティティセンターとは」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの代わりに一時的な認証情報を使用することをお勧めします。詳細は「IAM ユーザーガイド」の「人間のユーザーが一時的な認証情報を使用して AWS にアクセスするには ID プロバイダーとのフェデレーションの使用が必要です」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替える、または AWS CLI や AWS API オペレーションを呼び出すことで、ロールを引き受けることができます。詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。詳細については、IAM ユーザーガイド の IAM でのクロスアカウントリソースアクセス を参照してください。

ポリシーを使用したアクセス権の管理

AWS でアクセスを制御するには、ポリシーを作成して AWS ID またはリソースにアタッチします。ポリシーは、アイデンティティやリソースとの関連付けに伴うアクセス許可を定義します。AWS は、プリンシパルがリクエストを行うときに、これらのポリシーを評価します。大半のポリシーは JSON ドキュメントとして AWS に保存されます。JSON ポリシードキュメントの詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

アイデンティティベースのポリシー

アイデンティティベースのポリシーは、アイデンティティ (ユーザー、グループ、またはロール) にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。アイデンティティベースポリシーの作成方法については、IAM ユーザーガイド の カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する を参照してください。

アイデンティティベースのポリシーは、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。管理ポリシーとインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。例としては、IAM ロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーで IAM の AWS マネージドポリシーを使用することはできません。

その他のポリシータイプ

AWS は、より一般的なポリシータイプで付与された最大数のアクセス許可を設定できる、追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできるアクセス許可の数の上限を設定します。詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可境界」を参照してください。
- サービスコントロールポリシー (SCP) - AWS Organizations 内の組織または組織単位の最大のアクセス許可を指定します。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。
- リソースコントロールポリシー (RCP) – は、アカウント内のリソースで利用できる最大数のアクセス許可を定義します。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを作成する際にパラメータとして渡される高度なポリシーです。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成されるアクセス許可を理解するのがさらに難しくなります。複数のポリシータイプが関連するとき、リクエストを許可するかどうかを AWS が決定する方法の詳細については、「IAM ユーザーガイド」の「ポリシーの評価ロジック」を参照してください。

Oracle Database@AWS と IAM の連携方法

IAM を使用して Oracle Database@AWS へのアクセスを管理する前に、Oracle Database@AWS で利用できる IAM の機能について説明します。

IAM の特徴量	Oracle Database@AWS のサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	あり
ポリシー条件キー	あり
ACL	なし
ABAC (ポリシー内のタグ)	部分的
一時認証情報	あり
プリンシパルアクセス権限	あり
サービスロール	いいえ
サービスリンクロール	はい

Oracle Database@AWS およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要を把握するには、「IAM ユーザーガイド」の「IAM と連携する AWS のサービス」を参照してください。

Oracle Database@AWS のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティ

ベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。JSON ポリシーで使用できるすべての要素について学ぶには、IAM ユーザーガイドのIAM JSON ポリシーの要素のリファレンスを参照してください。

Oracle Database@AWS のアイデンティティベースのポリシーの例

Oracle Database@AWS のアイデンティティベースポリシーの例を確認するには、「Oracle Database@AWS のアイデンティティベースのポリシー」を参照してください。

Oracle Database@AWS 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーションユーザー、または AWS のサービス を含めることができます。

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。詳細については、IAM ユーザーガイドのIAM でのクロスアカウントリソースアクセスを参照してください。

Oracle Database@AWS のポリシーアクション

ポリシーアクションのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのようなリソースにどのような条件でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

Oracle Database@AWS アクションのリストを確認するには、「サービス認可リファレンス」の「Oracle Database@AWS で定義されるアクション」を参照してください。

Oracle Database@AWS のポリシーアクションは、アクションの前に以下のプレフィックス を使用します。

```
odb
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "odb:action1",
      "odb:action2"
         ]
```

Oracle Database@AWS のアイデンティティベースポリシーの例を確認するには、「Oracle Database@AWS のアイデンティティベースのポリシー」を参照してください。

Oracle Database@AWS のポリシーリソース

ポリシーリソースのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

`Resource` JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。リソースレベルのアクセス許可をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

Oracle Database@AWS リソースのタイプとその ARN のリストを確認するには、「サービス認可リファレンス」の「Oracle Database@AWS で定義されるリソース」を参照してください。どのアクションで各リソースの ARN を指定できるかについては、「Oracle Database@AWS で定義されるアクション」を参照してください。

Oracle Database@AWS のアイデンティティベースポリシーの例を確認するには、「Oracle Database@AWS のアイデンティティベースのポリシー」を参照してください。

Oracle Database@AWS 向けのポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。イコールや未満などの条件演算子を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドのAWS グローバル条件コンテキストキーを参照してください。

Oracle Database@AWS の条件キーのリストを確認するには、「サービス認可リファレンス」の「Oracle Database@AWS の条件キー」を参照してください。条件キーを使用できるアクションおよびリソースについては、「Oracle Database@AWS で定義されるアクション」を参照してください。

Oracle Database@AWS のアイデンティティベースポリシーの例を確認するには、「Oracle Database@AWS のアイデンティティベースのポリシー」を参照してください。

Oracle Database@AWS の ACL

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Oracle Database@AWS を備えた ABAC

ABAC (ポリシー内のタグ) のサポート: 一部

属性ベースのアクセスコントロール (ABAC) は、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグを付けることで、プリンシパルのタグがリソースタグと一致するときに操作を許可する ABAC ポリシーを設計できます。

タグに基づいてアクセスを管理するには、aws:ResourceTag/*key-name*、aws:RequestTag/*key-name*、または aws:TagKeys の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

Oracle Database@AWS での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一時的な認証情報は、AWSリソースへの短期的なアクセスを提供し、フェデレーションの使用時またはロールの切り替え時に自動的に作成されます。AWS では、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをお勧めします。詳細については、「IAM ユーザーガイド」の「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」を参照してください。

Oracle Database@AWS のクロスサービスプリンシパル権限

転送アクセスセッション (FAS) のサポート: あり

転送アクセスセッション (FAS) は、AWS のサービスを呼び出すプリンシパルのアクセス許可と、リクエスト元の AWS のサービスを組み合わせて、ダウンストリームのサービスに対してリクエストを行います。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

Oracle Database@AWS のサービスロール

サービスロールのサポート: なし

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。

> **Warning**
>
> サービスロールの権限を変更すると、Oracle Database@AWS の機能が破損する可能性があります。Oracle Database@AWS が指示する場合以外は、サービスロールを編集しないでください。

Oracle Database@AWS のサービスリンクロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、AWS のサービスにリンクされているサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスにリンクされたロールは、AWS アカウント に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

Oracle Database@AWS サービスにリンクされたロールの作成または管理の詳細については、Oracle Database@AWS のサービスにリンクされたロールの使用 を参照してください。

Oracle Database@AWS のアイデンティティベースのポリシー

デフォルトでは、ユーザーとロールには Oracle Database@AWS リソースを作成または変更するアクセス許可はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。

これらのサンプルの JSON ポリシードキュメントを使用して IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

Oracle Database@AWS で定義されるアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、「サービス認可リファレンス」の「Oracle Database@AWS のアクション、リソース、および条件キー」を参照してください。

トピック

- ポリシーに関するベストプラクティス
- Oracle Database@AWS コンソールを使用する
- ユーザーに Oracle Database@AWS リソースのプロビジョニングを許可する

- 自分の権限の表示をユーザーに許可する

ポリシーに関するベストプラクティス

ID ベースのポリシーは、あるユーザーがアカウント内で Oracle Database@AWS リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS マネージドポリシーの使用を開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードへのアクセス許可の付与を開始するには、多くの一般的なユースケースのためにアクセス許可を付与する AWS マネージドポリシーを使用します。これらは AWS アカウントで使用できます。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。詳細については、IAM ユーザーガイド の AWS マネージドポリシー または ジョブ機能の AWS マネージドポリシー を参照してください。
- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイド の IAM でのポリシーとアクセス許可 を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。たとえば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。また、CloudFormation などの特定の AWS のサービスを介して使用する場合、条件を使用してサービスアクションへのアクセスを許可することもできます。詳細については、IAM ユーザーガイド の IAM JSON ポリシー要素:条件 を参照してください。
- IAM アクセスアナライザー を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM アクセスアナライザー は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の IAM Access Analyzer でポリシーを検証する を参照してください。
- 多要素認証 (MFA) を要求する – AWS アカウントで IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイド の MFA を使用した安全な API アクセス を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイド の IAM でのセキュリティのベストプラクティス を参照してください。

Oracle Database@AWS コンソールを使用する

Oracle Database@AWS コンソールにアクセスするには、許可の最小限のセットが必要です。これらのアクセス許可により、AWS アカウントの Oracle Database@AWS リソースの一覧と詳細を表示できます。最小限必要なアクセス許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) ではコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソール権限を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスを許可します。

ユーザーに Oracle Database@AWS リソースのプロビジョニングを許可する

このポリシーにより、ユーザーはプロビジョニング Oracle Database@AWS リソースへのフルアクセスが可能になります。VPC から DNS 解決を設定するには、アウトバウンド Route 53 リゾルバーを作成し、OCI ドメイン名を持つ DNS トラフィックを OCI DNS リスナー IP に転送するルールを追加します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowODBAndEC2Actions",
            "Effect": "Allow",
            "Action": [
                "odb:GetOciOnboardingStatus",
                "odb:CreateOdbNetwork",
                "odb:DeleteOdbNetwork",
                "odb:GetOdbNetwork",
                "odb:ListOdbNetworks",
                "odb:UpdateOdbNetwork",
                "odb:CreateOdbPeeringConnection",
                "odb:DeleteOdbPeeringConnection",
                "odb:GetOdbPeeringConnection",
                "odb:ListOdbPeeringConnections",
```

```
                "odb:PutResourcePolicy",
                "odb:GetResourcePolicy",
                "odb:DeleteResourcePolicy",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeVpcEndpointAssociations",
                "ec2:CreateVpcEndpoint",
                "ec2:DeleteVpcEndpoints",
                "ec2:DescribeVpcEndpoints"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowSLRActions",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "odb.amazonaws.com",
                        "vpc-lattice.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowTaggingActions",
            "Effect": "Allow",
            "Action": [
                "odb:TagResource",
                "odb:UntagResource",
                "odb:ListTagsForResource"
            ],
            "Resource": "arn:aws:odb:*:*:odb-network/*"
        },
        {
            "Sid": "AllowOdbVpcLatticeActions",
            "Effect": "Allow",
            "Action": [
                "vpc-lattice:CreateServiceNetwork",
                "vpc-lattice:DeleteServiceNetwork",
```

```
                "vpc-lattice:GetServiceNetwork",
                "vpc-lattice:CreateServiceNetworkResourceAssociation",
                "vpc-lattice:DeleteServiceNetworkResourceAssociation",
                "vpc-lattice:GetServiceNetworkResourceAssociation",
                "vpc-lattice:CreateResourceGateway",
                "vpc-lattice:DeleteResourceGateway",
                "vpc-lattice:GetResourceGateway",
                "vpc-lattice:CreateServiceNetworkVpcEndpointAssociation"
            ],
            "Resource": "*"
        }
    ]
}
```

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI か AWS API を使用してプログラム的に、このアクションを完了するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
```

```
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS の マネージドポリシーOracle Database@AWS

アクセス許可セットとロールにアクセス許可を追加するには、自分でポリシーを作成するよりも、AWS マネージドポリシーを使用する方が簡単です。チームに必要な権限のみを提供する IAM カスタマーマネージドポリシーを作成するには時間と専門知識が必要です。すぐに使用を開始するために、AWS マネージドポリシーを使用できます。これらのポリシーは、一般的なユースケースをターゲット範囲に含めており、AWS アカウント で利用できます。AWS マネージドポリシーの詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS のサービス は、AWS マネージドポリシーを維持し、更新します。AWS マネージドポリシーの権限を変更することはできません。サービスでは新しい機能を利用できるようにするために、AWS マネージドポリシーに権限が追加されることがあります。この種類の更新は、ポリシーがアタッチされている、すべてのアイデンティティ (アクセス許可セットとロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは、AWS マネージドポリシーから許可を削除しないため、ポリシーの更新によって既存の許可が破棄されることはありません。

さらに、AWS は複数のサービスにまたがるジョブ機能の特徴に対するマネージドポリシーもサポートしています。例えば、ReadOnlyAccess AWS マネージドポリシーでは、すべての AWS のサービス およびリソースへの読み取り専用アクセスを許可します。あるサービスで新しい機能を立ち上げる場合は、AWS は、追加された演算とリソースに対し、読み込み専用の許可を追加します。ジョブ機能のポリシーの一覧および詳細については、「IAM ユーザーガイド」の「AWS のジョブ機能のマネージドポリシー」を参照してください。

トピック

- AWS マネージドポリシー: AmazonODBServiceRolePolicy

AWS マネージドポリシー: AmazonODBServiceRolePolicy

IAM エンティティに `AmazonODBServiceRolePolicy` ポリシーをアタッチすることはできません。このポリシーは、ユーザーに代わって Oracle Database@AWS がアクションを実行することを許可する、サービスにリンクされたロールにアタッチされます。詳細については、「Oracle Database@AWS のサービスにリンクされたロールの使用」を参照してください。

JSON ポリシードキュメントの最新バージョンなど、ポリシーについてさらに詳しく確認するには、「AWS マネージドポリシーリファレンスガイド」の「AmazonODBServiceRolePolicy」を参照してください。

OCI における Oracle Database@AWS 認証と認可

AWS API を使用して Oracle Database@AWS のリソースを作成すると、それらのリソースはリンクされた Oracle Cloud Infrastructure (OCI) テナンシーに論理的に存在します。これらのリソースをデプロイするに、AWS はユーザーに代わって OCI API と通信します。混乱した代理問題を軽減するには、OCI と Oracle Database@AWS は AWS STS を信頼できるエンティティとして使用し、アクセスセッションを転送して、リンクされたテナンシーで OCI API を使用するインテントを承認します。そのため、OCI IP スペースからの `sts:getCallerIdentity` API のイベントが AWS CloudTrail の証跡とイベント履歴に記録されます。Oracle Database@AWS API を使用する場合は、これらのイベントが発生する可能性があります。

Oracle Database@AWS ID とアクセスのトラブルシューティング

次の情報は、Oracle Database@AWS と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- Oracle Database@AWS でアクションを実行する権限がない
- iam:PassRole を実行する権限がありません
- 自分の AWS アカウント 以外のユーザーに Oracle Database@AWS リソースへのアクセスを許可したい

Oracle Database@AWS でアクションを実行する権限がない

あるアクションを実行する権限がないというエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要な odb:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 odb:GetWidget on resource: my-example-widget
```

この場合、odb:*GetWidget* アクションを使用して *my-example-widget* リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、AWS 管理者に問い合わせてください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Oracle Database@AWS にロールを渡すことができるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールやサービスリンクロールを作成せずに、既存のロールをサービスに渡すことができます。そのためには、サービスにロールを渡すアクセス許可が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して Oracle Database@AWS でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与されたアクセス許可が必要です。Mary には、ロールをサービスに渡すアクセス許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、AWS 管理者に問い合わせてください。サインイン認証情報を提供した担当者が管理者です。

自分の AWS アカウント 以外のユーザーに Oracle Database@AWS リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外のユーザーが、リソースへのアクセスに使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまた

はアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください。

- Oracle Database@AWS がこれらの機能をサポートしているかどうかを確認するには、「Oracle Database@AWS と IAM の連携方法」を参照してください。
- 所有している AWS アカウント 全体のリソースへのアクセス権を提供する方法については、IAM ユーザーガイド の 所有している別の AWS アカウント へのアクセス権を IAM ユーザーに提供 を参照してください。
- サードパーティの AWS アカウント にリソースへのアクセス権を提供する方法については、「IAM ユーザーガイド」の「サードパーティが所有する AWS アカウント へのアクセス権を付与する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイド の 外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可 を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

Oracle Database@AWS のコンプライアンス検証

Oracle Database@AWS を使用する際のお客様のコンプライアンス責任は、お客様のデータの機密性や貴社のコンプライアンス目的、適用可能な法律および規制によって決定されます。クラウドでのコンプライアンスに関する Oracle のドキュメントは、Oracle ウェブサイトで入手できます。

Oracle Database@AWS での耐障害性

AWS グローバルインフラストラクチャは AWS リージョンおよびアベイラビリティーゾーンを中心に構築されています。AWS リージョンは、低レイテンシー、高スループット、そして高度な冗長ネットワークで接続される物理的に独立、隔離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンを使用すると、中断することなくゾーン間で自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用できます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョンとアベイラビリティーゾーンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

Oracle Database@AWS では、AWS グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズに対応できるように複数の機能を提供しています。

Oracle Database@AWS のサービスにリンクされたロールの使用

Oracle Database@AWS では AWS Identity and Access Management (IAM) のサービスリンクロールを使用します。サービスリンクロールは、Oracle Database@AWS に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは Oracle Database@AWS によって事前定義されており、サービスがユーザーに代わって他の AWS のサービス を呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールは必要なアクセス許可を手動で追加する必要がないため、より簡単に Oracle Database@AWS を使用できます。Oracle Database@AWS はこのサービスにリンクされたロールのアクセス許可を定義し、特に定義されている場合を除き、Oracle Database@AWS のみがそのロールを引き受けます。定義されたアクセス許可には、信頼ポリシーとアクセス許可ポリシーが含まれ、そのアクセス許可ポリシーを他の IAM エンティティにアタッチすることはできません。

ロールを削除するには、まず関連リソースを削除します。これにより、リソースにアクセスするための許可を意図せず削除することが防止され、Oracle Database@AWS リソースが保護されます。

Oracle Database@AWS のサービスリンクロールのアクセス許可

Oracle Database@AWS は、AWSServiceRoleForODB というサービスにリンクされたロールを使用して、Oracle Database@AWS がリソースの代わりに AWS のサービスを呼び出せるようにします。

サービスにリンクされたロール AWSServiceRoleForODB は、次のサービスを信頼してロールを引き受けます。

- `odb.amazonaws.com`
- `vpc-lattice.amazonaws.com`

このサービスにリンクされたロールには、アカウントで操作するためのアクセス許可を付与する `AmazonODBServiceRolePolicy` というアクセス許可ポリシーがアタッチされています。詳細については、「AWS マネージドポリシー: AmazonODBServiceRolePolicy」を参照してください。

> **Note**
>
> サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、許可を設定する必要があります。次のエラーメッセージが表示された場合は、以下のように対応します。
> リソースを作成できません。サービスにリンクされたロールを作成するために必要なアクセス許可があることを確認します。それ以外の場合は、時間をおいてからもう一度お試しください。
> 次のアクセス許可が有効であることを確認します。
>
> ```
> {
>     "Action": "iam:CreateServiceLinkedRole",
>     "Effect": "Allow",
>     "Resource": "arn:aws:iam::*:role/aws-service-role/odb.amazonaws.com/
> AWSServiceRoleForODB",
>     "Condition": {
>         "StringLike": {
>             "iam:AWSServiceName":"odb.amazonaws.com",
>             "iam:AWSServiceName":"vpc-lattice.amazonaws.com"
>         }
>     }
> }
> ```
>
> 詳細については、「IAM ユーザーガイド」の「サービスリンクされたロールのアクセス許可」を参照してください。

Oracle Database@AWS のサービスリンクロールの作成

サービスリンクロールを手動で作成する必要はありません。Exadata データベースを作成すると、Oracle Database@AWS によって、サービスにリンクされたロールが作成されます。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は同じ方法でアカウントにロールを再作成できます。Exadata データベースを作成すると、Oracle Database@AWS によって、サービスにリンクされたロールが再度作成されます。

Oracle Database@AWS のサービスにリンクされたロールの編集

Oracle Database@AWS では、AWSServiceRoleForODB のサービスにリンクされたロールを編集することはできません。サービスリンクロールの作成後は、さまざまなエンティティがロールを参照す

る可能性があるため、ロール名を変更することはできません。ただし、IAM を使用してロールの説明を編集することはできます。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの編集」を参照してください。

Oracle Database@AWS のサービスリンクロールの削除

サービスリンクロールを必要とする機能やサービスが不要になった場合は、ロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングされたり、メンテナンスされたりすることがなくなります。ただし、サービスにリンクされたロールを削除する前に、すべてのリソースを削除する必要があります。

Oracle Database@AWS のサービスリンクロールのクリーンアップ

IAM を使用してサービスにリンクされたロールを削除するには、まずそのロールにアクティブなセッションがないことを確認し、そのロールで使用されているリソースをすべて削除する必要があります。

サービスにリンクされたロールにアクティブなセッションがあるかどうかを、IAM コンソールで確認するには

1. AWS マネジメントコンソール にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. IAM コンソールのナビゲーションペインで [ロール] を選択します。次に、AWSServiceRoleForODB ロールの名前 (チェックボックスではありません) を選択します。
3. 選択したロールの [概要] ページで、[アクセスアドバイザー] タブを選択します。
4. [Access Advisor] タブで、サービスにリンクされたロールの最新のアクティビティを確認します。

> **Note**
>
> Oracle Database@AWS が [AWSServiceRoleForODB] ロールを使用しているかどうか不明な場合は、ロールを削除してみてください。サービスでロールが使用されている場合、削除は失敗し、ロールが使用されている AWS リージョン リージョンを表示できます。ロールが使用されている場合は、ロールを削除する前にセッションが終了するのを待つ必要があります。サービスにリンクされたロールのセッションを取り消すことはできません。

AWSServiceRoleForODB ロールを削除する場合は、まず Oracle Database@AWS リソースをすべて削除する必要があります。

Oracle Database@AWS のサービスにリンクされたロールをサポートするリージョン

Oracle Database@AWS では、このサービスが利用可能なすべての AWS リージョン で、サービスリンクロールの使用をサポートしています。詳細については、「AWS リージョン およびエンドポイント」を参照してください。

AWS マネージドポリシーに対する Oracle Database@AWS の更新

このサービスがこれらの変更の追跡を開始してからの、Oracle Database@AWS の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動通知については、[Oracle Database@AWS Document history] (ドキュメントの履歴) ページの RSS フィードをサブスクライブしてください。

変更	説明	日付
Oracle Database@AWS のサービスリンクロールのアクセス許可 – 既存のポリシーの更新	Oracle Database@AWS は、`AWSServiceRoleForODB` サービスにリンクされたロールの `AmazonODBServiceRolePolicy` に新しいアクセス許可を追加しました。これらのアクセス許可により、Oracle Database@AWS は次の手順を実行できます。 • Amazon VPC Transit Gateway アタッチメントの記述 • Amazon EC2 アタッチメントの記述 • Amazon EventBridge ソースのアクティブ化 詳細については、「Oracle Database@AWS のサービスリンクロールのアクセス許可」を参照してください。	2025 年 6 月 30 日

変更	説明	日付
Oracle Database@AWS のサービスリンクロールのアクセス許可 – 既存のポリシーの更新	Oracle Database@AWS は、AWSServiceRoleForODB サービスにリンクされたロールの AmazonODBServiceRolePolicy に新しいアクセス許可を追加しました。これらのアクセス許可により、Oracle Database@AWS は次の手順を実行できます。 • Amazon EventBridge ソースの記述 • イベントバスの記述と作成 詳細については、「Oracle Database@AWS のサービスリンクロールのアクセス許可」を参照してください。	2025 年 6 月 26 日
AWS マネージドポリシー: AmazonODBServiceRolePolicy – 新しいサービスリンクロールポリシー	Oracle Database@AWS は、AWSServiceRoleForODB サービスリンクロールに AmazonODBServiceRolePolicy を追加しました。詳細については、「AWS マネージドポリシー: AmazonODBServiceRolePolicy」を参照してください。	2024 年 12 月 2 日
Oracle Database@AWS は変更の追跡を開始しました	Oracle Database@AWS が AWS マネージドポリシーの変更の追跡を開始しました。	2024 年 12 月 2 日

Oracle Database@AWS のモニタリング

モニタリングは、Oracle Database@AWS とその他 AWS ソリューションの信頼性、可用性、およびパフォーマンスの維持における重要な要素です。AWS は、Oracle Database@AWS をモニタリングし、問題が発生した場合には報告を行い、必要に応じて自動アクションを実行するために以下のモニタリングツールを提供しています。

- Amazon CloudWatch は、AWS のリソースおよび AWS で実行しているアプリケーションをリアルタイムでモニタリングします。メトリクスの収集と追跡、カスタマイズしたダッシュボードの作成、および指定したメトリクスが指定したしきい値に達したときに通知またはアクションを実行するアラームの設定を行うことができます。例えば、CloudWatch で Amazon EC2 インスタンスの CPU 使用率などのメトリクスを追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。
- Amazon CloudWatch Logs では、Amazon EC2 インスタンス、CloudTrail、その他ソースから得たログファイルのモニタリング、保存、およびアクセスが可能です。CloudWatch Logs は、ログファイル内の情報をモニタリングし、特定のしきい値が満たされたときに通知します。高い耐久性を備えたストレージにログデータをアーカイブすることも可能です。詳細については、「Amazon CloudWatch Logs ユーザーガイド」を参照してください。
- Amazon EventBridge を使用すると、AWS のサービスを自動化し、アプリケーションの可用性の問題やリソースの変更などのシステムイベントに自動的に対応できます。AWS のサービスからのイベントは、ほぼリアルタイムに EventBridge に提供されます。簡単なルールを記述して、注目するイベントと、イベントがルールに一致した場合に自動的に実行するアクションを指定できます。詳細については、「Amazon EventBridge ユーザーガイド」を参照してください。
- AWS CloudTrail は、AWS アカウントにより、またはそのアカウントに代わって行われた API コールや関連イベントを取得し、指定した Amazon S3 バケットにログファイルを配信します。AWS を呼び出したユーザーとアカウント、呼び出し元の IP アドレス、および呼び出しの発生日時を特定できます。詳細については、AWS CloudTrailユーザーガイドを参照してください。

Amazon CloudWatch での Oracle Database@AWS のモニターリング

raw データを収集して読み取り可能なほぼリアルタイムのメトリクスに処理する CloudWatch を使用して Oracle Database@AWS をモニタリングできます。これらの統計は 15 か月間保持されるため、履歴情報にアクセスし、ウェブアプリケーションまたはサービスの動作をより的確に把握できます。また、特定のしきい値を監視するアラームを設定し、これらのしきい値に達したときに通知を送

信したりアクションを実行したりできます。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

Oracle Database@AWS の Amazon CloudWatch メトリクス

この Oracle Database@AWS サービスは、VM クラスター、コンテナデータベース、およびプラグ可能なデータベースの AWS/ODB 名前空間で Amazon CloudWatch にメトリクスを報告します。

トピック

クラウド VM クラスターのメトリクス

Oracle Database@AWS サービスは、クラウド VM クラスターの AWS/ODB 名前空間の以下のメトリクスをレポートします。

メトリクス	説明	単位
ASMDiskgroupUtilization	Disk Group で使用される使用可能なスペースの割合。使用可能なスペースは、拡張可能なスペースです。DATA ディスクグループは Oracle データベースファイルを保存します。RECO ディスクグループには、アーカイブやフラッシュバックログなどの復旧用のデータベースファイルが含まれています。	割合 (%)
CpuUtilization	CPU 使用率。	割合 (%)
FilesystemUtilization	プロビジョニングされたファイルシステムの使用率。	割合 (%)

メトリクス	説明	単位
LoadAverage	5 分間のシステム負荷の平均。	整数
MemoryUtilization	スワップなしで新しいアプリケーションを開始するのに使用可能なメモリの割合。使用可能なメモリは、次のコマンドで取得できます。cat /proc/meminfo	割合 (%)
NodeStatus	ホストが到達可能かどうかを示します。	整数
OcpusAllocated	割り当てられた OCPUの数。	整数
SwapUtilization	合計スワップスペースの使用率。	割合 (%)

コンテナデータベースのメトリクス

Oracle Database@AWS サービスは、コンテナデータベースの AWS/ODB 名前空間の以下のメトリクスをレポートします。

メトリクス	説明	単位
BlockChanges	1 秒あたりに変更された平均ブロック数。	1 秒あたりの変更
CpuUtilization	すべてのコンシューマーグループで集計された、パーセンテージ表示の CPU 使用率。使用率は、データベースが使用できる CPU の数に関して報告されます。これは OCPU の二倍になります。	割合 (%)

メトリクス	説明	単位
CurrentLogons	選択した間隔中に成功したログオンの数。	カウント
ExecuteCount	選択した間隔中に SQL ステートメントを実行したユーザー呼び出しと再帰呼び出しの数。	カウント
ParseCount	選択した間隔中のハード解析とソフト解析の数。	カウント
StorageAllocated	収集時にデータベースに割り当てられたストレージスペースの合計。	GB
StorageAllocatedByTablespace	収集時にテーブルスペースに割り当てられたストレージスペースの合計。コンテナデータベースの場合、このメトリクスはルートコンテナテーブルスペースを提供します。	GB
StorageUsed	収集時にデータベースが使用したストレージスペースの合計。	GB
StorageUsedByTablespace	収集時にテーブルスペースが使用したストレージスペースの合計。コンテナデータベースの場合、このメトリクスはルートコンテナテーブルスペースを提供します。	GB

メトリクス	説明	単位
StorageUtilization	現在使用中のプロビジョニングされたストレージ容量の割合。すべてのテーブルスペースに割り当てられたスペースの合計を表します。	割合 (%)
StorageUtilizationByTablespace	これは、収集時にテーブルスペースが利用したストレージ容量の割合を示します。コンテナデータベースの場合、このメトリクスはルートコンテナテーブルスペースを提供します。	割合 (%)
TransactionCount	選択した間隔中のユーザーコミットとユーザーロールバックの合計数。	カウント
UserCalls	選択した間隔中のログオン、解析、および実行呼び出しの合計数。	カウント

プラグ可能なデータベースのメトリクス

Oracle Database@AWS サービスは、プラグ可能なデータベースの AWS/ODB 名前空間の以下のメトリクスをレポートします。

メトリクス	説明	単位
AllocatedStorageUtilizationByTablespace	割り当てられたすべてから、テーブルスペースが使用するスペースの割合。コンテナデータベースの場合、このメトリクスはルートコンテナテーブルスペースのデータを	割合 (%)

メトリクス	説明	単位
	提供します。(統計: 平均値、間隔: 30 分)	
AvgGCCRBlockReceiveTime	グローバルキャッシュ CR (整合性のある読み込み) ブロックの平均受信時間。RAC / クラスターデータベースのみ。(統計: 平均値、間隔: 5 分)	ミリ秒
AvgGCCurrentBlockReceiveTime	グローバルキャッシュの現在のブロックの平均受信時間。統計は平均値をレポートします。Real Application Cluster (RAC) データベースのみ。(統計: 平均値、間隔: 5 分)	ミリ秒
BlockChanges	1 秒あたりに変更された平均ブロック数。(統計: 平均値、間隔: 1 分)	1 秒あたりの変更
BlockingSessions	現在のブロッキングセッション。コンテナデータベースには適用されません。(統計: 最大、間隔: 15 分)	カウント
CPUTimeSeconds	時間間隔におけるデータベースインスタンスのフォアグラウンドセッションごとの CPU 累積時間の平均レート。平均アクティブセッションの CPU 時間コンポーネント。(統計: 平均値、間隔: 1 分)	1 秒あたりの秒数
CpuCount	選択した間隔中の CPU の数。	カウント

メトリクス	説明	単位
CpuUtilization	すべてのコンシューマーグループで集計された、パーセンテージ表示の CPU 使用率。使用率は、データベースが使用できる CPU の数に関して報告されます。これは OCPU の二倍になります。(統計: 平均値、間隔: 1 分)	割合 (%)
CurrentLogons	選択した間隔中に成功したログオンの数。(統計: 合計、間隔: 1 分)	カウント
DBTimeSeconds	時間間隔におけるデータベースインスタンスのフォアグラウンドセッションごとのデータベース累積時間 (CPU + 待機) の平均レート。平均アクティブセッションとも呼ばれます。(統計: 平均値、間隔: 1 分)	1 秒あたりの秒数
DbmgmtJobExecutionsCount	1 つのマネージドデータベースまたはデータベースグループで実行された SQL ジョブの数とそのステータス。ステータスディメンションの値は、「成功」、「失敗」、「進行中」になります。(統計: 合計、間隔: 1 分)	カウント
ExecuteCount	選択した間隔中に SQL ステートメントを実行したユーザー呼び出しと再帰呼び出しの数。(統計: 合計、間隔: 1 分)	カウント

メトリクス	説明	単位
FRASpaceLimit	フラッシュ復旧エリアスペースの制限。プラグ可能なデータベースには適用されません。(統計: 最大、間隔: 15 分)	GB
FRAUtilization	フラッシュリカバリエリアの使用率。プラグ可能なデータベースには適用されません。(統計: 平均値、間隔: 15 分)	割合 (%)
GCCRBlocksReceived	1 秒あたりに受信したグローバルキャッシュ CR (整合性のある読み込み) ブロック。RAC / クラスターデータベースのみ。(統計: 平均値、間隔: 5 分)	1 秒あたりのブロック数
GCCurrentBlocksReceived	1 秒あたりに受信したグローバルキャッシュの現在のブロックを表します。統計は平均値をレポートします。Real Application Cluster (RAC) データベースのみ。(統計: 平均値、間隔: 5 分)	1 秒あたりのブロック数
IOPS	1 秒あたりの入出力操作の平均回数。(統計: 平均値、間隔: 1 分)	1 秒あたりのオペレーション数
IOThroughputMB	1 秒あたりの MB 単位の平均スループット。(統計: 平均値、間隔: 1 分)	MB 毎秒

メトリクス	説明	単位
InterconnectTraffi cMB	平均ノード間データ転送レート。RAC / クラスターデータベースのみ。(統計: 平均値、間隔: 5 分)	MB 毎秒
InvalidObjects	データベースオブジェクト数が無効です。コンテナデータベースには適用されません。(統計: 最大、間隔: 24 時間)	カウント
LogicalBlocksRead	1 秒あたりに SGA/メモリ (バッファキャッシュ) から 読み取られた平均ブロック数。(統計: 平均値、間隔: 1 分)	1 秒あたりの読み取り数
MaxTablespaceSize	可能な最大テーブルスペースサイズ。コンテナデータベースの場合、このメトリクスはルートコンテナテーブルスペースのデータを提供します。(統計: 最大、間隔: 30 分)	GB
MemoryUsage	MB 単位のメモリプールの合計サイズ。(統計: 平均値、間隔: 15 分)	MB
MonitoringStatus	リソースのモニタリングステータス。メトリクスの収集が失敗すると、エラー情報がこのメトリクスにキャプチャされます。(統計: 平均値、間隔: 5 分)	該当しない

メトリクス	説明	単位
NonReclaimableFRA	再利用不可能な高速復旧エリア。プラグ可能なデータベースには適用されません。(統計: 平均値、間隔: 15 分)	割合 (%)
OcpusAllocated	選択した間隔中にサービスが割り当てた OCPU の実際の数。(統計: カウント、間隔: 1 分)	整数
ParseCount	選択した間隔中のハード解析とソフト解析の数。(統計: 合計、間隔: 1 分)	カウント
ParsesByType	1 秒あたりのハード解析またはソフト解析の数。(統計: 平均値、間隔: 1 分)	1 秒あたりの分析数
ProblematicScheduledDBMSJobs	問題のあるスケジュールされたデータベースジョブの数。コンテナデータベースには適用されません。(統計: 最大、間隔: 15 分)	カウント
ProcessLimitUtilization	プロセス制限の使用率。プラグ可能なデータベースには適用されません。(統計: 平均値、間隔: 1 分)	割合 (%)
Processes	データベースはカウントを処理します。プラグ可能なデータベースには適用されません。(統計: 最大、間隔: 1 分)	カウント

メトリクス	説明	単位
ReclaimableFRA	再利用可能な高速復旧エリア。プラグ可能なデータベースには適用されません。(統計: 平均値、間隔: 15 分)	割合 (%)
ReclaimableFRASpace	フラッシュリカバリエリアの再利用可能なスペース。プラグ可能なデータベースには適用されません。(統計: 平均値、間隔: 15 分)	GB
RedoSizeMB	1 秒あたりに生成された REDO の平均量 (MB 単位)。(統計: 平均値、間隔: 1 分)	MB 毎秒
SessionLimitUtilization	セッション制限の使用率。プラグ可能なデータベースには適用されません。(統計: 平均値、間隔: 1 分)	割合 (%)
Sessions	データベースのセッション数。(統計: 平均値、間隔: 1 分)	カウント
StorageAllocated	間隔中にテーブルスペースが割り当てたスペースの最大量。コンテナデータベースの場合、このメトリクスはルートコンテナテーブルスペースのデータを提供します。(統計: 最大、間隔: 30 分)	GB

メトリクス	説明	単位
StorageAllocatedByTablespace	間隔中にテーブルスペースが割り当てたスペースの最大量。コンテナデータベースの場合、このメトリクスはルートコンテナテーブルスペースのデータを提供します。(統計: 最大、間隔: 30 分)	GB
StorageUsed	間隔中に使用されたスペースの最大量。(統計: 最大、間隔: 30 分)	GB
StorageUsedByTablespace	間隔中にテーブルスペースが使用したスペースの最大量。コンテナデータベースの場合、このメトリクスはルートコンテナテーブルスペースのデータを提供します。(統計: 最大、間隔: 30 分)	GB
StorageUtilization	現在使用中のプロビジョニングされたストレージ容量の割合。すべてのテーブルスペースに割り当てられたスペースの合計を表します。(統計: 平均値、間隔: 30 分)	割合 (%)
StorageUtilizationByTablespace	テーブルスペースが使用したスペースの割合。コンテナデータベースの場合、このメトリクスはルートコンテナテーブルスペースのデータを提供します。(統計: 平均値、間隔: 30 分)	割合 (%)

メトリクス	説明	単位
TransactionCount	選択した間隔中のユーザーコミットとユーザーロールバックの合計数。(統計: 合計、間隔: 1 分)	カウント
TransactionsByStatus	1 秒あたりにコミットまたはロールバックされたトランザクションの数。(統計: 平均値、間隔: 1 分)	1 秒あたりのトランザクション
UnusableIndexes	データベーススキーマで使用できないインデックスの数。コンテナデータベースには適用されません。(統計: 最大、間隔: 24 時間)	カウント
UsableFRA	使用可能な高速復旧エリア。プラグ可能なデータベースには適用されません。(統計: 平均値、間隔: 15 分)	割合 (%)
UsedFRASpace	フラッシュ復旧エリアスペースの使用状況。プラグ可能なデータベースには適用されません。(統計: 最大、間隔: 15 分)	GB
UserCalls	選択した間隔中のログオン、解析、および実行呼び出しの合計数。(統計: 合計、間隔: 1 分)	カウント

メトリクス	説明	単位
WaitTimeSeconds	時間間隔におけるデータベースインスタンスのフォアグラウンドセッションごとのアイドル状態でない累積待機時間の平均レート。平均アクティブセッションの待機時間コンポーネント。(統計: 平均値、間隔: 5 分)	1 秒あたりの秒数

Oracle Database@AWS 用の Amazon CloudWatch ディメンション

次の表に示す任意のディメンションを使用して、Oracle Database@AWS メトリクスデータをフィルタリングができます。

ディメンション	以下で要求されたデータをフィルタリングします。
cloudVmClusterId	VM クラスターの識別子。
cloudExadataInfrastructureId	Exadata インフラストラクチャの識別子。
collectionName	コレクションの名前。
deploymentType	インフラストラクチャのタイプ。
diskgroupName	ディスクグループの名前
errorCode	エラーコード。
errorSeverity	エラーの重要度。
filesystemName	ファイルシステムの名前。
hostName	ホストマシンの名前。
instanceName	データベースインスタンスの名前。

ディメンション	以下で要求されたデータをフィルタリングします。
instanceNumber	データベースインスタンスのインスタンス番号。
ioType	I/O オペレーションのタイプ。
jobId	ジョブの一意の識別子。
managedDatabaseGroupId	Managed Database Group の識別子。
managedDatabaseId	Managed Database の識別子。
memoryPool	メモリプールのタイプ。
memoryType	メモリのタイプ。
ociCloudVmClusterId	VM クラスターの OCI 識別子。
ociCloudExadataInfrastructureId	Exadata インフラストラクチャの OCI 識別子。
parseType	解析のタイプ。
resourceId	リソースの識別子。
resourceId_Database	データベースの識別子。
resourceId_DbNode	データベースノードの識別子。
resourceName	リソースの名前です。
resourceName_Database	データベースの名前。
resourceName_DbNode	データベースノードの名前。
resourceType	データベースのタイプ。
schemaName	スキーマの名前。

ディメンション	以下で要求されたデータをフィルタリングします。
status	データベースのステータス。
tablespaceContents	テーブルスペースの内容。
tablespaceName	テーブルスペースの名前。
tablespaceType	テーブルスペースのタイプ。
transactionStatus	トランザクションのステータス。
waitClass	待機イベントのクラス。

Amazon EventBridge で Oracle Database@AWS イベントをモニタリングする

EventBridge で Oracle Database@AWS イベントをモニタリングできます。EventBridge では、アプリケーションおよび AWS サービスからのリアルタイムデータのストリームを提供します。EventBridge は、このデータを AWS Lambda や Amazon Simple Notification Service などのターゲットにルーティングします。

> **Note**
>
> EventBridge は、以前は Amazon CloudWatch Events と呼ばれていました。詳細については、「Amazon EventBridge ユーザーガイド」の「EventBridge は、Amazon CloudWatch Events の進化形です」を参照してください。

Oracle Database@AWS イベントの概要

Oracle Database@AWS イベントは、リソースライフサイクルの変更を示す構造化メッセージです。イベントバスは、イベントを受信して、ゼロ個以上の送信先またはターゲットに配信するルーターです。Oracle Database@AWS イベントは以下のソースから生成されます。

AWS からのイベント

これらのイベントは AWS 側の Oracle Database@AWS API から生成され、AWS アカウントのデフォルトのイベントバスに配信されます。

OCI からのイベント

これらのイベントは、Oracle Exadata インフラストラクチャや VM クラスターに関連するイベントなど、OCI から直接生成されます。Oracle Database@AWS にサブスクライブすると、OCI からイベントを受信するために、プレフィックス `aws.partner/odb/` が付いたイベントバスが AWS アカウントに作成されます。

AWS からの Oracle Database@AWS イベント

AWS からの Oracle Database@AWS イベントには、作成および削除中の ODB ネットワークに関連するライフサイクルの変更が含まれます。これらのイベントは、AWS アカウント のデフォルトのイベントバスに配信されます。配信タイプは、ベストエフォートです。

ODB ネットワークイベント

イベント	イベント ID	メッセージ
作成	ODB-EVENT-0001	ODB ネットワーク odbnet_ID が正常に作成されました
作成に失敗	ODB-EVENT-0011	ODB ネットワーク odbnet_ID の作成に失敗しました
削除	ODB-EVENT-0002	ODB ネットワーク odbnet_ID が正常に削除されました
削除に失敗	ODB-EVENT-0012	ODB ネットワーク odbnet_ID の削除に失敗しました

例: ODB ネットワークの作成イベント

次の例は、ODB ネットワークの作成に成功したイベントを示しています。

```
{
```

```
  "version": "0",
  "id": "01234567-EXAMPLE",
  "detail-type": "ODB Network Event",
  "source": "aws.odb",
  "account": "123456789012",
  "time": "2025-06-12T10:23:43Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:odb:us-east-1:123456789012:odbnetwork/odbnet-1234567890abcdef"
  ],
  "detail": {
    "eventId": "ODB-EVENT-0001",
    "message": "Successfully created ODB network odbnet-1234567890abcdef"
  }
}
```

OCI からの Oracle Database@AWS イベント

ほとんどのイベントは OCI から直接生成されます。Oracle Database@AWS は、OCI からイベントを受信するためのプレフィックス `aws.partner/odb/` を持つイベントバスを AWS アカウントに作成します。このイベントバスは削除しないことをお勧めします。

OCI は、次のような包括的なイベントタイプを提供します。

- Oracle Exadata インフラストラクチャ
- VM クラスターイベント
- CDB イベント
- PDB イベント

OCI がサポートする特定のイベントタイプと詳細については、「Oracle Exadata Database Service on Dedicated Infrastructure Events」および「Events for Autonomous Database on Dedicated Exadata Infrastructure」を参照してください。

Oracle Database@AWS イベントのフィルタリング

Amazon EventBridge のイベントバスでイベントバス設定に関する EventBridge の推奨ベストプラクティスに従うことができます。ユースケースに応じて、EventBridge ルールを設定して、イベントを受信および使用するイベントとターゲットをフィルタリングできます。

AWS からの ODB ネットワークイベントのフィルタリング

AWS からの ODB ネットワークイベントの場合、次のイベントパターンを使用してフィルタリングできます。

```
{
  "source": ["aws.odb"],
  "detail-type": ["ODB Network Event"]
}
```

このパターンは、デフォルトのイベントバスで EventBridge `put-rule` API を使用して適用できます。詳細については、「Amazon EventBridge API リファレンス」の「PutRule」を参照してください。

OCI からの Oracle Database@AWS イベントのフィルタリング

OCI からの Oracle Database@AWS イベントの場合、「Amazon EventBridge API リファレンス」の「PutRule」の例のようなコマンドを使用してルールを設定できます。以下のガイドラインに注意してください。

- フィルタリングするイベントタイプに応じて、カスタムイベントパターンを使用します。
- Oracle Database@AWS が作成したバスの名前に、EventBusNameを設定します。

イベントをフィルタリングし、アカウント間で EventBridge ターゲットを設定する方法の詳細については、「Amazon EventBridge の AWS アカウント間でイベントを送受信する」を参照してください。

Oracle Database@AWS イベントのトラブルシューティング

イベント配信またはイベントコンテンツで問題が発生した場合、以下を実行します。

- ODB ネットワークイベントについては、AWS サポート にお問い合わせください。
- ODB ネットワークイベント以外の Oracle Database@AWS イベントについては、Oracle Cloud Support にお問い合わせください。

詳細については、「Oracle Database@AWS のサポートを取得する」を参照してください。

Oracle Database@AWSを使用したAWS CloudTrailAPI コールのログ記録

Oracle Database@AWS は、ユーザー、ロール、または AWS のサービス によって実行されたアクションの記録を提供するサービスである AWS CloudTrail と統合されています。CloudTrail は、Oracle Database@AWS のすべての API コールをイベントとしてキャプチャします。キャプチャされたコールには、Oracle Database@AWS コンソールのコールと、Oracle Database@AWS API オペレーションへのコードのコールが含まれます。CloudTrail で収集された情報を使用して、Oracle Database@AWS に対するリクエスト、リクエスト元の IP アドレス、リクエストの作成日時、その他の詳細を確認できます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- ルートユーザーまたはユーザー認証情報のどちらを使用してリクエストが送信されたか。
- リクエストが IAM Identity Center ユーザーに代わって行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービス によって送信されたかどうか。

> **Note**
>
> Oracle Database@AWS は、AWS Security Token Service (STS) からの `GetCallerIdentity` API コールを CloudTrail ログに記録します。これらの STS API コールは、ユーザーに代わって OCI とやり取りするときに Oracle Database@AWS の ID を検証します。これらは、正常かつ安全な AWS オペレーションで、機密情報を公開しません。

アカウントを作成すると、AWS アカウント で CloudTrail がアクティブになり、自動的に CloudTrail の[イベント履歴] にアクセスできるようになります。CloudTrail の [イベント履歴] では、AWS リージョン で過去 90 日間に記録された管理イベントの表示、検索、およびダウンロードが可能で、変更不可能な記録を確認できます。詳細については、「AWS CloudTrail ユーザーガイド」の「CloudTrail イベント履歴の使用」を参照してください。[イベント履歴] の閲覧には CloudTrail の料金はかかりません。

AWS アカウント で過去 90 日間のイベントを継続的に記録するには、証跡または CloudTrail Lake イベントデータストアを作成します。

CloudTrail 証跡

証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。AWS マネジメントコンソール を使用して作成した証跡はマルチリージョンです。AWS CLI を使用する際は、単一リージョンまたは複数リージョンの証跡を作成できます。アカウント内のすべて AWS リージョン でアクティビティを把握するため、マルチリージョン証跡を作成することをお勧めします。単一リージョンの証跡を作成する場合、証跡の AWS リージョン に記録されたイベントのみを表示できます。証跡の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS アカウントの証跡の作成」および「組織の証跡の作成」を参照してください。

証跡を作成すると、進行中の管理イベントのコピーを 1 つ無料で CloudTrail から Amazon S3 バケットに配信できますが、Amazon S3 ストレージには料金がかかります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

CloudTrail Lake イベントデータストア

[CloudTrail Lake] を使用すると、イベントに対して SQL ベースのクエリを実行できます。CloudTrail Lake は、行ベースの JSON 形式の既存のイベントを Apache ORC 形式に変換します。ORC は、データを高速に取得するために最適化された単票ストレージ形式です。イベントは、イベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基づいた、イベントのイミュータブルなコレクションです。どのイベントが存続し、クエリに使用できるかは、イベントデータストアに適用するセレクタが制御します。CloudTrail Lake の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS CloudTrail Lake の使用」を参照してください。

CloudTrail Lake のイベントデータストアとクエリにはコストがかかります。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。

Oracle Database@AWSCloudTrail の 管理イベント

管理イベントでは、AWS アカウント のリソースに対して実行される管理オペレーションについての情報が得られます。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。CloudTrail は、デフォルトで管理イベントをログ記録します。

Oracle Database@AWS は、すべての Oracle Database@AWS コントロールプレーンオペレーションを管理イベントとして記録します。

Oracle Database@AWS イベントの例

各イベントは任意の送信元からの単一のリクエストを表し、リクエストされた API オペレーション、オペレーションの日時、リクエストパラメータなどに関する情報を含みます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、イベントは特定の順序で表示されません。

次の例は、CreateOdbNetwork オペレーションを示す CloudTrail イベントを示しています。


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:yourRole",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/yourRole",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-11-06T21:17:29Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-11-06T21:17:44Z",
    "eventSource": "odb.amazonaws.com",
```

```
    "eventName": "CreateOdbNetwork",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "python-requests/2.28.2",
    "requestParameters": {
        "availabilityZoneId": "use1-az6",
        "backupSubnetCidr": "123.45.6.7/89",
        "clientSubnetCidr": "123.44.6.7/89",
        "clientToken": "testClientToken",
        "defaultDnsPrefix": "testLabel",
        "displayName": "yourOdbNetwork"
    },
    "responseElements": {
        "displayName": "yourOdbNetwork",
        "odbNetworkId": "odbnet_1234567",
        "status": "PROVISIONING"
    },
    "requestID": "daf2e3f5-96a3-4df7-a026-863f96db793e",
    "eventID": "797163d3-5726-441d-80a7-6eeb7464acd4",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "odb.us-east-1.amazonaws.com"
    }
}
```


CloudTrail レコードの内容については、「AWS CloudTrail ユーザーガイド」の「CloudTrail record contents」を参照してください。

Oracle Database@AWS のトラブルシューティング

以下のセクションは、Oracle Database@AWS で発生する可能性のあるネットワーク問題のトラブルシューティングに役立ちます。

トピック

ODB ネットワークの作成に失敗する

ODB ネットワークを作成できない場合の一般的な原因は次のとおりです。

制限された CIDR 範囲

ODB ネットワークは、クライアントサブネットとバックアップサブネットに特定の CIDR 範囲を使用します。これらのサブネットに選択した CIDR 範囲が、制限されたまたは予約された IP アドレス範囲と重複していないことを確認します。

次の CIDR 範囲は予約されており、ODB ネットワークには使用できません。

- Oracle クラウドの予約済みの範囲: 169.254.0.0/16
- リザーブドクラス D: 224.0.0.0 - 239.255.255.255
- リザーブドクラス E: 240.0.0.0 - 255.255.255.255
- 今後の OCI の使用: 100.105.0.0/16

VPC ドキュメントで説明されている CIDR 範囲の EC2 ルールに従います。詳細については、「CIDR ブロック関連付けの制限」を参照してください。

さらに、指定された CIDR 範囲と ODB ネットワークへの VPC 接続に使用される CIDR 範囲との重複を回避します。

VPC CIDR の重複

ODB ネットワークに指定した CIDR 範囲は、既存の VPC で使用される CIDR 範囲と重複しないようにする必要があります。CIDR 範囲が重複すると、ルーティングの競合が発生し、ODB ネッ

トワークが正常に作成できなくなる可能性があります。ODB ピアリング VPC の CIDR 範囲を確認し、ODB ネットワークの CIDR が一意で、重複していないことを確認します。

VPC の所有権

接続する ODB ネットワークと VPC は、同じ AWS アカウントが所有している必要があります。ODB ネットワークを別のアカウントが所有する VPC にピアリングしようとすると、作成は失敗します。ODB ネットワークと VPC の両方が同じ AWS アカウントによって所有されていることを確認します。

トランジットゲートウェイがない

トランジットゲートウェイを VPC にアタッチせずに CIDR 範囲を ODB ネットワークにピア接続されている CIDR リストに追加すると、作成または更新オペレーションは失敗します。アタッチメントが使用される CIDR 範囲に関する要件はありません。

VPC と ODB ネットワークまたは VM クラスター間の接続の問題

VPC から ODB ネットワークまたは内部の VM クラスターに接続できない場合、一般的な原因は以下のとおりです。

- VPC 設定の検証 - Oracle Database@AWS コンソールで、ODB ネットワークとピア接続されている VPC を特定します。VPC ID が ODB ネットワークの詳細に表示されているものと一致していることを確認します。
- ルートテーブルの検査 - Amazon VPC コンソールで、アプリケーションが実行されているサブネットにアタッチされているルートテーブルを見つけます。ODB ネットワークのクライアントサブネットの CIDR に一致する送信先 CIDR とのルートを確認します。このルートが正しい ODB ネットワーク ARN を指していることを確認します。ルートがない場合、ODB ネットワークのクライアントサブネット CIDR に新しいルートを追加します。
- ピア接続された CIDR の検証 - ODB ネットワークの詳細の `Peered CIDRs` セクションを確認します。VPC から関連するすべての CIDR ブロックが一覧表示されていることを確認します。必要な CIDR がない場合は、ピア接続された CIDR を更新します。
- セキュリティグループルールの確認 - Amazon EC2 コンソールで、VPC 内のリソースのセキュリティグループを見つけます。インバウンドルールとアウトバウンドルールを確認し、必要に応じて更新して必要なトラフィックを許可します。
- アベイラビリティーゾーンの確認 - Amazon VPC コンソールで、サブネットのアベイラビリティーゾーン (AZ) を特定します。ODB ネットワークがサブネットと同じ AZ にもデプロイされていることを確認します。

- 複数の ODB ネットワークピアリング接続の回避 – Oracle Database@AWS コンソールで VPC ピアリング接続を確認します。ODB ネットワークへのアクティブな接続が 1 つだけあることを確認します。1 つ以上の ODB ネットワークピアリングが表示された場合は、追加のネットワークピアリングを削除します。

VPC から解決できない VM クラスターのホスト名またはスキャン名

VM クラスターのホスト名またはスキャン名が VPC から解決できない場合、VPC と次のリソースで DNS 転送を設定して、ODB ネットワークでホストされている DNS レコードを解決します。

- DNS クエリを ODB ネットワークに送信するアウトバウンドエンドポイント。詳細については、「Oracle Database@AWS の ODB ネットワークでのアウトバウンドエンドポイントの設定」を参照してください。
- リゾルバーが ODB ネットワークの DNS に転送する DNS クエリのドメイン名を指定するリゾルバールール。詳細については、「Oracle Database@AWS でのリゾルバールールの設定」を参照してください。

Oracle Database@AWS のサポートを取得する

Oracle Database@AWS の情報とサポートを取得する方法について説明します。

Oracle サポートの範囲と連絡先情報

Oracle Cloud Support は、Oracle Database@AWS の質問すべてに対するサポートの最前線です。サポートに連絡するには、Oracle Cloud Infrastructure (OCI) コンソールにサインインし、"救命いかだ"のアイコンを選択します。My Oracle Cloud Support アカウントをお持ちでない場合、「My Oracle Cloud Support アカウントとアクセス」を参照してください。

Oracle サポートが役立つ問題の例には、以下のものがあります。

- データベース接続の問題 (Oracle TNS)
- Oracle データベースのパフォーマンスの問題
- Oracle Database のエラーの解決
- サービスに関連付けられた OCI テナンシーとの通信に関連するネットワークの問題

- 容量を増やすためのクォータ (制限) の引き上げ (詳細については、「データベースリソースの制限引き上げのリクエスト」を参照してください)
- Oracle Database インフラストラクチャにコンピューティングとストレージ容量を追加するスケーリング
- 新しい世代のハードウェアのアップグレード
- AWS Marketplace 料金に関連する請求の問題

OCI コンソールの外部で Oracle サポートに連絡する必要がある場合、問題が Oracle Database@AWS に関連していることを Oracle サポートエージェントに伝えてください。これは、サービスのリクエストが、これらのデプロイを専門とする OCI サポートチームによって処理されるためです。

電話による Oracle サポートへのお問い合わせ

1. 1-800-223-1711 を呼び出します。米国以外の場合は、Oracle Support Contacts Global Directory にアクセスして、お住まいの国または地域の連絡先情報を確認してください。
2. オプション「2」を選択して、新しいサービスリクエスト (SR) を開きます。
3. 「不明」な場合、オプション「4」を選択します。
4. マルチクラウドシステムに問題があること、および製品の名前をエージェントに知らせます。ユーザーに代わって内部サービスリクエストが開き、OCI サポートエンジニアが直接連絡します。

Oracle の Cloud Customer Connect コミュニティのマルチクラウドフォーラムに質問を送信することもできます。このオプションは、すべてのお客様にご利用いただけます。

My Oracle Cloud Support アカウントとアクセス

My Oracle Cloud Support サービスリクエストチケットを作成するには、組織の Oracle Database@AWS サービスの管理者がリクエストを承認する必要があります。Oracle Database@AWS 管理者の場合、Oracle Database@AWS サービスアクティベーション E メールに記載されている My Oracle Cloud Support のオンボーディング手順を完了します。

My Oracle Cloud Support のオンボーディング手順については、以下のトピックを参照してください。

- Oracle サポートアカウントの設定

- サポートリクエストの作成

My Oracle Cloud Support サポートリクエストを開くユーザーを承認する手順については、「サポートの管理者タスク」を参照してください。

AWS サポート スコープと連絡先情報

AWS サポート は、AWS に関連するすべての問題や質問に対するサポートの最前線です。他の AWS サービスと同様に、問題の AWS サポート ケースを作成します。AWS サポート チームは、必要に応じて OCI サポートと協力します。

AWS サポート が役立つ Oracle Database@AWS の問題の例には、以下のものがあります。

- ネットワークアドレス変換 (NAT)、ファイアウォール、DNS とトラフィック管理、AWS サブネットを含む仮想ネットワークの問題
- データベースのホスト接続、ソフトウェアのインストール、レイテンシー、ホストパフォーマンスなどの踏み台と仮想マシン (VM) の問題
- Amazon CloudWatch 内の Exadata VM クラスターメトリクスレポート
- AWS サービスに関連する請求の問題

AWS サポート に関する詳細については、「AWS サポート の使用開始」を参照してください。

Oracle サービスレベルアグリーメント

Oracle Database@AWS サービスレベルアグリーメント (SLA) について質問がある場合、または SLA 違反に対してサービスクレジットをリクエストする場合、Oracle アカウントマネージャーにお問い合わせください。詳細については、「サービスレベルアグリーメント」を参照してください。

Oracle Database@AWS のクォータ

Oracle Database@AWS はマルチクラウドサービスです。AWS は Oracle Database@AWS リソースのクォータを設定または強制しません。クォータは Oracle Cloud Infrastructure (OCI) によって適用されます。OCI クォータの詳細については、Oracle Cloud Infrastructure ドキュメントの「Quotas and Service Limits」を参照してください。

Oracle Database@AWS ユーザーガイドのドキュメント履歴

Oracle Database@AWS ドキュメントのリリースの説明は、次の表のとおりです。

変更	説明	日付
Oracle Database@AWS がアジアパシフィック (シドニー) リージョンとカナダ (中部) リージョンをサポート	これらのリージョンで Oracle Database@AWS リソースを作成できます。詳細については、「Oracle Database@AWS のサポート対象リージョン」を参照してください。	2026 年 2 月 2 日
Oracle Database@AWS がアジアパシフィック (東京) リージョン、米国東部 (オハイオ) リージョン、欧州 (フランクフルト) リージョンをサポート	これらのリージョンで Oracle Database@AWS リソースを作成できます。詳細については、「Oracle Database@AWS のサポート対象リージョン」を参照してください。	2025 年 12 月 22 日
Oracle Database@AWS が AWS アカウント間での使用権限の共有をサポート	AWS License Manager を使用して、同じ AWS 組織内の AWS アカウント間で Oracle Database@AWS の AWS Marketplace 使用権限を共有できるようになりました。詳細については、「Oracle Database@AWS での使用権限の共有」を参照してください。	2025 年 12 月 19 日
Oracle Database@AWS がゼロ ETL 統合データフィルターの変更をサポート	Oracle Database@AWS は、Amazon Redshift との既存のゼロ ETL 統合のデータフィルターの変更をサポー	2025 年 10 月 15 日

	トしています。データフィルターパターンを更新して、指定されたスキーマとテーブルをデータレプリケーションに含めるか除外できます。詳細については、「ゼロ ETL 統合の管理」を参照してください。	
Oracle Database@AWS がピアリング接続のためのピアネットワーク CIDR 管理をサポート	ODB ピアリング接続を作成または更新するときに、ピアネットワーク CIDR を指定できます。ピア VPC 内のどのサブネットが ODB ネットワークにアクセスできるかを制御します。VPC アカウントは、ODB ネットワークを所有しなくても CIDR 範囲を更新できます。詳細については、「Oracle Database@AWS での Amazon VPC への ODB ピアリングの設定」を参照してください。	2025 年 10 月 10 日
Oracle Database@AWS が Amazon Redshift とのゼロ ETL 統合をサポート	Oracle Database@AWS が VPC Lattice と統合され、Amazon Redshift とのゼロ ETL 統合が可能になりました。詳細については、「Oracle Database@AWS のサービス統合」を参照してください。	2025 年 7 月 2 日

IAM サービスリンクロール許可に対する更新	この AmazonODBServiceRolePolicy ポリシーでは、VPC Transit Gateway アタッチメントを記述し、Amazon EC2 サブネットを記述し、Amazon EventBridge ソースをアクティブ化するための追加のアクセス許可が付与されるようになりました。詳細については、「Oracle Database@AWS での AWS マネージドポリシーの更新」を参照してください。	2025 年 6 月 30 日
IAM サービスリンクロール許可に対する更新	この AmazonODBServiceRolePolicy ポリシーにより、Amazon EventBridge スケジューラのイベントを記述し、イベントバスを作成または記述するための追加のアクセス許可が付与されるようになりました。詳細については、「Oracle Database@AWS での AWS マネージドポリシーの更新」を参照してください。	2025 年 6 月 26 日

Oracle Database@AWS が米国西部 (オレゴン) リージョンをサポート	米国西部 (オレゴン) リージョンで Oracle Database@AWS リソースを作成できます。サポートされている物理 AZ ID は usw2-az3 および usw2-az4 です。詳細については、「Oracle Database@AWS のサポート対象リージョン」を参照してください。	2025 年 6 月 26 日
Oracle Database@AWS が AWS アカウント間でのリソース共有をサポート	AWS Resource Access Manager (AWS RAM) を使用して、Exadata インフラストラクチャと VM クラスターを組織内の他の AWS アカウントと共有できるようになりました。インフラストラクチャを一度プロビジョニングして複数のアカウント間で共有できるため、責任の分離を維持しながらコストを削減できます。詳細については、「Oracle Database@AWS でのリソース共有」を参照してください。	2025 年 6 月 26 日

Oracle Database@AWS が Amazon EventBridge のイベントをサポート	Oracle Database@AWS は Amazon EventBridge にイベントを配信して、リソースのライフサイクルの変更をモニタリングします。イベントは AWS と OCI ソースの両方から生成されるため、ODB ネットワーク、Exadata インフラストラクチャ、VM クラスター、データベースへの変更を追跡できます。詳細については「Amazon EventBridge を使用した Oracle Database@AWS イベントのモニタリング」を参照してください。	2025 年 6 月 26 日
Oracle Database@AWS がクロスリージョンサブスクリプションをサポート	Oracle Database@AWS はクロスリージョンサブスクリプションをサポートしているため、一度サブスクライブすれば使用可能なすべての AWS リージョンでサービスを使用できます。詳細については、「複数のリージョンで Oracle Database@AWS をサブスクライブする」を参照してください。	2025 年 6 月 26 日

Oracle Database@AWS が別のリソースとしての ODB ピアリング接続をサポート	ODB ピアリング接続は、ピアリング接続を作成、表示、削除するための専用 API を備えた別のリソースになりました。ODB ネットワークと Amazon VPC 間のピアリング接続は、同じアカウントまたは異なるアカウントで作成できます。詳細については、「ODB ピアリング接続の操作」を参照してください。	2025 年 6 月 26 日
Oracle Database@AWS が ODB ネットワークを Amazon S3 と統合	Oracle Database@AWS が VPC Lattice と統合され、Amazon S3 への Oracle マネージドバックアップと Amazon S3 への直接 ODB ネットワークアクセスが可能になりました。詳細については、「Oracle Database@AWS のサービス統合」を参照してください。	2025 年 6 月 26 日
Oracle Database@AWS が Autonomous VM クラスターをサポート	Exadata インフラストラクチャ上に Autonomous VM クラスターを作成できるようになりました。Autonomous VM クラスターは、機械学習と AI を使用して主要な管理タスクを自動化するフルマネージド型データベースです。詳細については、「ステップ 3: Oracle Database@AWS で Exadata VM クラスターまたは Autonomous VM クラスターを作成する」を参照してください。	2025 年 5 月 28 日

Oracle Database@AWS がカスタマイズ可能なメンテナンスウィンドウをサポート	Oracle 管理またはカスタマー管理のスケジュールのオプションを使用して、Exadata インフラストラクチャのメンテナンスウィンドウを設定できるようになりました。パッチ適用モード (ローリングまたは非ローリング) を選択し、メンテナンスのタイミングの設定を指定することもできます。詳細については、「Oracle Database@AWS で Oracle Exadata インフラストラクチャを作成する」を参照してください。	2025 年 5 月 1 日
Oracle Database@AWS が新しいアベイラビリティーゾーン (AZ) をサポート	物理 ID `use1-az4` または `use1-az6` を使用して AZ に ODB ネットワークを作成できるようになりました。詳細については、「Oracle Exadata インフラストラクチャ」を参照してください。	2025 年 3 月 26 日

Oracle Database@AWS が Amazon VPC Transit Gateway をサポート	ODB ネットワークにピア接続されている VPC に Transit Gateway を接続する場合は、複数の VPC をこのゲートウェイに接続できます。これらの VPC で実行されているアプリケーションは、ODB ネットワークで実行されている Exadata VM クラスターにアクセスできます。詳細については、「Oracle Database@AWS の Amazon VPC Transit Gateway の設定」を参照してください。	2025 年 3 月 26 日
Oracle Database@AWS が Exadata X11M のデータベースおよびストレージサーバータイプをサポート	Exadata X11M を使用してインフラストラクチャを作成するときに、データベースサーバータイプとストレージサーバータイプを指定できます。詳細については、「Oracle Database@AWS で Oracle Exadata インフラストラクチャを作成する」を参照してください。	2025 年 2 月 4 日
新しいサービスリンクロールポリシー	Oracle Database@AWS は、`AWSServiceRoleForODB` サービスリンクしたロールに対する新しいポリシー `AmazonODBServiceRolePolicy` を追加しました。詳細については、「Oracle Database@AWS での AWS マネージドポリシーの更新」を参照してください。	2024 年 12 月 2 日

初回リリース	Oracle Database@AWS ユーザーガイドの初版リリース	2024 年 12 月 2 日