Oracle Database@AWS 사용자 안내서

Oracle Database@AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Oracle Database@AWS: Oracle Database@AWS 사용자 안내서

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

Oracle Database@AWS이란 무엇인가요? 1
특성 1
관련 서비스 2
액세스 3
가격 책정 3
다음 단계 3
작동 방식 5
OCI 하위 사이트 5
Oracle Exadata 인프라 5
ODB 네트워크 6
가상 프라이빗 클라우드(VPC) 8
ODB 피어링 8
ODB 피어링 연결 생성 9
AWS 서비스 통합 9
여러 VPC에서 트래픽 라우팅 10
AWS Transit Gateway 10
AWS Cloud WAN 11
Exadata VM 클러스터 11
Autonomous VM 클러스터 11
Oracle Exadata 데이터베이스 12
온보딩 13
AWS 계정에 가입 13
관리자 액세스 권한이 있는 사용자 생성 13
비공개 제안 요청 15
여러 리전에서 구독 16
시작하기 17
사전 조건 17
지원되는 OCI 서비스 17
지원되는 리전 18
IP 주소 스페이스 계획 18
ODB 네트워크의 IP 주소에 대한 제한 사항 19
클라이언트 서브넷 CIDR 요구 사항 19
백업 서브넷 CIDR 요구 사항 20
IP 사용 시나리오 20

1단계: ODB 네트워크 생성 22
2단계: Oracle Exadata 인프라 생성 24
3단계: VM 클러스터 생성 26
4단계: Oracle Exadata 데이터베이스 생성 30
ODB 피어링 31
ODB 피어링 설정 31
ODB 피어링 업데이트 33
ODB 피어링을 위한 VPC 라우팅 테이블 구성 34
DNS 구성 34
Oracle Database@AWS에서 DNS 작동 방식 35
아웃바운드 엔드포인트 구성 35
해석기 규칙 구성 36
DNS 구성 테스트 38
Oracle Database@AWS에 대한 Amazon VPC Transit Gateway 구성 38
요구 사항 39
제한 사항 39
전송 게이트웨이 설정 및 구성 40
Oracle Database@AWS에 대한 AWS Cloud WAN 구성 41
권한 공유 43
공유 방법 43
AWS License Manager와의 권한 공유 43
AWS Resource Access Manager(AWS RAM)와 리소스 공유 43
제한 사항 43
계정 간 권한 공유 44
권한을 공유하기 위한 사전 조건 44
권한 공유에 필요한 권한 44
권한 공유 45
리소스 공유 46
AWS RAM 통합 46
이점 46
리소스 공유 작동 방식 47
공유 리소스에 대한 권한 47
제한 사항 48
리소스 공유 제한 사항 48
공유 리소스 생성 및 사용에 대한 제한 사항 49
공유 리소스 삭제에 대한 제한 사항 49

계정 간 리소스 공유 50
리소스 공유를 위한 사전 조건 50
리소스 공유 50
리소스 공유 보 51
리소스 공유 업데이트 또는 삭제 52
서비스 초기화 53
서비스 초기화란 무엇입니까? 53
다음 단계 54
신뢰할 수 있는 계정의 공유 리소스 작업 54
신뢰할 수 있는 계정의 제한 사항 55
VM 클러스터 생성 55
공유 리소스 보기 56
공유 ODB 네트워크를 사용한 ODB 피어링 설정 57
관리 59
ODB 네트워크 업데이트 59
ODB 네트워크 삭제 60
VM 클러스터 삭제 60
Exadata 인프라 삭제 61
ODB 피어링 연결 삭제 61
백업 62
Oracle 관리형 백업 62
사용자 관리형 백업 62
사전 조건 63
Oracle 안전 백업 66
Storage Gateway 67
S3 탑재 지점 69
S3에 대한 액세스 비활성화 71
Amazon S3 통합 문제 해결 72
Redshift와 제로 ETL 통합 73
지원되는 데이터베이스 버전 73
작동 방식 74
사전 조건 74
일반적인 사전 요구 사항 74
데이터베이스 사전 조건 75
고려 사항 79
제한 사항 79

설정 80
1단계: ODB 네트워크에 대한 제로 ETL 활성화 81
2단계: Oracle 데이터베이스 구성 81
3단계: AWS Secrets Manager 및 AWS Key Management Service 설정 82
4단계: IAM 권한 구성 84
5단계: Amazon Redshift 리소스 정책 구성 87
6단계: AWS Glue를 사용하여 제로 ETL 통합 생성 88
7단계: Amazon Redshift에서 대상 데이터베이스 생성 89
제로 ETL 통합 확인 90
데이터 필터링 90
모니터링 91
통합 상태 모니터링 91
성능 모니터링 91
관리 92
제로 ETL 통합 수정 92
제로 ETL 통합 삭제 94
모범 사례 95
문제 해결 96
통합 설정 실패 97
복제 문제 97
데이터 일관성 문제 98
모니터링 및 디버깅 98
보안 99
데이터 보호 100
데이터 암호화 101
전송 중 암호화 101
키 관리 101
Identity and Access Management(IAM) 101
대상 102
ID를 통한 인증 102
정책을 사용하여 액세스 관리 103
Oracle Database@AWS에서 IAM을 사용하는 방식 105
ID 기반 정책 110
AWS 관리형 정책 114
OCI에서 Oracle Database@AWS 인증 및 권한 부여 115
문제 해결 115

규정 준수 확인 117
복원력 117
서비스 연결 역할 118
Oracle Database@AWS에 대한 서비스 연결 역할 권한 118
Oracle Database@AWS 서비스 연결 역할이 지원되는 리전 120
정책 업데이트 120
모니터링 122
CloudWatch를 사용하여 모니터링 122
CloudWatch 지표 123
CloudWatch 차원 134
이벤트 모니터링 136
이벤트 개요 136
AWS의 이벤트 136
OCI의 이벤트 137
이벤트 필터링 138
Oracle Database@AWS 이벤트 문제 해결 139
CloudTrail 로그 139
CloudTrail의 Oracle Database@AWS 관리 이벤트 141
Oracle Database@AWS 이벤트 예제 141
문제 해결 143
ODB 네트워크를 생성할 수 없음 143
VPC와 ODB 네트워크 또는 VM 클러스터 간의 연결 문제 해결 144
VPC에서 VM 클러스터의 확인할 수 없는 호스트 이름 또는 스캔 이름 145
Oracle Database@AWS에 대한 지원 받기 145
Oracle 지원 범위 및 연락처 정보 145
My Oracle Cloud Support 계정 및 액세스 146
AWS Support 범위 및 연락처 정보 146
Oracle 서비스 수준 계약 147
할당량 148
문서 이력 149

Oracle Database@AWS이란 무엇인가요?

Oracle Database@AWS는 AWS 데이터 센터 내에서 Oracle Cloud Infrastructure(OCI)에서 관리하는 Oracle Exadata 인프라에 액세스할 수 있는 서비스입니다. Oracle Exadata 워크로드를 마이그레이션하고, AWS에서 실행되는 애플리케이션과 지연 시간이 짧은 연결을 설정하고, AWS 서비스와 통합할 수 있습니다. AWS Marketplace를 통해 AWS 약정 및 Oracle Support 보상에 포함되는 단일 인보이스를 받습니다.

다음 다이어그램은 Oracle Exadata 인프라를 호스팅하는 AWS 데이터 센터에 연결된 OCI 리전의 개략적인 개요를 보여줍니다. AWS 가용 영역(AZ) 내에서 Amazon VPC를 데이터 센터에 연결된 프라이빗 네트워크에 피어링할 수 있습니다. 이러한 네트워크를 피어링하면 VPC의 애플리케이션 서버가 Oracle Exadata 인프라에서 실행되는 Oracle 데이터베이스에 액세스할 수 있습니다.

Oracle Database@AWS의 기능

Oracle Database@AWS를 사용하면 다음 기능의 이점을 누릴 수 있습니다.

Oracle Exadata 데이터베이스 워크로드를 AWS로 마이그레이션

Oracle Database@AWS를 사용하면 Oracle Exadata 워크로드를 전용 인프라의 Oracle Exadata Database Service 또는 AWS내 전용 Exadata 인프라의 Oracle Autonomous Database로 쉽게 마이그레이션할 수 있습니다. 마이그레이션은 최소한의 변경 사항, 전체 기능 가용성, 아키텍처 호환성 및 온프레미스 Exadata 배포와 동일한 성능을 제공합니다. Recovery Manager(RMAN), Oracle Data Guard, 전송 가능한 테이블스페이스, Oracle Data Pump, Oracle GoldenGate, AWS Database Migration Service, Oracle 제로 가동 중지 시간 마이그레이션과 같은 표준 Oracle 데이터베이스 마이그레이션 도구를 사용할 수 있습니다.

애플리케이션 지연 시간 단축

Oracle Exadata와 AWS에서 실행되는 애플리케이션 간에 지연 시간이 짧은 연결을 설정할 수 있습니다. AWS에서 호스팅되는 애플리케이션에 근접하면 네트워크 지연을 최소화하고 성능을 개선할 수 있습니다.

데이터 통합을 통한 혁신

제로 ETL 통합을 사용하여 Oracle과 AWS 간에 데이터를 통합하고 분석, 기계 학습 및 생성형 AI를 통해 심층적인 인사이트를 생성하고 새로운 혁신을 개발할 수 있습니다. Amazon Redshift를 사용한 제로 ETL 통합을 통해 Oracle Database@AWS에 저장된 트랜잭션 데이터에 대해 거의 실시간에 가까운 분석 및 기계 학습(ML)을 활성화할 수 있습니다.

간소화된 관리 및 운영

협업 지원, 구매, 관리 및 운영을 통해 Oracle과 AWS간의 통합 환경을 활용할 수 있습니다. Oracle Database 서비스를 사용하면 Oracle Support Rewards와 같은 기존 AWS 약정 및 Oracle 라이선스 혜택을 받을 수 있습니다. 익숙한 AWS 도구와 인터페이스를 사용하여 Oracle Database@AWS 리소스를 구매, 프로비저닝 및 관리할 수 있습니다. AWS API, CLI 또는 SDK를 사용하여 리소스를 프로비저닝하고 관리할 수 있습니다. AWS API는 리소스를 프로비저닝하고 관리하는 데 필요한 해당 OCI API를 직접적으로 호출합니다.

AWS 서비스와의 원활한 통합

동일한 환경에서 실행되는 다른 AWS 서비스 및 애플리케이션과 통합할 수 있습니다. 예를 들어, Oracle Database@AWS는 Amazon EC2, Amazon VPC 및 IAM과 통합됩니다. 모니터링을 위한 Amazon CloudWatch 및 이벤트 관리를 위한 Amazon EventBridge와 같은 AWS 서비스와 Oracle Database@AWS를 통합할 수도 있습니다. 데이터베이스 백업의 경우 11 9s의 내구성을 초과하도록 설계된 Amazon S3를 사용할 수 있습니다.

AWS 서비스 관련

Oracle Database@AWS는 다음 서비스를 통해 Oracle 데이터베이스 애플리케이션의 가용성 및 확장성을 개선합니다.

- Amazon EC2 - Oracle 애플리케이션 서버 역할을 하는 가상 서버를 제공합니다. EC2 애플리케이션 서버에 트래픽을 라우팅하도록 로드 밸런서를 구성할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서를 참조하세요.
- Amazon Virtual Private Cloud (VPC) — 정의한 논리적으로 격리된 가상 네트워크에서 AWS 리소스를 시작할 수 있습니다. Oracle Exadata 인프라는 VPC에 피어링할 수 있는 ODB 네트워크라는 특별한 네트워크에 있습니다. 그런 다음 VPC에서 애플리케이션 서버를 실행하고 Exadata 데이터베이스에 액세스할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서를 참조하세요.
- Amazon VPC Lattice - ODB 네트워크에서 Amazon S3 및 Oracle 관리형 백업과 같은 AWS 서비스에 대한 기본 액세스를 제공합니다. 자세한 내용은 Amazon VPC Lattice란 무엇인가?를 참조하세요.
- Amazon CloudWatch - Oracle Database@AWS용 모니터링 서비스를 제공합니다. OCI는 Oracle Exadata 시스템에 대한 지표 데이터를 수집하여 CloudWatch로 전송합니다. 자세한 내용은 Amazon CloudWatch를 사용한 Oracle Database@AWS 모니터링 섹션을 참조하세요.
- AWS Identity and Access Management(IAM) - 사용자를 위해 Oracle Database@AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 해줍니다. IAM을 사용하여 AWS 리소스를 사용할 수 있는

사람을 제어(인증)하고 사용자가 사용할 수 있는 리소스 및 사용 방법을 제어(권한 부여)합니다. 자세한 내용은 Oracle Database@AWS의 Identity and Access Management(IAM) 섹션을 참조하세요.

- AWS 분석 서비스 - Exadata 데이터베이스에서 더 빠르게 인사이트를 얻을 수 있도록 광범위하고 비용 효율적인 분석 서비스 세트를 제공합니다. 각 서비스는 대화형 분석, 빅 데이터 처리, 데이터 웨어하우징, 실시간 분석, 운영 분석, 대시보드 및 시각화와 같은 다양한 분석 사용 사례를 위해 특별히 구축되었습니다. 자세한 내용은 Analytics on AWS를 참조하세요.

Oracle Database@AWS 액세스

AWS Management Console을 사용하여 Oracle Database@AWS를 생성, 액세스 및 관리할 수 있습니다. Oracle Database@AWS에 액세스할 때 사용할 수 있는 웹 인터페이스를 제공합니다.

Oracle Database@AWS 요금

AWS Marketplace에서 Oracle Database@AWS 상품을 구매할 수 있습니다. 먼저 Oracle 영업 담당자에게 문의합니다. 그러면 Oracle에서 비공개 요금 계약에 따라 AWS Marketplace에서 제안을 제공합니다. AWS 청구서에는 사용량에 따른 요금이 표시됩니다.

Oracle 애플리케이션과 Oracle 데이터베이스가 동일한 가용 영역(AZ)에서 호스팅되는 경우 데이터 전송 요금이 부과되지 않습니다. AZ 간 통신에는 표준 데이터 전송 요금이 적용됩니다.

제로 ETL, Oracle 관리형 백업 및 Amazon S3와 같은 Oracle Database@AWS 관리형 통합을 사용하는 경우 VPC Lattice를 통한 리소스 공유 및 액세스에 대한 표준 데이터 처리 요금이 적용됩니다. Oracle Database@AWS 관리형 통합에는 시간당 요금이 부과되지 않습니다. 자세한 내용은 Amazon VPC Lattice 요금을 참조하세요.

다음 단계

이제 Oracle Database@AWS 리소스 생성을 시작할 준비가 되었습니다.

1. Oracle Database@AWS가 어떻게 작동하는지 자세히 알아봅니다. 자세한 내용은 Oracle Database@AWS 작동 방식 섹션을 참조하세요.

> **Note**
>
> AWS 및 Oracle Exadata에 익숙하고 즉시 시작하려면 이 단계를 건너뜁니다.

2. AWS Management Console을 통해 Oracle Database@AWS에 대한 비공개 제안을 요청한 다음 제안을 수락합니다. 자세한 내용은 Oracle Database@AWS에 대한 비공개 제안 요청 섹션을 참조하세요.

   > **Note**
   >
   > 이 미리 보기에서 비공개 제안을 요청하려면 AWS에 문의하여 허용 목록에 AWS 계정를 추가해야 합니다.

3. AWS 콘솔을 사용하여 ODB 네트워크, Oracle Exadata 인프라 및 Exadata VM 클러스터를 생성합니다. OCI 도구를 사용하여 Exadata 데이터베이스를 생성합니다. 자세한 내용은 Oracle Database@AWS 시작하기 섹션을 참조하세요.
4. 계정 간에 리소스를 AWS Resource Access Manager(AWS RAM)와 공유합니다. 자세한 내용은 신뢰할 수 있는 계정의 공유 Oracle Database@AWS 리소스 작업 섹션을 참조하세요.

Oracle Database@AWS 작동 방식

Oracle Database@AWS는 Oracle Cloud Infrastructure(OCI)를 AWS 클라우드와 통합합니다. 다음 섹션에서는 이 멀티 클라우드 아키텍처의 주요 구성 요소에 대해 알아볼 수 있습니다.

전용 인프라의 Oracle Exadata Database Service는 Exadata Database Machine을 제공하는 OCI 서비스입니다. Oracle Exadata Database Machine은 엔터프라이즈 데이터 센터에서 사용할 수 있는 통합되고 사전 구성되며 사전 테스트된 풀 스택 플랫폼입니다. AWS 콘솔, CLI 또는 API를 사용하여 AWS 가용 영역(AZ)에서 Oracle Exadata 인프라 및 VM 클러스터를 생성할 수 있습니다.

AWS에서 리소스를 생성한 후 OCI API를 사용하여 Oracle Exadata 데이터베이스를 생성하고 관리합니다. Amazon VPC에 피어링하는 ODB 네트워크를 사용하면 Amazon EC2 애플리케이션 서버가 Exadata 데이터베이스에 액세스할 수 있습니다. 이러한 방식으로 Oracle Exadata 데이터베이스는 AWS 환경에 통합됩니다.

다음 다이어그램은 Oracle Database@AWS 아키텍처를 보여줍니다.

OCI 하위 사이트

Oracle Cloud Infrastructure는 OCI 리전 및 가용성 도메인에서 호스팅됩니다. OCI 리전은 OCI 리전 내의 격리된 데이터 센터 클러스터인 OCI 가용성 도메인(AD)으로 구성됩니다. OCI 하위 사이트는 OCI 가용성 도메인을 AWS 리전의 가용 영역(AZ)으로 확장하는 데이터 센터입니다. Exadata 인프라는 논리적으로는 OCI 리전에 상주하고 물리적으로는 AWS 리전에 상주합니다.

Oracle Database@AWS용 OCI 하위 사이트는 물리적으로 AWS 데이터 센터에 상주합니다. AWS는 Exadata 인프라를 호스팅하고 OCI는 데이터 센터 내에 Exadata 인프라 하드웨어를 프로비저닝하고 유지 관리합니다. Exadata 인프라, 프라이빗 네트워크 및 VM 클러스터는 AWS 콘솔, CLI 또는 API를 사용하여 구성할 수 있습니다. Amazon EC2 및 Amazon VPC와 같은 AWS 서비스를 사용하여 인프라에서 실행되는 Oracle Exadata 데이터베이스에 대한 애플리케이션 액세스를 허용할 수 있습니다.

Oracle Exadata 인프라

Oracle Exadata 인프라는 Oracle Exadata 데이터베이스를 실행하는 데이터베이스 서버 및 스토리지 서버의 기본 아키텍처입니다. 인프라는 AWS 가용 영역(AZ)에 있습니다. Exadata 인프라에서 VM 클러스터를 생성하려면 AWS 콘솔, CLI 또는 API를 사용합니다.

Oracle Exadata 인프라는 데이터베이스 서버라는 물리적 머신에 배포됩니다. 이러한 서버는 Amazon EC2 전용 서버와 유사한 컴퓨팅 리소스를 제공합니다. 각 데이터베이스 서버는 하이퍼바이저에서 실행되는 하나 이상의 가상 머신(VM)을 호스팅합니다. 이러한 관계를 보여주는 아키텍처 다이어그램은 Exadata Database Service on Dedicated Infrastructure Technical Architecture를 참조하세요.

Oracle Database@AWS에서 Exadata 인프라를 생성할 때 다음과 같은 정보를 지정합니다.

- 총 데이터베이스 서버 수
- 총 스토리지 서버 수
- Exadata 시스템 모델(X11M)
- 인프라를 호스팅하는 AZ(Oracle Database@AWS용 리전 지원 참조)

Oracle Exadata 인프라를 생성하는 방법을 알아보려면 2단계: Oracle Database@AWS에서 Oracle Exadata 인프라 생성 섹션을 참조하세요.

ODB 네트워크

ODB 네트워크는 AWS 가용 영역(AZ)에서 OCI 인프라를 호스팅하는 프라이빗 격리 네트워크입니다. ODB 네트워크는 IP 주소의 CIDR 범위로 구성됩니다. ODB 네트워크는 OCI 하위 사이트 내에 있는 네트워크에 직접 매핑되므로 AWS와 OCI 간의 통신 수단으로 사용됩니다. Exadata VM 클러스터를 생성할 때 ODB 네트워크를 지정해야 합니다(3단계: Oracle Database@AWS에서 Exadata VM 클러스터 또는 Autonomous VM 클러스터 생성 참조).

Oracle Database@AWS API를 사용하여 ODB 네트워크에서 리소스를 프로비저닝합니다. ODB 네트워크는 AWS에서 관리하지만 Amazon VPC를 ODB 네트워크에 연결하도록 ODB 피어링 연결을 설정할 수 있습니다. 자세한 내용은 ODB 피어링 섹션을 참조하세요.

ODB 네트워크를 생성할 때 다음 정보를 지정합니다.

- 가용 영역 - ODB 네트워크는 AZ에 고유합니다.

  다음 AWS 리전에서 Oracle Database@AWS를 사용할 수 있습니다.

  미국 동부(버지니아 북부)

  물리적 ID `use1-az4` 및 `use1-az6`와 함께 AZ를 사용할 수 있습니다.

미국 서부(오리건)

물리적 ID usw2-az3 및 usw2-az4와 함께 AZ를 사용할 수 있습니다.

아시아 태평양(도쿄)

물리적 ID apne1-az1 및 apne1-az4와 함께 AZ를 사용할 수 있습니다.

미국 동부(오하이오)

물리적 ID use2-az1 및 use2-az2와 함께 AZ를 사용할 수 있습니다.

유럽(프랑크푸르트)

물리적 ID euc1-az1 및 euc1-az2와 함께 AZ를 사용할 수 있습니다.

캐나다(중부)

물리적 ID cac1-az4와 함께 AZ를 사용할 수 있습니다.

아시아 태평양(시드니)

물리적 ID apse2-az4와 함께 AZ를 사용할 수 있습니다.

계정에서 이전 물리적 AZ ID에 매핑되는 논리적 AZ 이름을 찾으려면 다음 명령을 실행합니다.

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

- 클라이언트 CIDR 주소 - ODB 네트워크에는 Exadata VM 클러스터 및 Autonomous VM 클러스터용 클라이언트 서브넷 CIDR이 필요합니다.
- 백업 CIDR 주소 - ODB 네트워크에는 VM 클러스터의 관리형 데이터베이스 백업을 위한 백업 서브넷 CIDR이 필요합니다. Exadata VM 클러스터의 경우 백업 서브넷은 선택 사항입니다.
- AWS 서비스 통합 - Amazon Redshift를 사용한 Amazon S3 및 제로 ETL과 같은 AWS 서비스 통합을 위한 네트워크 경로를 구성할 수 있습니다. 자세한 내용은 AWS 서비스 통합 섹션을 참조하세요.

자세한 내용은 1단계: Oracle Database@AWS에서 ODB 네트워크 생성 섹션을 참조하세요.

가상 프라이빗 클라우드(VPC)

가상 프라이빗 클라우드(VPC)는 AWS 클라우드에서 생성하는 가상 네트워크입니다. AWS 클라우드의 다른 가상 네트워크와 논리적으로 격리되어 있으므로 자체 IP 주소 범위 선택, 서브넷 생성, 라우팅 테이블 및 네트워크 게이트웨이 구성 등 가상 네트워킹 환경을 완벽하게 제어할 수 있습니다. 자세한 내용은 Amazon VPC란 무엇인가?를 참조하세요

Amazon EC2 인스턴스를 VPC에서 시작할 수 있습니다. EC2 인스턴스는 Oracle Exadata 데이터베이스와 통신하는 애플리케이션 서버를 호스팅할 수 있습니다. VPC의 다른 EC2 인스턴스와 마찬가지로 애플리케이션 서버를 관리하고 시작할 수 있습니다. 자세한 내용은 Amazon EC2란 무엇입니까?를 참조하세요.

기본적으로 ODB 네트워크는 VPC와 연결되어 있지 않습니다. ODB 네트워크를 기존 AWS 인프라에 연결하려면 ODB 네트워크와 하나의 VPC 간에 피어링 연결을 생성합니다. ODB 네트워크를 생성할 때 VPC를 지정할 수 있습니다. 자세한 내용은 1단계: Oracle Database@AWS에서 ODB 네트워크 생성 섹션을 참조하세요.

ODB 피어링

ODB 피어링은 Amazon VPC와 ODB 네트워크 간에 트래픽을 비공개로 라우팅할 수 있는 사용자 생성 네트워크 연결입니다. VPC와 ODB 네트워크 간에는 1:1 관계가 있습니다. 피어링 후 VPC 내의 Amazon EC2 인스턴스는 동일한 네트워크 내에 있는 것처럼 ODB 네트워크의 Oracle Exadata 데이터베이스와 통신할 수 있습니다.

> **Note**
>
> ODB 피어링은 두 VPC 간에 트래픽을 라우팅하는 두 VPC 간의 피어링 연결인 VPC 피어링과 다릅니다.

AWS RAM을 사용하여 한 계정의 ODB 네트워크와 다른 계정의 VPC를 피어링할 수 있습니다. ODB 네트워크를 다른 계정과 공유하는 경우 신뢰할 수 있는 계정이 피어링을 직접 시작할 수 있습니다. ODB 피어링 연결을 시작하는 계정은 연결을 소유하고 관리합니다.

ODB 피어링 연결을 생성하거나 업데이트할 때 피어 네트워크 CIDR을 지정할 수 있습니다. 이렇게 하면 피어 VPC에서 ODB 네트워크에 액세스할 수 있는 서브넷을 제어할 수 있습니다. VPC 계정

은 ODB 네트워크를 소유하지 않고도 CIDR 범위를 업데이트할 수 있습니다. 자세한 내용은 Oracle Database@AWS의 Amazon VPC에 대한 ODB 피어링 구성을 참조하세요.

VPC 내의 리소스는 여러 가용 영역(AZ)에 걸쳐 있을 수 있습니다. ODB 네트워크에서 리소스는 단일 AZ에 바인딩됩니다. ODB 네트워크를 생성할 때 이 AZ를 정의합니다.

ODB 피어링 연결 생성

ODB 피어링 연결은 ODB 네트워크의 특성이 아니라 자체 ID(접두사 `odbpcx-`) 및 수명 주기를 가진 독립 리소스입니다. 전용 API 세트를 사용하여 피어링 연결을 관리합니다. 예를 들어 Oracle Database@AWS 콘솔 또는 `CreateOdbPeeringConnection` API를 사용하여 기존 ODB 네트워크에 대한 ODB 피어링 연결을 생성합니다. 자세한 내용은 Oracle Database@AWS에서 ODB 피어링 연결 생성 섹션을 참조하세요.

ODB 피어링 연결을 생성하면 Oracle Database@AWS가 다음 작업을 자동으로 수행합니다.

1. Oracle VCN CIDR과 겹치는 CIDR 블록을 확인하는 등 네트워크 구성을 검증합니다.
2. 기본 네트워크 피어링 인프라를 설정합니다.
3. VPC CIDR 주소를 사용하여 ODB 네트워크(VPC 아님) 라우팅 테이블을 구성합니다.

ODB 피어링 연결을 생성한 후 Amazon EC2 `create-route` 명령을 사용하여 VPC 라우팅 테이블을 수동으로 업데이트합니다. 자세한 내용은 ODB 피어링을 위한 VPC 라우팅 테이블 구성 섹션을 참조하세요.

AWS 서비스 통합

Oracle 데이터베이스에 향상된 기능과 연결 옵션을 제공하기 위해 Oracle Database@AWS는 Amazon VPC Lattice를 사용하여 AWS 서비스와 통합됩니다. 추가 VPC나 복잡한 네트워킹 설정 없이 ODB 네트워크에서 직접 AWS 서비스에 대한 네트워크 경로를 구성할 수 있습니다.

Oracle Database@AWS는 다음과 같은 AWS 관리형 서비스 통합을 지원합니다.

Amazon S3

다음과 같은 방법으로 Amazon S3를 Oracle Database@AWS와 통합할 수 있습니다.

- Amazon S3에 대한 Oracle 관리형 자동 백업 - Oracle Database@AWS는 자동 백업을 위한 네트워크 액세스를 자동으로 활성화합니다. 이 통합은 비활성화할 수 없습니다. OCI 콘솔에서 Amazon S3를 관리형 백업 대상으로 설정하면 OCI는 자동 백업을 S3 버킷에 업로드합니다.

- ODB 네트워크에서 Amazon S3에 직접 액세스 - S3에 대한 직접 ODB 네트워크 액세스를 활성화한 다음 스크립트, 가져오기 및 내보내기 파일, 관련 파일을 S3 버킷에 저장할 수 있습니다. 이 액세스를 비활성화할 수 있습니다. 이 설정은 Oracle 관리형 자동 백업에 대한 자동 네트워크 액세스와는 별개입니다.

Amazon Redshift 제로 ETL 통합

ODB 네트워크와 Amazon Redshift의 제로 ETL 통합을 활성화할 수 있습니다. 이 통합을 통해 기존 추출, 전환, 적재(ETL) 프로세스 없이 Oracle Database@AWS에서 실행되는 Oracle 데이터베이스에서 Amazon Redshift로 데이터를 복제할 수 있습니다. 이 통합은 Oracle 데이터를 Amazon Redshift와 자동으로 동기화하여 실시간 분석 및 AI 워크로드를 지원합니다.

AWS 서비스에 대한 관리형 통합 외에도 VPC Lattice를 사용하여 다른 VPC에서 호스팅되는 서비스 및 리소스에 액세스하거나 VPC에서 ODB 네트워크 인스턴스에 액세스할 수도 있습니다. VPC Lattice 콘솔, CLI 및 API를 사용하여 액세스 및 리소스를 관리할 수 있습니다. 자세한 정보는 다음 자료를 참조하세요.

- Oracle Database@AWS에 백업
- Amazon Redshift와 Oracle Database@AWS 제로 ETL 통합
- Amazon VPC Lattice란 무엇입니까? 및 Oracle Database@AWS용 VPC Lattice

여러 VPC에서 트래픽 라우팅

여러 VPC가 하나의 ODB 네트워크의 Oracle Database@AWS 리소스에 액세스하도록 허용하려면 AWS Transit Gateway 또는 AWS Cloud WAN을 사용할 수 있습니다.

AWS Transit Gateway

Amazon VPC Transit Gateway는 VPC와 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 네트워크 전송 허브입니다. ODB 네트워크는 ODB 네트워크와 단일 VPC 간의 일대일 직접 피어링만 지원합니다. ODB 네트워크를 VPC에 피어링한 다음 이 VPC를 전송 게이트웨이에 연결할 수 있습니다. 게이트웨이는 여러 VPC에 연결할 수 있습니다. 이 전송 게이트웨이 구성을 사용하면 여러 VPC 서브넷 간의 트래픽을 단일 ODB 네트워크로 라우팅할 수 있습니다.

자세한 내용은 Oracle Database@AWS에 대한 Amazon VPC Transit Gateway 구성 섹션을 참조하세요.

AWS Cloud WAN

AWS Cloud WAN은 클라우드 및 온프레미스 환경에서 리소스를 연결하는 통합 글로벌 네트워크를 구축, 관리 및 모니터링할 수 있는 관리형 광역 네트워크(WAN) 서비스입니다. 중앙 대시보드를 사용하면 AWS 글로벌 네트워크에서 온프레미스 지사, 데이터 센터 및 VPC를 연결할 수 있습니다.

ODB 네트워크를 VPC에 피어링한 다음 이 VPC를 Cloud WAN 코어 네트워크에 연결할 수 있습니다. 이 구성을 사용하면 Cloud WAN을 사용하여 여러 VPC 또는 온프레미스 네트워크와 ODB 네트워크 간에 트래픽을 라우팅할 수 있습니다. 자세한 내용은 Oracle Database@AWS에 대한 AWS Cloud WAN 구성 섹션을 참조하세요.

Exadata VM 클러스터

Exadata VM 클러스터는 긴밀하게 결합된 Exadata VM 세트입니다. 각 VM에는 Oracle Real Application Clusters(Oracle RAC) 및 Oracle Grid Infrastructure를 포함하여 Oracle Enterprise Edition의 모든 기능을 포함하는 전체 Oracle 데이터베이스 설치가 있습니다. VM 클러스터에서 Oracle Exadata 데이터베이스를 하나 이상 생성할 수 있습니다. VM 및 VM 클러스터의 아키텍처를 보여주는 다이어그램은 Exadata Database Service on Dedicated Infrastructure Technical Architecture를 참조하세요.

VM 클러스터를 생성할 때 다음을 포함하는 정보를 지정합니다.

- ODB 네트워크
- Oracle Exadata 인프라
- 클러스터에 VM을 배치할 데이터베이스 서버
- 사용 가능한 Exadata 스토리지의 총량

VM 클러스터의 각 VM에 대해 CPU 코어, 메모리 및 로컬 스토리지를 구성할 수 있습니다. 자세한 내용은 3단계: Oracle Database@AWS에서 Exadata VM 클러스터 또는 Autonomous VM 클러스터 생성 섹션을 참조하세요.

Autonomous VM 클러스터

Autonomous VM 클러스터는 기계 학습 및 AI를 사용하여 키 관리 작업을 자동화하는 완전 관리형 데이터베이스입니다. 기존 데이터베이스와 달리 Autonomous 데이터베이스는 사람의 개입 없이 데이터베이스를 자동으로 프로비저닝, 보안, 업데이트, 백업 및 조정합니다.

VM당 ECPU 코어 수, CPU당 데이터베이스 메모리, 데이터베이스 스토리지 및 최대 Autonomous 컨테이너 데이터베이스 수를 구성할 수 있습니다. 자세한 내용은 3단계: Oracle Database@AWS에서 Exadata VM 클러스터 또는 Autonomous VM 클러스터 생성 섹션을 참조하세요.

Oracle Exadata 데이터베이스

Oracle Exadata는 Oracle 데이터베이스를 실행하기 위한 고성능 플랫폼을 제공하는 엔지니어링 시스템입니다. Oracle Database@AWS에서는 AWS 콘솔을 사용하여 Exadata 데이터베이스를 호스팅하는 Oracle Exadata 인프라 및 VM 클러스터를 생성합니다. 그런 다음 OCI API를 사용하여 Oracle 데이터베이스를 생성하고 관리합니다. 자세한 내용은 4단계: Oracle Cloud Infrastructure에서 Oracle Exadata 데이터베이스 생성 섹션을 참조하세요.

Oracle Database@AWS에 온보딩

Oracle Database@AWS 사용을 시작하기 전에 AWS에 가입하고 필요한 사용자를 생성해야 합니다. 그런 다음 Oracle의 비공개 제안을 수락하여 AWS Marketplace에서 Oracle Database@AWS를 구매할 수 있습니다.

AWS 계정에 가입

AWS 계정이 없는 경우 다음 절차에 따라 계정을 생성합니다.

AWS 계정에 가입하려면

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중 전화 또는 텍스트 메시지를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   AWS 계정 루트 사용자에 가입하면 AWS 계정루트 사용자가 만들어집니다. 루트 사용자에게는 계정의 모든 AWS 서비스및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

가입 프로세스가 완료되면 AWS은 사용자에게 확인 이메일을 전송합니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 확인하고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

AWS 계정에 가입하고 AWS 계정 루트 사용자에 보안 조치를 한 다음, AWS IAM Identity Center을 활성화하고 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 생성합니다.

귀하의 AWS 계정 루트 사용자보호

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 AWS Management Console에 계정 소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인사용 설명서의 루트 사용자로 로그인을 참조하세요.

2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정루트 사용자용 가상 MFA 디바이스 활성화(콘솔)를 참조하세요.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center사용 설명서의 AWS IAM Identity Center설정을 참조하세요.

2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   IAM Identity Center 디렉터리를 ID 소스로 사용하는 방법에 대한 자습서는 AWS IAM Identity Center사용 설명서의 기본 IAM Identity Center 디렉터리로 사용자 액세스 구성을 참조하세요.

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자로 로그인하는 데 도움이 필요한 경우 AWS 로그인 사용 설명서의 AWS액세스 포털에 로그인을 참조하세요.

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.

2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 그룹 추가를 참조하세요.

Oracle Database@AWS에 대한 비공개 제안 요청

AWS Marketplace 판매자 비공개 제안 기능을 사용하면 Oracle Database@AWS 요금 및 EULA 조건을 Oracle에 요청하고 받을 수 있습니다. Oracle과 요금 및 조건을 협상하면, Oracle은 사용자가 지정하는 AWS 계정 계정에 비공개 제안을 생성합니다. 비공개 제안을 수락하고 협상된 요금 및 이용 약관을 받습니다. 현재 Oracle Database@AWS 대시보드를 사용할 수 있습니다. 비공개 제안 계약이 만료 날짜에 도달하면 자동으로 제품의 공개 요금으로 전환되거나 Oracle Database@AWS 구독이 취소됩니다. 비공개 제안에 대한 자세한 내용은 AWS Marketplace의 비공개 제안 섹션을 참조하세요.

Oracle Database@AWS에 대한 비공개 제안을 요청하고 수락하려면

1. 에 로그인합니다AWS Management Console
2. 검색한 다음 Oracle Database@AWS를 선택합니다.
3. 비공개 제안 요청을 선택합니다.

> **Note**
>
> 비공개 제안을 수락해야 Oracle Database@AWS 대시보드를 사용할 수 있습니다.

4. Oracle Cloud Infrastructure(OCI) 사이트에서 리전 및 연락처 정보와 같은 세부 정보를 지정합니다.
5. OCI 담당자가 연락하여 비공개 제안을 제공할 때까지 기다립니다.
6. AWS Management Console에서 비공개 제안 보기를 선택합니다.
7. 제안을 선택한 다음 제안 보기를 선택합니다.
8. 계약 생성을 선택하고 후속 프롬프트에 응답하여 비공개 제안을 수락합니다.
9. 비공개 제안을 수락한 후에는 OCI 계정을 활성화해야 합니다. AWS Management Console에서 직접 Oracle 활성화 링크에 액세스할 수 있습니다.

    1. 콘솔에서 시작하기 섹션으로 이동합니다.
    2. 콘솔에 제공된 Oracle 활성화 링크를 클릭합니다. 또는 이메일을 통해 전송된 활성화 링크를 사용할 수도 있습니다.
    3. Oracle 활성화 페이지에서 새 Oracle 클라우드 계정을 생성할지 아니면 기존 계정에 추가할지 선택합니다.
    4. 화면의 지침에 따라 활성화 프로세스를 완료합니다.
    5. 활성화 요청을 제출하면 AWS Management Console에 활성화 진행 중 상태가 표시되고 사유가 표시된 상태로 대시보드가 일시적으로 비활성화됩니다.

6. 활성화가 완료되면 Oracle Database@AWS 대시보드를 사용할 수 있으므로 리소스를 관리할 수 있습니다.

10. AWS Management Console에서 대시보드를 선택합니다.

여러 리전에서 Oracle Database@AWS 구독

AWS Marketplace를 통해 Oracle Database@AWS를 구독하고 온보딩을 완료하면 AWS 계정이 OCI 테넌시에 연결됩니다. 이 링크는 관련 리소스와 함께 Oracle Database@AWS를 사용할 수 있는 모든 AWS 리전에 자동으로 복제됩니다. 각 리전에 대해 프로세스를 반복하지 않고 한 번 구독하고 온보딩합니다.

여러 리전에서 Oracle Database@AWS를 사용하려면 다음 단계를 수행합니다.

1. AWS Marketplace를 통해 Oracle Database@AWS를 구독하고 온보딩 프로세스를 완료합니다.

   Oracle Database@AWS를 처음 구독하면 홈 리전에서 계정이 활성화됩니다. Oracle Cloud Infrastructure(OCI)에서 홈 리전을 지정합니다.
2. OCI 콘솔을 통해 원하는 리전을 활성화합니다.

   OCI에서 리전을 활성화하지 않은 다음 Oracle Database@AWS 콘솔에서 이 리전으로 전환하면 구독하지 않았다는 오류가 표시됩니다. 이 경우 OCI에서 이 리전을 활성화해야 이 리전에서 Oracle Database@AWS 대시보드를 사용할 수 있습니다.
3. 구독 프로세스를 반복하지 않고 지원되는 모든 AWS 리전에서 Oracle Database@AWS에 액세스합니다.

Oracle Database@AWS 시작하기

Oracle Database@AWS 사용을 시작하기 위해 Oracle Database@AWS 콘솔, CLI 또는 API를 사용하여 다음 리소스를 생성할 수 있습니다.

1. ODB 네트워크
2. Oracle Exadata 인프라
3. Exadata VM 클러스터 또는 Autonomous VM 클러스터
4. ODB 피어링 연결

인프라에서 Oracle Exadata 데이터베이스를 생성하려면 Oracle Database@AWS 대시보드 대신 Oracle Cloud Infrastructure(OCI) 콘솔 또는 API를 사용해야 합니다. 따라서 다음 두 클라우드 환경에 리소스를 배포합니다. 네트워크 및 인프라 리소스는 AWS에 있고 데이터베이스 관리 컨트롤 플레인은 OCI에 있습니다. 자세한 내용은 Oracle Cloud Infrastructure 설명서의 Oracle Database@AWS를 참조하세요.

Oracle Database@AWS 설정을 위한 사전 조건

Oracle Exadata 인프라를 구성하기 전에 다음을 수행해야 합니다.

- Oracle Database@AWS에 온보딩 단원의 단계를 따르십시오. Oracle Database@AWS를 사용하려면 비공개 제안을 수락해야 합니다.
- IAM 위탁자에게 사용자가 Oracle Database@AWS 리소스를 프로비저닝하도록 허용에 나열된 정책 권한을 부여합니다. 이러한 권한은 Oracle Database@AWS를 사용하는 데 필요합니다.

Oracle Database@AWS에서 지원되는 OCI 서비스

Oracle Database@AWS는 다음 Oracle Cloud Infrastructure(OCI) 서비스를 지원합니다.

- 전용 인프라의 Oracle Exadata Database Service - AWS내에서 액세스할 수 있는 완전 관리형 전용 Exadata 환경을 제공합니다. 자세한 내용은 OCI 설명서의 전용 인프라의 Oracle Cloud Exadata Database Service를 참조하세요.
- 전용 Exadata 인프라의 Autonomous 데이터베이스 - OCI에서 실행되는 고도로 자동화된 완전 관리형 데이터베이스 환경을 커밋된 하드웨어 및 소프트웨어 리소스와 함께 제공합니다. 자세한 내용은 OCI 설명서의 전용 Exadata 인프라의 Autonomous 데이터베이스 정보를 참조하세요.

Oracle Database@AWS용 리전 지원

다음 AWS 리전에서 Oracle Database@AWS를 사용할 수 있습니다.

미국 동부(버지니아 북부)

물리적 ID use1-az4 및 use1-az6와 함께 AZ를 사용할 수 있습니다.

미국 서부(오리건)

물리적 ID usw2-az3 및 usw2-az4와 함께 AZ를 사용할 수 있습니다.

아시아 태평양(도쿄)

물리적 ID apne1-az1 및 apne1-az4와 함께 AZ를 사용할 수 있습니다.

미국 동부(오하이오)

물리적 ID use2-az1 및 use2-az2와 함께 AZ를 사용할 수 있습니다.

유럽(프랑크푸르트)

물리적 ID euc1-az1 및 euc1-az2와 함께 AZ를 사용할 수 있습니다.

캐나다(중부)

물리적 ID cac1-az4와 함께 AZ를 사용할 수 있습니다.

아시아 태평양(시드니)

물리적 ID apse2-az4와 함께 AZ를 사용할 수 있습니다.

계정에서 이전 물리적 AZ ID에 매핑되는 논리적 AZ 이름을 찾으려면 다음 명령을 실행합니다.

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

Oracle Database@AWS에서 IP 주소 스페이스 계획

Oracle Database@AWS에서 IP 주소 스페이스를 신중하게 계획합니다. ODB 네트워크에 프로비저닝할 수 있는 클러스터당 VM 수를 포함하여 VM 클러스터 수를 기준으로 IP 주소 사용을 고려합니다. 자세한 내용은 Oracle Cloud Infrastructure 설명서의 ODB 네트워크 설계를 참조하세요.

주제

- ODB 네트워크의 IP 주소에 대한 제한 사항
- ODB 네트워크에 대한 클라이언트 서브넷 CIDR 요구 사항
- ODB 네트워크에 대한 백업 서브넷 CIDR 요구 사항
- ODB 네트워크의 IP 사용 시나리오

ODB 네트워크의 IP 주소에 대한 제한 사항

ODB 네트워크의 CIDR 범위에 대한 다음 제한 사항에 유의하세요.

- ODB 네트워크를 생성한 후에는 ODB 네트워크의 클라이언트 또는 백업 서브넷 CIDR 범위를 수정할 수 없습니다.
- IPv4 CIDR 블록 연결 제한의 테이블에 있는 제한된 연결 열에는 VPC CIDR 범위를 사용할 수 없습니다.
- Exadata X9M의 경우 IP 주소 100.106.0.0/16 및 100.107.0.0/16은 OCI 자동화를 통한 클러스터 상호 연결용으로 예약되어 있으므로 다음을 수행할 수 없습니다.
  - ODB 네트워크의 클라이언트 또는 백업 CIDR 범위에 이러한 범위를 할당합니다.
  - ODB 네트워크에 연결하는 데 사용되는 VPC CIDR에 이 범위를 사용합니다.
- 다음 CIDR 범위는 Oracle Cloud Infrastructure용으로 예약되어 있으며 ODB 네트워크에 사용할 수 없습니다.
  - Oracle Cloud 예약 범위 CIDR 169.254.0.0/16
  - 예약 클래스 D 224.0.0.0 — 239.255.255.255
  - 예약 클래스 E 240.0.0.0 — 255.255.255.255
- 클라이언트 및 백업 서브넷의 IP 주소 CIDR 범위는 겹칠 수 없습니다.
- 클라이언트 및 백업 서브넷에 할당된 IP 주소 CIDR 범위를 ODB 네트워크에 연결하는 데 사용되는 VPC CIDR 범위와 겹칠 수 없습니다.
- VM 클러스터의 VM을 다른 ODB 네트워크로 프로비저닝할 수 없습니다. 네트워크는 VM 클러스터의 속성이므로 VM 클러스터의 VM만 동일한 ODB 네트워크에 프로비저닝할 수 있습니다.

ODB 네트워크에 대한 클라이언트 서브넷 CIDR 요구 사항

다음 표에서는 클라이언트 서브넷 CIDR의 서비스 및 인프라에서 사용하는 IP 주소 수를 확인할 수 있습니다. 클라이언트 서브넷의 최소 CIDR 크기는 /27이고 최대 크기는 /16입니다.

IP 주소 수	사용 주체	참고
6	Oracle Database@AWS	이러한 IP 주소는 ODB 네트워크에서 프로비저닝하는 VM 클러스터 수에 관계없이 예약됩니다. Oracle Database@AWS는 다음을 사용합니다. • AWS의 ODB 네트워크 리소스용으로 예약된 IP 주소 3개 • OCI 네트워킹 서비스용으로 예약된 IP 주소 3개
3	각 VM 클러스터	이러한 IP 주소는 각 VM 클러스터에 있는 VM 수에 관계없이 단일 클라이언트 액세스 이름(SCAN)용으로 예약됩니다.
4	각 VM	이러한 IP 주소는 인프라의 VM 수에만 의존합니다.

ODB 네트워크에 대한 백업 서브넷 CIDR 요구 사항

다음 표에서는 클라이언트 서브넷 CIDR의 서비스 및 인프라에서 사용하는 IP 주소 수를 확인할 수 있습니다. 백업 서브넷의 최소 CIDR 크기는 /28이고 최대 크기는 /16입니다.

IP 주소 수	사용 주체	참고
3	Oracle Database@AWS	이러한 IP 주소는 ODB 네트워크에서 프로비저닝하는 VM 클러스터 수에 관계없이 예약됩니다. Oracle Database@AWS는 다음을 사용합니다. • CIDR 범위 시작 부분에 IP 주소 2개 • CIDR 범위 끝에 IP 주소 1개
3	각 VM	이러한 IP 주소는 인프라의 VM 수에만 의존합니다.

ODB 네트워크의 IP 사용 시나리오

다음 표에서는 VM 클러스터의 다양한 구성에 대해 ODB 네트워크에서 사용되는 IP 주소를 볼 수 있습니다. /28은 클라이언트 서브넷 CIDR이 2개의 VM이 있는 VM 클러스터 1개를 배포하기 위한 기술적 최소 CIDR 범위인 반면, 최소 /27 CIDR 범위를 사용하는 것이 좋습니다. 이 경우 IP 범위는 VM 클러스터에서 완전히 사용되지 않으며 추가 IP 주소 할당을 허용합니다.

구성	사용된 클라이언트 IP	최소 클라이언트 IP	사용된 백업 IP	최소 백업 IP
VM 클러스터 1개와 VM 2개	17(서비스 6개 + 클러스터 3개 + 4*2)	32(/27 CIDR 범위)	9(서비스 3개 + 3*2)	16(/28 CIDR 범위)
VM 클러스터 1개와 VM 3개	21(서비스 6개 + 클러스터 3개 + 4*3)	32(/27 CIDR 범위)	12(서비스 3개 + 3*3)	16(/28 CIDR 범위)
VM 클러스터 1개와 VM 4개	25(서비스 6개 + 클러스터 3개 + 4*4)	32(/27 CIDR 범위)	15(서비스 3개 + 3*4)	16(/28 CIDR 범위)
VM 클러스터 1개와 VM 8개	41(서비스 6개 + 클러스터 3개 + 4*8)	64(/26 CIDR 범위)	27(서비스 3개 + 3*8)	32(/27 CIDR 범위)

다음 표는 특정 클라이언트 CIDR 범위를 고려할 때 각 구성의 인스턴스 수를 보여줍니다. 예를 들어 VM이 4개인 VM 클러스터 1개는 클라이언트 서브넷에서 24개의 IP 주소를 사용합니다. CIDR 범위가 /25인 경우 128개의 IP 주소를 사용할 수 있습니다. 따라서 서브넷에 VM 클러스터 5개를 프로비저닝할 수 있습니다.

VM 클러스터 구성	/27 포함 숫자(32 IP)	/26 포함 숫자(64 IP)	/25 포함 숫자(128 IP)	/24 포함 숫자(256 IP)	/23일 때의 숫자(512 IP)	/22일 때의 숫자(1024 IP)
VM 클러스터 1개와 VM 2개(16 IP)	1	3	7	15	30	60
VM 클러스터 1개와 VM 3개(20 IP)	1	3	6	12	24	48
VM 클러스터 1개와 VM 4개(24 IP)	1	2	5	10	20	40
각각 VM이 2개인 VM 클러스터 2개(27 IP)	1	2	4	9	18	36

VM 클러스터 구성	/27 포함 숫자(32 IP)	/26 포함 숫자(64 IP)	/25 포함 숫자(128 IP)	/24 포함 숫자(256 IP)	/23일 때의 숫자 (512 IP)	/22일 때의 숫자 (1024 IP)
각각 VM이 3개인 VM 클러스터 2개(35 IP)	0	1	3	7	14	28
각각 VM이 4개인 VM 클러스터 2개(43 IP)	0	1	2	5	11	23

1단계: Oracle Database@AWS에서 ODB 네트워크 생성

ODB 네트워크는 가용 영역(AZ)에서 OCI 인프라를 호스팅하는 프라이빗 격리 네트워크입니다. ODB 네트워크와 Oracle Exadata 인프라는 VM 클러스터를 프로비저닝하고 Exadata 데이터베이스를 생성하기 위한 사전 조건입니다. ODB 네트워크와 Oracle Exadata 인프라를 어느 순서로든 생성할 수 있습니다. 자세한 내용은 ODB 네트워크 및 ODB 피어링(을)를 참조하세요.

이 작업에서는 사용자가 Oracle Database@AWS에서 IP 주소 스페이스 계획 섹션을 읽었다고 가정합니다. 나중에 ODB 네트워크를 수정하거나 삭제하려면 Oracle Database@AWS 관리 섹션을 참조하세요.

ODB 네트워크를 생성하려면

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 오른쪽 상단에서 AWS 리전을 선택합니다. 자세한 내용은 Oracle Database@AWS용 리전 지원 섹션을 참조하세요.
3. 왼쪽 창에서 ODB 네트워크를 선택합니다.
4. ODB 네트워크 생성을 선택합니다.
5. ODB 네트워크 이름에 네트워크 이름을 입력합니다. 이름은 1~255자여야 하며 영문자 또는 밑줄로 시작해야 합니다. 연속된 하이픈은 포함될 수 없습니다.
6. 가용 영역에서 AZ 이름을 선택합니다. 지원되는 AZ는 Oracle Database@AWS용 리전 지원 섹션을 참조하세요.
7. 클라이언트 서브넷 CIDR에서 클라이언트 연결에 대한 CIDR 범위를 지정합니다. 자세한 내용은 ODB 네트워크에 대한 클라이언트 서브넷 CIDR 요구 사항 섹션을 참조하세요.

8. 백업 서브넷 CIDR에서 백업 연결의 CIDR 범위를 지정합니다. 백업 트래픽을 격리하고 복원력을 개선하려면 백업 CIDR과 클라이언트 CIDR을 겹치지 않는 것이 좋습니다. 자세한 내용은 ODB 네트워크에 대한 백업 서브넷 CIDR 요구 사항 섹션을 참조하세요.
9. DNS 구성에서 다음 옵션 중 하나를 선택합니다.

   기본값

   도메인 이름 접두사에 도메인의 접두사로 사용할 이름을 입력합니다. 도메인 이름은 oraclevcn.com으로 고정됩니다. 예를 들어 **myhost**를 입력하면 정규화된 도메인 이름은 myhost.oraclevcn.com입니다.

   사용자 지정 도메인 이름

   도메인 이름에 전체 도메인 이름을 입력합니다. 예를 들어 myhost.myodb.com을 입력할 수 있습니다.
10. (선택 사항) 서비스 통합에서 VPC Lattice를 사용하여 네트워크와 통합할 서비스를 선택합니다. Oracle Database@AWS는 다양한 AWS 서비스와 통합되어 Oracle 데이터베이스에 향상된 기능과 연결 옵션을 제공합니다. 다음 통합 중 하나를 선택합니다.

    Amazon S3

    Amazon S3에 대한 직접 ODB 네트워크 액세스를 활성화합니다. 데이터베이스는 데이터 가져오기/내보내기 또는 사용자 지정 백업을 위해 S3에 액세스할 수 있습니다. JSON 정책을 입력할 수 있습니다. 자세한 내용은 Oracle Database@AWS의 Amazon S3에 대한 사용자 관리형 백업 섹션을 참조하세요.

    제로 ETL

    Amazon Redshift를 사용하여 트랜잭션 데이터에 대한 실시간 분석 및 기계 학습을 활성화합니다. 자세한 내용은 Amazon Redshift와 Oracle Database@AWS 제로 ETL 통합 섹션을 참조하세요.

> **Note**
>
> ODB 네트워크를 생성하면 Oracle Database@AWS가 Amazon S3에 대한 Oracle 관리형 백업의 네트워크 액세스를 자동으로 사전 구성합니다. 이 통합은 활성화하거나 비활성화할 수 없습니다. 자세한 내용은 AWS 서비스 통합 섹션을 참조하세요.

11. (선택 사항) 태그에서 네트워크에 대한 최대 50개의 태그를 입력합니다. 태그는 리소스를 구성하고 추적하는 데 사용할 수 있는 키-값 페어입니다.
12. ODB 네트워크 생성을 선택합니다.

ODB 네트워크를 생성한 후 VPC에 피어링할 수 있습니다. ODB 피어링은 Amazon VPC와 ODB 네트워크 간에 트래픽을 비공개로 라우팅할 수 있는 사용자 생성 네트워크 연결입니다. 피어링 후 VPC 내의 Amazon EC2 인스턴스는 동일한 네트워크 내에 있는 것처럼 ODB 네트워크의 리소스와 통신할 수 있습니다. 자세한 내용은 Oracle Database@AWS에서 Amazon VPC에 대한 ODB 피어링 구성 섹션을 참조하세요.

2단계: Oracle Database@AWS에서 Oracle Exadata 인프라 생성

Oracle Exadata 인프라는 Oracle Exadata 데이터베이스를 실행하는 데이터베이스 서버, 스토리지 서버 및 네트워킹의 기본 아키텍처입니다. Exadata X9M 또는 X11M을 시스템 모델로 선택합니다. 그런 다음 AWS 콘솔을 사용하여 Exadata 인프라에서 VM 클러스터를 생성할 수 있습니다.

Oracle Exadata 인프라와 ODB 네트워크를 어느 순서로든 생성할 수 있습니다. 인프라를 생성할 때 네트워킹 정보를 지정할 필요가 없습니다.

Oracle Exadata 인프라를 생성한 후에는 수정할 수 없습니다. Exadata 인프라를 삭제하려면 Oracle Database@AWS에서 Oracle Exadata 인프라 삭제 섹션을 참조하세요.

Exadata 인프라를 생성하려면

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 왼쪽 창에서 Exadata 인프라를 선택합니다.
3. Exadata 인프라 생성을 선택합니다.
4. Exadata 인프라 이름에 이름을 입력합니다. 이름은 1~255자여야 하며 영문자 또는 밑줄로 시작해야 합니다. 연속된 하이픈은 포함될 수 없습니다.
5. 가용 영역에서 지원되는 AZ 중 하나를 선택합니다. 그리고 다음을 선택합니다.
6. Exadata 시스템 모델에서 Exadata.X9M 또는 Exadata.X11M을 선택합니다. Exadata.X11M에서 다음 서버 유형도 선택합니다.
   - 데이터베이스 서버 유형에서 Exadata 인프라의 데이터베이스 서버 모델 유형을 선택합니다. 현재 X11M이 유일한 선택 항목입니다.

- 스토리지 서버 유형에서 Exadata 인프라의 스토리지 서버 모델 유형을 선택합니다. 현재 X11M-HC가 유일한 선택 항목입니다.

7. 데이터베이스 서버의 경우 기본값인 2를 그대로 두거나 슬라이더를 움직여 최대 32개의 서버를 선택합니다. 2개 이상을 지정하려면 OCI에서 한도 증가를 요청합니다.

   각 Exadata X9M 데이터베이스 서버는 126개 OCPU를 지원합니다. 각 Exadata X11M 데이터베이스 서버는 760개 ECPU를 지원합니다. 서버 수를 변경하면 총 컴퓨팅 수가 변경됩니다. OCPU 및 ECPU에 대한 자세한 내용은 Oracle 설명서의 Autonomous 데이터베이스의 컴퓨팅 모델을 참조하세요.

8. 스토리지 서버의 경우 기본값인 3을 그대로 두거나 슬라이더를 움직여 최대 64개의 서버를 선택합니다. 3개 이상을 지정하려면 OCI에서 한도 증가를 요청합니다. 각 X9M 스토리지 서버는 64TB를 제공합니다. 각 X11m 스토리지 서버는 80TB를 제공합니다. 서버 수를 변경하면 스토리지의 총 TB가 변경됩니다. 그리고 다음을 선택합니다.

9. 유지 관리 기간의 경우 시스템 유지 관리가 발생할 수 있는 시기를 구성합니다.

   a. 일정 기본 설정에 대해 다음 옵션 중 하나를 선택합니다.

      - Oracle 관리형 일정 - Oracle에서 유지 관리 활동을 위한 최적의 시간을 결정합니다.
      - 고객 관리형 일정 - 유지 관리 활동이 발생할 수 있는 시기를 지정합니다.

   b. 패치 모드의 경우, 다음 옵션 중 하나를 선택합니다.

      - 롤링 - 업데이트는 한 번에 하나의 노드에 적용되므로 패치 적용 중에 데이터베이스를 계속 사용할 수 있습니다.
      - 비롤링 - 업데이트는 모든 노드에 동시에 적용되므로 가동 중지 시간이 필요할 수 있습니다.

   c. 고객 관리형 일정을 선택한 경우 다음 추가 설정을 구성합니다.

      - 유지 관리 월에서 유지 관리를 수행할 수 있는 월을 선택합니다.
      - 해당 월의 주에서 유지 관리를 수행할 수 있는 주(첫 번째, 두 번째, 세 번째, 네 번째 또는 마지막)를 선택합니다.
      - 요일에서 유지 관리를 수행할 수 있는 요일(월요일~일요일)을 선택합니다.
      - 시작 시간에서 유지 관리 기간이 시작되는 시간을 선택합니다. 시간은 UTC 단위입니다.
      - 알림 리드 타임에서 예정된 유지 관리에 대한 알림을 미리 받을 일수를 선택합니다.

> **Note**
>
> Oracle Cloud Infrastructure는 이 기간 동안 시스템 유지 관리를 수행합니다. 유지 관리 중에는 Exadata 인프라를 계속 사용할 수 있지만 짧은 기간 동안 지연 시간이 길어질 수 있습니다.

10. (선택 사항) OCI 유지 관리 알림 연락처에 최대 10개의 이메일 주소를 입력합니다. AWS는 이러한 이메일 주소를 OCI에 전달합니다. 업데이트가 발생하면 OCI는 나열된 주소로 알림을 메일로 보냅니다.
11. (선택 사항) 태그에 인프라에 대해 최대 50개의 태그를 입력합니다. 태그는 리소스를 구성하고 추적하는 데 사용할 수 있는 키-값 페어입니다.
12. 다음을 선택하고 인프라 설정을 검토합니다.
13. Exadata 인프라 생성을 선택합니다.

3단계: Oracle Database@AWS에서 Exadata VM 클러스터 또는 Autonomous VM 클러스터 생성

Exadata VM 클러스터는 Oracle Exadata 데이터베이스를 생성할 수 있는 VM 세트입니다. Exadata 인프라에서 VM 클러스터를 생성합니다. 동일한 ODB 네트워크에서 서로 다른 Oracle Exadata 인프라를 사용하여 여러 VM 클러스터를 배포할 수 있습니다. Exadata VM 클러스터에서 생성하는 데이터베이스를 완전히 관리할 수 있습니다.

Autonomous VM 클러스터는 Autonomous 데이터베이스(ADB)를 실행하는 VM 수준에서 가상화된 Oracle Exadata 컴퓨팅 및 스토리지 리소스의 사전 할당된 풀입니다. Exadata VM 클러스터에서 생성하는 사용자 관리형 데이터베이스와 달리 Autonomous 데이터베이스는 데이터베이스 관리자가 아닌 Oracle에서 자체 조정, 자체 패치 및 관리합니다.

VM 클러스터를 생성할 때 다음 제한 사항을 고려하세요.

- ODB 네트워크 및 Oracle Exadata 인프라를 생성한 AZ에만 VM 클러스터를 배포할 수 있습니다.
- 계정 간에 VM 클러스터를 공유하지 않는 경우 Oracle Exadata 인프라와 동일한 AWS 계정에 있어야 합니다. AWS RAM을 사용하여 한 AWS 계정의 ODB 네트워크 및 Oracle Exadata 인프라를 신뢰할 수 있는 계정과 공유하는 경우 신뢰할 수 있는 계정은 자체 계정에 VM 클러스터를 생성할 수 있습니다.
- ODB 네트워크에는 VM 클러스터만 배포할 수 있습니다. 다른 리소스는 허용되지 않습니다.

- VM 클러스터를 생성한 후에는 스토리지 할당을 변경할 수 없습니다.

> **Important**
>
> 생성 프로세스는 VM 클러스터의 크기에 따라 6시간 이상 걸릴 수 있습니다.

Exadata VM cluster

Exadata VM 클러스터를 생성하려면

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 왼쪽 창에서 Exadata VM 클러스터를 선택합니다.
3. VM 클러스터 생성을 선택합니다.
4. VM 클러스터 이름에 이름을 입력합니다. 이름은 1~255자여야 하며 영문자 또는 밑줄로 시작해야 합니다. 연속된 하이픈은 포함될 수 없습니다.
5. (선택 사항) 그리드 인프라 클러스터 이름에 사용 중인 Oracle Database 버전과 일치하는 VM 클러스터의 그리드 인프라 버전을 입력합니다. 이름은 1~11자여야 하며 하이픈을 포함할 수 없습니다.
6. 시간대에서 시간대를 입력합니다.
7. 라이선스 옵션에서 Bring Your Own License (BYOL) 또는 라이선스 포함을 선택한 후 다음을 선택합니다. 이 라이선스는 Oracle에서 제공하는 OCI 라이선스이며 AWS에서 제공하는 라이선스가 아닙니다.
8. 다음과 같이 Exadata 인프라 설정을 구성합니다.

   a. 인프라에서 다음을 선택합니다.

      - Exadata 인프라 이름에서 이 VM 클러스터에 사용할 인프라를 선택합니다.
      - 그리드 인프라 버전에서 이 VM 클러스터에 사용할 버전을 선택합니다.
      - Exadata 이미지 버전에서 이 VM 클러스터에 사용할 버전을 선택합니다. 사용 가능한 최고 버전인 표시된 버전을 선택하는 것이 좋습니다.

   b. 데이터베이스 서버에서 VM 클러스터를 호스팅할 데이터베이스 서버를 하나 이상 선택합니다.

   c. 구성에서 다음을 수행합니다.

- 각 VM의 CPU 코어 수, 메모리 및 로컬 스토리지를 선택하거나 기본값을 그대로 사용합니다.
- VM 클러스터의 총 Exadata 스토리지 양을 선택하거나 기본값을 그대로 사용합니다.

d. (선택 사항) 스토리지 할당에서 다음 옵션 중 하나를 선택합니다.

- Exadata 희소 스냅샷에 대한 스토리지 할당 활성화
- 로컬 백업에 대한 스토리지 할당 활성화

옵션을 선택하면 사용 가능한 스토리지 할당이 변경됩니다. 나중에 이 스토리지 할당을 변경할 수 없습니다. 선택 사항을 검토한 다음, 다음을 선택합니다.

9. 다음과 같이 연결을 구성합니다.

a. ODB 네트워크에서 기존 ODB 네트워크를 선택합니다.

b. 호스트 이름 접두사에 VM 클러스터의 접두사를 입력합니다. 도메인 이름을 포함하지 않아야 합니다. 접두사는 Oracle Exadata VM 클러스터 호스트 이름의 처음 부분을 구성합니다.

> **Note**
>
> 호스트 도메인 이름은 oraclevcn.com으로 고정됩니다.

c. SCAN 리스너 포트(TCP/IP)에 단일 클라이언트 액세스 이름(SCAN) 리스너에 대한 TCP 액세스의 포트 번호를 입력합니다. 기본 포트는 1521입니다. 또는 2484, 6100, 6200, 7060, 7070, 7085 및 7879 포트 번호를 제외하고 1024–8999 범위의 사용자 지정 SCAN 포트를 입력할 수 있습니다. 그리고 다음을 선택합니다.

d. SSH 키 페어의 경우 VM 클러스터에 대한 SSH 액세스에 사용되는 하나 이상의 키 페어의 퍼블릭 키 부분을 입력합니다. 그리고 다음을 선택합니다.

10. (선택 사항) 다음과 같이 진단 및 태그를 선택합니다.

a. 진단 이벤트, 상태 모니터, 인시던트 로그 및 추적 수집에 대한 진단 수집을 활성화할지 여부를 선택합니다. Oracle은 이 진단 정보를 사용하여 문제를 식별, 추적 및 해결할 수 있습니다.

b. 태그에서 VM 클러스터에 대한 최대 50개의 태그를 입력합니다. 태그는 리소스를 구성하고 추적하는 데 사용할 수 있는 키-값 페어입니다. 그리고 다음을 선택합니다.

11. 설정을 검토합니다. 그 다음에 VM 클러스터 생성을 선택합니다.

Autonomous VM cluster

Autonomous VM 클러스터를 생성하려면

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 왼쪽 창에서 Autonomous VM 클러스터를 선택합니다.
3. Autonomous VM 클러스터 생성을 선택합니다.
4. VM 클러스터 이름에 이름을 입력합니다. 이름은 1~255자여야 하며 영문자 또는 밑줄로 시작해야 합니다. 연속된 하이픈은 포함될 수 없습니다.
5. 시간대에서 시간대를 입력합니다.
6. 라이선스 옵션에서 Bring Your Own License (BYOL) 또는 라이선스 포함을 선택한 후 다음을 선택합니다. 이 라이선스는 Oracle에서 제공하는 OCI 라이선스이며 AWS에서 제공하는 라이선스가 아닙니다.
7. 다음과 같이 Exadata 인프라 설정을 구성합니다.

   a. Exadata 인프라 이름에서 이 Autonomous VM 클러스터에 사용할 인프라를 선택합니다.

   b. 데이터베이스 서버의 경우 Autonomous VM 클러스터를 호스팅할 데이터베이스 서버를 하나 이상 선택합니다.

   c. 구성에서 다음을 수행합니다.

      - VM당 ECPU 코어 수, CPU당 데이터베이스 메모리, 데이터베이스 스토리지 및 최대 Autonomous 컨테이너 데이터베이스 수를 선택하거나 기본값을 수락합니다.
      - Autonomous VM 클러스터의 총 Exadata 스토리지 양을 선택하거나 기본값을 수락합니다.

8. 다음과 같이 연결을 구성합니다.

   a. ODB 네트워크에서 기존 ODB 네트워크를 선택합니다.

   b. SCAN 리스너 포트(TCP/IP)에 포트(비 TLS)의 포트 번호를 입력합니다. 기본 포트는 1521입니다. 또는 2484, 6100, 6200, 7060, 7070, 7085 및 7879 포트 번호를 제외하고 1024~8999 범위의 포트(TLS)를 입력할 수 있습니다. 그리고 다음을 선택합니다.

      상호 TLS 인증(mTLS) 활성화를 선택하여 상호 TLS 인증을 허용합니다.

9. (선택 사항) 다음과 같이 진단 및 태그를 선택합니다.

a. Oracle 관리형 일정 또는 고객 관리형 일정으로 수정 구성을 예약할지 여부를 선택합니다. 고객 관리형 일정을 선택하는 경우 유지 관리 월, 월의 주, 요일 및 시작 시간(UTC)을 설정합니다.

b. 태그의 경우 Autonomous VM 클러스터에 대해 최대 50개의 태그를 입력합니다. 태그는 리소스를 구성하고 추적하는 데 사용할 수 있는 키-값 페어입니다. 그리고 다음을 선택합니다.

10. 설정을 검토합니다. 그런 다음 Autonomous VM 클러스터 생성을 선택합니다.

4단계: Oracle Cloud Infrastructure에서 Oracle Exadata 데이터베이스 생성

Oracle Database@AWS에서는 AWS 콘솔, CLI 또는 API를 사용하여 다음 리소스를 생성하고 관리할 수 있습니다.

- ODB 네트워크
- Oracle Exadata 인프라
- Exadata VM 클러스터 및 Autonomous VM 클러스터
- ODB 피어링 연결

생성한 인프라에서 Oracle Exadata 데이터베이스를 생성하고 관리하려면 Oracle Database@AWS 대시보드 대신 Oracle Cloud Infrastructure 콘솔을 사용해야 합니다. Exadata VM 클러스터에서 사용자 관리형 Exadata 데이터베이스를 생성하고 Autonomous Exadata VM 클러스터에서 Autonomous Database를 생성할 수 있습니다. OCI에서 Oracle 데이터베이스를 생성하는 방법에 대한 자세한 내용은 Oracle Cloud Infrastructure 설명서의 Exadata 데이터베이스를 참조하세요.

Oracle Exadata 데이터베이스를 생성하려면

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 왼쪽 창에서 Exadata VM 클러스터 또는 Autonomous VM 클러스터를 선택합니다.
3. 세부 정보 페이지를 보려면 VM 클러스터를 선택합니다.
4. OCI에서 관리를 선택하여 Oracle Cloud Infrastructure 콘솔로 리디렉션합니다.
5. OCI에서 사용자 관리형 Exadata 데이터베이스 또는 Autonomous 데이터베이스를 생성합니다.

Oracle Database@AWS에서 Amazon VPC에 대한 ODB 피어링 구성

ODB 피어링은 Amazon VPC와 ODB 네트워크 간에 트래픽을 비공개로 라우팅할 수 있는 사용자 생성 네트워크 연결입니다. VPC와 ODB 네트워크 간에는 일대일 관계가 있습니다. 콘솔, CLI 또는 API를 사용하여 피어링 연결을 생성한 후에는 VPC 라우팅 테이블을 업데이트하고 DNS 확인을 구성해야 합니다. ODB 피어링에 대한 개념적 개요는 ODB 피어링 섹션을 참조하세요.

Oracle Database@AWS에서 ODB 피어링 연결 생성

ODB 피어링 연결을 사용하면 Oracle Exadata 인프라와 Amazon VPC에서 실행되는 애플리케이션 간에 프라이빗 네트워크 연결을 설정할 수 있습니다. 각 ODB 피어링 연결은 ODB 네트워크와 독립적으로 생성, 보기 및 삭제할 수 있는 별도의 리소스입니다.

ODB 피어링 연결을 생성할 때 피어 네트워크 CIDR 범위를 지정할 수 있습니다. 이 기법은 필요한 서브넷에 대한 네트워크 액세스를 제한하고, 공격의 잠재적 대상을 줄이고, 규정 준수 요구 사항에 맞게 보다 세분화된 네트워크 세분화를 지원합니다.

다음과 같은 유형의 ODB 피어링 연결을 생성할 수 있습니다.

동일 계정 ODB 피어링

ODB 네트워크와 동일한 AWS 계정의 Amazon VPC 간에 ODB 피어링 연결을 생성할 수 있습니다.

교차 계정 ODB 피어링

AWS RAM을 사용하여 ODB 네트워크를 공유한 후 한 계정의 ODB 네트워크와 다른 계정의 Amazon VPC 간에 ODB 피어링 연결을 생성할 수 있습니다. VPC 소유자 계정은 ODB 네트워크를 소유하지 않고도 피어링 연결에 지정된 CIDR 범위를 관리할 수 있습니다.

VPC와 ODB 네트워크 간에는 1:1 관계가 있습니다. VPC와 여러 ODB 네트워크 간에 또는 ODB 네트워크와 여러 VPC 간에 ODB 피어링 연결을 생성할 수 없습니다.

콘솔

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 탐색 창에서 ODB 피어링 연결을 선택합니다.

3. 피어링 연결 생성을 선택합니다.
4. (선택 사항) ODB 피어링 이름에 연결의 고유한 이름을 입력합니다.
5. ODB 네트워크에서 피어링할 ODB 네트워크를 선택합니다.
6. 피어 네트워크에서 ODB 네트워크와 피어링할 Amazon VPC를 선택합니다.
7. (선택 사항) 피어 네트워크 CIDR에서 ODB 네트워크에 액세스할 수 있는 피어 VPC의 추가 CIDR 블록을 지정합니다. CIDR을 지정하지 않으면 피어 VPC의 모든 CIDR에 대한 액세스가 허용됩니다.
8. (선택 사항) 태그에 키와 값 페어를 추가합니다.
9. 피어링 연결 생성을 선택합니다.

ODB 피어링 연결을 생성한 후 피어링된 ODB 네트워크로 트래픽을 라우팅하도록 Amazon VPC 라우팅 테이블을 구성합니다. 자세한 내용은 ODB 피어링을 위한 VPC 라우팅 테이블 구성 섹션을 참조하세요. Oracle Database@AWS는 ODB 네트워크 라우팅 테이블을 자동으로 구성합니다.

AWS CLI

ODB 피어링 연결을 생성하려면 `create-odb-peering-connection` 명령을 사용합니다.

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

ODB 네트워크에 대한 액세스를 특정 CIDR 범위로 제한하려면 `--peer-network-cidrs-to-be-added` 파라미터를 사용합니다. CIDR 범위를 지정하지 않으면 모든 범위에 액세스할 수 있습니다.

```
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 피어링 연결을 나열하려면 `list-odb-peering-connections` 명령을 사용합니다.

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

특정 ODB 피어링 연결에 대한 세부 정보를 가져오려면 `get-odb-peering-connection` 명령을 사용합니다.

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

ODB 피어링 연결 업데이트

기존 ODB 피어링 연결을 업데이트하여 피어 네트워크 CIDR을 추가하거나 제거할 수 있습니다. 피어 VPC에서 ODB 네트워크에 액세스할 수 있는 서브넷을 제어합니다.

콘솔

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 탐색 창에서 ODB 피어링 연결을 선택합니다.
3. 업데이트할 ODB 피어링 연결을 선택합니다.
4. 작업을 선택하고 피어링 연결 업데이트를 선택합니다.
5. 피어 네트워크 CIDR 섹션에서 필요에 따라 CIDR 블록을 추가하거나 제거합니다.
   - CIDR을 추가하려면 CIDR 추가를 선택하고 CIDR 블록을 입력합니다.
   - CIDR을 제거하려면 제거하려는 CIDR 블록 옆에 있는 X를 선택합니다.
6. 피어링 연결 업데이트를 선택합니다.

AWS CLI

ODB 피어링 연결에 피어 네트워크 CIDR을 추가하려면 `update-odb-peering-connection` 명령에서 `--peer-network-cidrs-to-be-added` 파라미터를 지정합니다.

```
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 피어링 연결에서 피어 네트워크 CIDR을 제거하려면 `update-odb-peering-connection` 명령에서 `--peer-network-cidrs-to-be-removed` 파라미터를 지정합니다.

```
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 피어링을 위한 VPC 라우팅 테이블 구성

라우팅 테이블에는 서브넷 또는 게이트웨이의 네트워크 트래픽이 전송되는 위치를 결정하는 라우팅이라는 규칙 세트가 포함되어 있습니다. 라우팅 테이블의 대상 CIDR은 트래픽이 이동할 IP 주소의 범위입니다. ODB 네트워크에 대한 ODB 피어링을 위해 VPC를 지정한 경우 VPC 라우팅 테이블을 ODB 네트워크의 대상 IP 범위로 업데이트합니다. ODB 피어링에 대한 자세한 내용은 ODB 피어링 섹션을 참조하세요.

라우팅 테이블을 업데이트하려면 AWS CLI `ec2 create-route` 명령을 사용합니다. 다음 예제에서는 Amazon VPC 라우팅 테이블을 업데이트합니다. 자세한 내용은 ODB 피어링을 위한 VPC 라우팅 테이블 구성 섹션을 참조하세요.

```
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 네트워크 라우팅 테이블은 VPC CIDR로 자동으로 업데이트됩니다. VPC의 모든 CIDR이 아닌 특정 서브넷 CIDR에 대해서만 ODB 네트워크에 대한 액세스를 허용하려면 ODB 피어링 연결을 생성할 때 피어 네트워크 CIDR을 지정하거나 기존 ODB 피어링 연결을 업데이트하여 피어링된 CIDR 범위를 추가하거나 제거할 수 있습니다. 자세한 내용은 Oracle Database@AWS에서 ODB 피어링 연결 생성 및 ODB 피어링 연결 업데이트(을)를 참조하세요.

VPC 라우팅 테이블에 대한 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 서브넷 라우팅 테이블과 AWS CLI 명령 참조의 ec2 create-route를 참조하세요.

Oracle Database@AWS에 대한 DNS 구성

Amazon Route 53는 DNS 라우팅에 사용할 수 있는 가용성과 확장성이 뛰어난 도메인 이름 시스템(DNS) 웹 서비스입니다. ODB 네트워크와 VPC 간에 ODB 피어링 연결을 생성할 때는 VPC 내에서 ODB 네트워크 리소스에 대한 DNS 쿼리를 해결하는 메커니즘이 필요합니다. Amazon Route 53를 사용하여 다음 리소스를 구성할 수 있습니다.

- 아웃바운드 엔드포인트

  엔드포인트는 DNS 쿼리를 ODB 네트워크로 전송하는 데 필요합니다.
- 해석기 규칙

이 규칙은 Route 53 Resolver가 ODB 네트워크의 DNS에 전달하는 DNS 쿼리의 도메인 이름을 지정합니다.

Oracle Database@AWS에서 DNS 작동 방식

Oracle Database@AWS는 ODB 네트워크의 도메인 이름 시스템(DNS) 구성을 자동으로 관리합니다. 도메인 이름의 경우 기본 도메인 이름에 대한 사용자 지정 접두사 `oraclevcn.com` 또는 전체 사용자 지정 도메인 이름을 지정할 수 있습니다. 자세한 내용은 1단계: Oracle Database@AWS에서 ODB 네트워크 생성 섹션을 참조하세요.

Oracle Database@AWS가 ODB 네트워크를 프로비저닝하면 다음 리소스가 생성됩니다.

- ODB 네트워크와 동일한 CIDR 블록이 있는 Oracle Cloud Infrastructure(OCI) Virtual Cloud Network(VCN)

  이 VCN은 고객의 연결된 OCI 테넌시에 있습니다. ODB 네트워크와 OCI VCN 간에는 1:1 매핑이 있습니다. 모든 ODB 네트워크는 OCI VCN과 연결됩니다.
- OCI VCN 내의 프라이빗 DNS 해석기

  이 DNS 해석기는 OCI VCN 내에서 DNS 쿼리를 처리합니다. OCI 자동화는 VM 클러스터에 대한 레코드를 생성합니다. 스캔에서는 `*.oraclevcn.com` FQDN(Fully Qualified Domain Name)을 사용합니다.
- 프라이빗 DNS 해석기에 대한 OCI VCN 내의 DNS 수신 엔드포인트

  DNS 수신 엔드포인트는 Oracle Database@AWS 콘솔의 ODB 네트워크 세부 정보 페이지에서 찾을 수 있습니다.

Oracle Database@AWS의 ODB 네트워크에서 아웃바운드 엔드포인트 구성

아웃바운드 엔드포인트를 사용하면 VPC에서 네트워크 또는 IP 주소로 DNS 쿼리를 전송할 수 있습니다. 엔드포인트는 쿼리가 시작되는 IP 주소를 지정합니다. VPC에서 ODB 네트워크로 DNS 쿼리를 전달하려면 Route 53 콘솔을 사용하여 아웃바운드 엔드포인트를 생성합니다. 자세한 내용은 네트워크로 아웃바운드 DNS 쿼리 전달을 참조하세요.

ODB 네트워크에서 아웃바운드 엔드포인트를 구성하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
2. 왼쪽 창에서 아웃바운드 엔드포인트를 선택합니다.
3. 탐색 모음에서 아웃바운드 엔드포인트를 생성할 VPC의 리전을 선택합니다.
4. Create outbound endpoint(아웃바운드 엔드포인트 생성)를 선택합니다.
5. 다음과 같이 아웃바운드 엔드포인트에 대한 일반 설정 섹션을 완료합니다.

   a. 다음에 대한 아웃바운드 TCP 및 UDP 연결을 허용하는 보안 그룹을 선택합니다.

      - ODB 네트워크에서 해석기가 DNS 쿼리에 사용하는 IP 주소입니다.
      - 해석기가 ODB 네트워크에서 DNS 쿼리에 사용하는 포트

   b. 엔드포인트 유형에서 IPv4를 선택합니다.

   c. 이 엔드포인트의 프로토콜에서 Do53을 선택합니다.
6. IP 주소에 다음 정보를 제공합니다.

   - IP 주소를 지정하거나 Route 53 Resolver가 서브넷의 사용 가능한 주소에서 IP 주소를 선택하도록 합니다. DNS 쿼리에 대해 최소 2개에서 최대 6개의 IP 주소를 선택합니다. 최소한 2개의 가용 영역에 IP 주소를 지정하는 것이 좋습니다.
   - 서브넷에서 다음을 포함한 서브넷을 선택합니다.
     - ODB 네트워크에서 DNS 리스너의 IP 주소에 대한 경로를 포함하는 라우팅 테이블
     - 해석기가 ODB 네트워크의 DNS 쿼리에 사용하는 IP 주소 및 포트에 대한 UDP 및 TCP 트래픽을 허용하는 네트워크 액세스 제어 목록(ACL)
     - 대상 포트 범위 1024-65535에서 해석기의 트래픽을 허용하는 네트워크 ACL
7. (선택 사항) 태그에 엔드포인트의 태그를 지정합니다.
8. 제출을 선택합니다.

Oracle Database@AWS에서 해석기 규칙 구성

해석기 규칙은 DNS 쿼리를 라우팅하는 방법을 결정하는 일련의 기준입니다. 재사용하거나 해석기가 ODB 네트워크의 DNS로 전달하는 DNS 쿼리의 도메인 이름을 지정하는 규칙을 생성합니다.

기존 해석기 규칙 사용

기존 해석기 규칙을 사용하려면 규칙 유형에 따라 작업이 달라집니다.

AWS 계정의 VPC와 동일한 AWS 리전에 있는 동일한 도메인에 대한 규칙

새 규칙을 생성하는 대신 VPC와 규칙을 연결합니다. 규칙 대시보드에서 규칙을 선택하고 AWS 리전의 해당 VPC와 연결합니다.

VPC와 동일한 리전에 있지만 다른 계정에 있는 동일한 도메인에 대한 규칙

AWS Resource Access Manager를 사용하여 원격 계정의 규칙을 계정과 공유합니다. 규칙을 공유할 때 해당 아웃바운드 엔드포인트도 공유합니다. 규칙을 계정과 공유한 후 규칙 대시보드에서 규칙을 선택하고 계정의 VPC와 연결합니다. 자세한 내용은 전달 규칙 관리 섹션을 참조하세요.

새 해석기 규칙 생성

기존 해석기 규칙을 재사용할 수 없는 경우 Amazon Route 53 콘솔을 사용하여 새 규칙을 생성합니다.

새 해석기 규칙을 생성하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
2. 왼쪽 창에서 규칙을 선택합니다.
3. 탐색 모음에서 아웃바운드 엔드포인트가 있는 VPC의 리전을 선택합니다.
4. 규칙 생성을 선택합니다.
5. 다음과 같이 아웃바운드 트래픽 규칙 섹션을 완료합니다.
   a. 규칙 유형에서 전달 규칙을 선택합니다.
   b. 도메인 이름에 ODB 네트워크의 전체 도메인 이름을 지정합니다.
   c. 이 규칙을 사용하는 VPC의 경우 DNS 쿼리가 ODB 네트워크로 전달되는 VPC와 연결합니다.
   d. 아웃바운드 엔드포인트에서 Oracle Database@AWS의 ODB 네트워크에서 아웃바운드 엔드포인트 구성에서 생성한 아웃바운드 엔드포인트를 선택합니다.

   > **Note**
   > 이 규칙과 연결된 VPC는 아웃바운드 엔드포인트를 생성한 VPC와 같을 필요가 없습니다.

6. 다음과 같이 대상 IP 주소 섹션을 완료합니다.
   a. IP 주소에서 ODB 네트워크에 있는 DNS 리스너 IP의 IP 주소를 지정합니다.

b. 포트에 대해 53을 지정합니다. 이는 해석기가 DNS 쿼리에 사용하는 포트입니다.

> **Note**
>
> Route 53 Resolver는 이 규칙과 일치하고 이 규칙과 연결된 VPC에서 시작된 DNS 쿼리를 참조된 아웃바운드 엔드포인트로 전달합니다. 이 쿼리는 대상 IP 주소에 지정한 대상 IP 주소로 전달됩니다.

c. 전송 프로토콜에서 Do53을 선택합니다.

7. (선택 사항) 태그에서 규칙에 대한 태그를 지정합니다.
8. 제출을 선택합니다.

Oracle Database@AWS에서 DNS 구성 테스트

아웃바운드 엔드포인트 및 해석기 규칙을 생성한 후 DNS가 올바르게 확인되는지 테스트합니다. 애플리케이션 VPC에서 Amazon EC2 인스턴스를 사용하여 다음과 같이 DNS 확인을 수행합니다.

Linux 또는 macOS의 경우

`dig` *`record-name record-type`* 형식의 명령을 사용합니다.

Windows –

`nslookup -type=`*`record-name record-type`* 형식의 명령을 사용합니다.

Oracle Database@AWS에 대한 Amazon VPC Transit Gateway 구성

Amazon VPC Transit Gateway는 가상 프라이빗 클라우드(VPC)와 온프레미스 네트워크를 상호 연결하는 네트워크 전송 허브입니다. 허브 앤 스포크 아키텍처의 각 VPC는 전송 게이트웨이에 연결하여 다른 연결된 VPC에 액세스할 수 있습니다. AWS Transit Gateway는 IPv4 및 IPv6 모두에 대한 트래픽을 지원합니다.

Oracle Database@AWS에서 ODB 네트워크는 하나의 VPC에 대한 피어링 연결만 지원합니다. 전송 게이트웨이를 ODB 네트워크에 피어링된 VPC에 연결하는 경우 여러 VPC를 이 게이트웨이에 연결할 수 있습니다. 이러한 다양한 VPC에서 실행되는 애플리케이션은 ODB 네트워크에서 실행되는 Exadata VM 클러스터에 액세스할 수 있습니다.

다음 다이어그램은 두 개의 VPC와 하나의 온프레미스 네트워크에 연결된 전송 게이트웨이를 보여줍니다.

위의 다이어그램에서 하나의 VPC가 ODB 네트워크에 피어링됩니다. 이 구성에서 ODB 네트워크는 전송 게이트웨이에 연결된 모든 VPC로 트래픽을 라우팅할 수 있습니다. 이러한 각 VPC의 라우팅 테이블에는 ODB 네트워크를 대상으로 하는 트래픽을 Transit Gateway로 보내는 경로와 로컬 경로가 둘 다 포함됩니다.

AWS Transit Gateway에서는 시간당 전송 게이트웨이에 대한 연결 수와 AWS Transit Gateway를 통해 흐르는 트래픽 양에 대해 요금이 부과됩니다. 비용 정보는 AWS Transit Gateway 요금을 참조하세요.

요구 사항

Oracle Database@AWS 환경이 다음 요구 사항을 충족하는지 확인하세요.

- ODB 네트워크에 피어링되는 VPC는 동일한 AWS 계정에 있어야 합니다. 피어링된 VPC가 ODB 네트워크와 다른 계정에 있는 경우 공유 구성에 관계없이 Transit Gateway Attachment가 실패합니다.
- ODB 네트워크에 피어링되는 VPC에는 Transit Gateway Attachment가 있어야 합니다.

> **Note**
>
> 전송 게이트웨이가 공유하도록 구성된 경우 모든 계정에 상주할 수 있습니다. 따라서 게이트웨이 자체가 VPC 및 ODB 네트워크와 동일한 계정에 있을 필요는 없습니다.

- Transit Gateway Attachment는 ODB 네트워크와 동일한 가용 영역(AZ)에 있어야 합니다.

제한 사항

Oracle Database@AWS용 Amazon VPC Transit Gateway의 제한 사항은 다음과 같습니다.

- Amazon VPC Transit Gateway는 ODB 네트워크를 연결로 사용하기 위한 기본 통합을 제공하지 않습니다. 따라서 다음과 같은 VPC 기능은 사용할 수 없습니다.
  - 퍼블릭 DNS 호스트 이름을 프라이빗 IP 주소로 확인
  - ODB 네트워크 토폴로지, 라우팅 및 연결 상태 변경에 대한 이벤트 알림
- ODB 네트워크로의 멀티캐스트 트래픽은 지원되지 않습니다.

전송 게이트웨이 설정 및 구성

Amazon VPC 콘솔 또는 `aws ec2` 명령을 사용하여 전송 게이트웨이를 생성하고 구성합니다. 다음 절차에서는 AWS 계정의 VPC에 피어링된 ODB 네트워크가 없다고 가정합니다. ODB 네트워크와 VPC가 이미 계정에 피어링되어 있는 경우 1~3단계를 건너뜁니다.

> **Note**
>
> VPC에서 연결을 연결하거나 다시 연결하는 경우 ODB ODB 네트워크에 CIDR 범위를 다시 입력해야 합니다.

Oracle Database@AWS에 대한 전송 게이트웨이를 설정하고 구성하려면

1. ODB 네트워크를 생성합니다. 자세한 내용은 1단계: Oracle Database@AWS에서 ODB 네트워크 생성 섹션을 참조하세요.
2. ODB 네트워크가 포함된 동일한 계정을 사용하여 VPC를 생성합니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC 생성을 참조하세요.
3. ODB 네트워크와 VPC 간에 ODB 피어링 연결을 생성합니다. 자세한 내용은 Oracle Database@AWS에서 Amazon VPC에 대한 ODB 피어링 구성 섹션을 참조하세요.
4. Amazon VPC Transit Gateway 사용을 시작하기의 단계에 따라 전송 게이트웨이를 설정합니다. 게이트웨이는 ODB 네트워크 및 VPC와 동일한 AWS 계정에 있거나 다른 계정에서 공유해야 합니다.

   > **Important**
   >
   > ODB 네트워크와 동일한 AZ에 Transit Gateway Attachment를 생성합니다.

5. 코어 네트워크에 연결하려는 VPC 및 온프레미스 네트워크의 ODB 네트워크에 CIDR 범위를 추가합니다. 자세한 내용은 Oracle Database@AWS에서 ODB 네트워크 업데이트 섹션을 참조하세요.

   CLI를 사용하는 경우, `--peered-cidrs-to-be-added` 및 `--peered-cidrs-to-be-removed`와 함께 `update-odb-network` 명령을 실행합니다. 자세한 내용은 AWS CLI 명령 참조를 참조하세요.

Oracle Database@AWS에 대한 AWS Cloud WAN 구성

AWS Cloud WAN은 관리형 광역 네트워크(WAN) 서비스입니다. AWS Cloud WAN을 사용하여 클라우드 및 온프레미스 환경에서 실행되는 리소스를 연결하는 통합 글로벌 네트워크를 구축, 관리 및 모니터링할 수 있습니다.

AWS Cloud WAN에서 글로벌 네트워크는 네트워크 객체의 상위 수준 컨테이너 역할을 하는 단일 프라이빗 네트워크입니다. 코어 네트워크는 AWS에서 관리하는 글로벌 네트워크의 일부입니다.

AWS Cloud WAN은 다음과 같은 주요 이점을 제공합니다.

- 여러 리전에서 보안을 유지하면서 운영을 간소화하는 중앙 집중식 네트워크 관리
- 여러 라우팅 도메인을 통해 트래픽을 격리하는 세분화 기능이 내장된 코어 네트워크
- 글로벌 네트워크에서 네트워크 관리를 자동화하고 일관된 구성을 정의하는 정책 지원

Oracle Database@AWS에서 ODB 네트워크는 하나의 VPC에 대한 피어링만 지원합니다. AWS Cloud WAN 코어 네트워크를 피어링된 VPC에 연결하면 글로벌 트래픽 라우팅이 활성화됩니다. 여러 리전에 걸쳐 연결된 VPC의 애플리케이션은 ODB 네트워크의 Exadata VM 클러스터에 액세스할 수 있습니다. 자체 세그먼트에서 ODB 네트워크 트래픽을 격리하거나 다른 세그먼트에 대한 액세스를 활성화할 수 있습니다.

다음 다이어그램은 3개의 VPC와 1개의 온프레미스 네트워크에 연결된 AWS Cloud WAN 코어 네트워크를 보여줍니다.

AWS Cloud WAN은 ODB 네트워크를 연결로 사용하기 위한 기본 통합을 제공하지 않습니다. 따라서 다음과 같은 VPC 기능은 사용할 수 없습니다.

- 퍼블릭 DNS 호스트 이름을 프라이빗 IP 주소로 확인
- ODB 네트워크 토폴로지, 라우팅 및 연결 상태 변경에 대한 이벤트 알림

AWS Cloud WAN에서는 다음에 대해 시간당 요금이 부과됩니다.

- 리전 수(코어 네트워크 엣지)
- 코어 네트워크 연결 수
- 연결을 통해 코어 네트워크를 통해 흐르는 트래픽의 양

자세한 요금 정보는 AWS Cloud WAN 요금을 참조하세요.

Oracle Database@AWS에 대한 코어 네트워크를 구성하려면

1. 코어 네트워크에 연결하려는 VPC 및 온프레미스 네트워크의 ODB 네트워크에 CIDR 범위를 추가합니다. 자세한 내용은 Oracle Database@AWS에서 ODB 네트워크 업데이트 섹션을 참조하세요.

   > **Note**
   >
   > VPC에서 연결을 연결하거나 다시 연결하는 경우 ODB ODB 네트워크에 CIDR 범위를 다시 입력해야 합니다.

2. AWS Cloud WAN 글로벌 네트워크 및 코어 네트워크 생성의 단계를 따릅니다.

Oracle Database@AWS의 권한 공유

Oracle Database@AWS를 사용하면 동일한 AWS 조직의 AWS 계정에서 Oracle Database@AWS에 대한 AWS Marketplace 권한을 공유할 수 있습니다. 이를 통해 다른 계정은 구독을 사용하여 자체 Oracle Exadata 인프라 및 ODB 네트워크 리소스를 프로비저닝할 수 있습니다.

공유 방법

Oracle Database@AWS는 다음 두 가지 공유 방법을 지원합니다.

AWS License Manager와의 권한 공유

- 다른 계정에 자체 Oracle Exadata 인프라 및 ODB 네트워크 리소스를 프로비저닝할 수 있는 기능 부여
- 각 계정은 전체 리소스 수명 주기 제어로 독립적으로 작동합니다.
- 팀 또는 사업부 간에 셀프 서비스 프로비저닝을 활성화하는 데 가장 적합

AWS Resource Access Manager(AWS RAM)와 리소스 공유

- 이미 프로비저닝된 Oracle Exadata 인프라 및 ODB 네트워크 리소스 공유
- 수신자 계정이 VM 클러스터를 생성할 수 있도록 인프라 관리를 중앙 집중화합니다.
- 여러 계정이 동일한 인프라를 사용하도록 하여 비용 최적화

조직의 요구 사항에 따라 두 공유 방법을 동시에 사용할 수 있습니다.

Oracle Database@AWS 권한 공유에 대한 제한 사항

Oracle Database@AWS 권한을 공유할 때는 다음 제한 사항에 유의하세요.

- AWS 조직 내의 AWS 계정와만 공유할 수 있습니다.
- 전체 조직 단위(OU) 또는 전체 조직과 공유할 수 없습니다.
- 계정은 하나의 구매자 계정에서만 권한을 받을 수 있습니다(단일 비공개 제안에서).
- 구매자 계정은 다른 구매자 계정과 권한을 공유할 수 없습니다.

- 수신자 계정은 공유 권한을 사용하려면 먼저 Oracle Database@AWS 서비스를 초기화해야 합니다.
- 권한 부여 작업은 미국 동부(버지니아 북부) 리전에서만 수행할 수 있습니다.

계정 간에 Oracle Database@AWS 권한 공유

비용을 최적화하면서 공동 작업을 활성화하려면 Oracle Database@AWS 권한을 동일한 AWS 조직 내의 다른 AWS 계정와 공유합니다. 이 주제에서는 AWS License Manager를 사용하여 권한을 공유하는 방법을 설명합니다.

권한을 공유하기 위한 사전 조건

Oracle Database@AWS 권한을 공유하기 전에 다음이 있는지 확인합니다.

- 활성 Oracle Database@AWS 구독(AWS Marketplace를 통해 비공개 제안을 수락한 구매자 계정이어야 함)
- 권한을 공유하려는 조직 내 AWS 계정의 ID
- 권한 부여자 및 피부여자가 AWS License Manager 리소스 및 작업을 사용하는 데 필요한 권한(자세한 내용은 AWS License Manager 사용 설명서의 License Manager에 대한 자격 증명 및 액세스 관리 참조)
- 사용자(권한 부여자) 및 권한 수신자(피부여자)에 대해 아래에 나열된 권한

권한 공유에 필요한 권한

Oracle Database@AWS에는 AWS License Manager 권한 외에도 다음 권한이 필요합니다.

권한 부여자 권한

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

피부여자 권한

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

AWS License Manager를 사용하여 다른 계정과 Oracle Database@AWS 권한 공유

권한을 다른 AWS 계정과 공유하려면 AWS License Manager를 사용하여 권한 부여를 생성합니다. 자세한 내용은 AWSLicense Manager 사용 설명서의 License Manager 권한 배포를 참조하세요.

권한 부여를 생성한 후 수신자(피부여자)는 다음을 수행해야 합니다.

- 권한 부여를 수락하고 활성화합니다. 자세한 내용은 AWS License Manager 사용 설명서의 License Manager에서 권한 부여 수락 및 활성화를 참조하세요.
- Oracle Database@AWS의 초기화 지침을 따릅니다.

초기화가 완료되면 피부여자는 공유 권한을 사용하여 Oracle Database@AWS 리소스를 프로비저닝할 수 있습니다.

Oracle Database@AWS의 리소스 공유

Oracle Database@AWS를 사용하면 동일한 AWS 조직의 여러 AWS 계정에서 Exadata 인프라와 ODB 네트워크를 공유할 수 있습니다. 이를 통해 인프라를 한 번 프로비저닝 후 신뢰할 수 있는 계정 간에 재사용할 수 있으므로 책임을 분리하면서 비용을 절감할 수 있습니다.

리소스를 공유하는 경우:

- 리소스를 소유한 계정(소유자 계정)은 리소스 수명 주기에 대한 제어를 유지합니다.
- 공유 리소스(신뢰할 수 있는 계정)에 대한 액세스 권한을 받는 계정은 부여된 권한에 따라 이러한 리소스를 보고 사용할 수 있습니다.
- 신뢰할 수 있는 계정은 공유 인프라에서 자체 리소스를 생성할 수 있지만 기본 공유 리소스는 삭제할 수 없습니다.

AWS RAM과 Oracle Database@AWS 통합

Oracle Database@AWS는 AWS Resource Access Manager(AWS RAM)를 사용하여 계정 간에 리소스를 안전하고 제어된 방식으로 공유할 수 있습니다. AWS RAM을 사용하면 동일한 AWS 조직 내의 여러 AWS 계정에서 Oracle Database@AWS 리소스를 안전하게 공유할 수 있습니다. AWS RAM은 리소스 공유를 간소화하고 운영 오버헤드를 줄이며 공유된 Oracle Database@AWS 리소스에 대한 보안 및 가시성을 제공합니다.

AWS RAM을 사용하여 리소스 공유로 생성한 사용자 소유 리소스를 공유할 수 있습니다. 리소스 공유는 공유할 리소스와 공유 대상 AWS 계정을 지정합니다.

Oracle Database@AWS에서 리소스 공유의 이점

계정 간에 Oracle Database@AWS 리소스를 공유하면 다음과 같은 이점이 있습니다.

- 비용 최적화 - 관리 계정을 통해 비용이 많이 드는 Exadata 인프라를 한 번 프로비저닝하고 여러 계정과 공유하여 전체 비용을 절감합니다.
- 책임 분리 - 협업을 허용하면서 인프라 관리자와 데이터베이스 사용자 간의 명확한 경계를 유지합니다.
- 간소화된 관리 - 분산 데이터베이스 작업을 활성화하면서 인프라 프로비저닝 및 관리를 중앙 집중화합니다.

- 일관된 거버넌스 - 공유 리소스에 일관된 정책 및 제어를 적용합니다.

예를 들어 관리자는 AWS 계정에서 Oracle Exadata 인프라 및 ODB 네트워크를 프로비저닝하고 개발자 계정과 공유할 수 있습니다. 그러면 개발자는 비용이 많이 드는 자체 하드웨어를 프로비저닝할 필요 없이 이 공유 인프라에서 VM 클러스터를 생성할 수 있습니다. 이 접근 방식은 계정 간에 적절한 책임 분리를 유지하면서 비용을 크게 줄입니다.

Oracle Database@AWS에서 리소스 공유가 작동하는 방식

다음과 같은 Oracle Database@AWS 리소스를 공유할 수 있습니다.

- Oracle Exadata 인프라
- ODB 네트워크

Oracle Database@AWS는 다음 프로세스를 통해 이전 리소스를 공유합니다.

1. 구매자 계정(AWS 마켓플레이스를 통해 Oracle Database@AWS 비공개 제안을 수락하는 계정)은 Exadata 인프라 및 ODB 네트워크와 같은 Oracle Database@AWS 리소스를 프로비저닝합니다.
2. 구매자 계정은 AWS RAM을 사용하여 리소스 공유를 생성하고 공유할 리소스와 공유할 신뢰할 수 있는 계정을 지정합니다.
3. 동일한 조직에 있는 신뢰할 수 있는 계정의 리소스 공유가 자동으로 수락됩니다.
4. 공유 리소스를 사용하기 전에 신뢰할 수 있는 계정은 `aws odb initialize-service` 명령을 사용하거나 Oracle Database@AWS 콘솔에서 계정 활성화를 선택하여 계정에서 Oracle Database@AWS 서비스를 초기화해야 합니다.
5. 초기화 후 신뢰할 수 있는 계정은 공유 Exadata 인프라 및 ODB 네트워크의 VM 클러스터와 같은 공유 인프라에서 자체 리소스를 생성할 수 있습니다.

신뢰할 수 있는 계정의 공유 리소스에 대한 권한

리소스를 공유하면 Oracle Database@AWS는 각 리소스 유형에 대해 특정 작업(관리형 권한)을 자동으로 선택합니다.

Exadata 인프라의 경우

Oracle Database@AWS는 신뢰할 수 있는 계정에 다음 권한을 부여합니다.

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

ODB 네트워크의 경우

신뢰할 수 있는 계정에는 다음 권한이 부여됩니다.

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

리소스 공유는 Oracle Database@AWS 리소스의 계층적 특성을 준수합니다. 예를 들어 Exadata 인프라를 공유하는 경우 신뢰할 수 있는 계정은 이 인프라에서 VM 클러스터를 생성할 수 있지만 Exadata 인프라 자체를 수정하거나 삭제할 수는 없습니다.

리소스가 공유 해제되면 신뢰할 수 있는 계정은 공유 인프라에서 새 리소스를 생성할 수 없게 됩니다. 그러나 이미 생성한 모든 리소스는 액세스 가능하고 작동합니다.

Oracle Database@AWS 리소스 공유에 대한 제한 사항

리소스를 공유하기 전에 다음 제한 사항에 유의하세요.

리소스 공유 제한 사항

Oracle Database@AWS 리소스를 공유할 때는 다음 제한 사항에 유의하세요.

- AWS 계정 ID와만 리소스를 공유할 수 있습니다.
- 동일한 AWS 조직 내에서 AWS 계정에 대한 리소스만 공유할 수 있습니다.
- 특정 AWS 리전 내에서 리소스를 공유합니다. 리전 간에 리소스를 공유하려면 각 리전에서 별도의 리소스 공유를 생성해야 합니다.
- 리소스 공유를 생성하면 각 리소스 유형에 대한 작업(관리형 권한)이 자동으로 선택되며 수정할 수 없습니다.
- Oracle Database@AWS를 리소스로 사용하고 다른 AWS 계정과 공유할 수 없습니다.
- 신뢰할 수 있는 계정은 하나의 구매자 계정(단일 비공개 제안)에서만 공유 리소스를 사용할 수 있습니다. 따라서 두 구매자 계정은 동일한 신뢰할 수 있는 계정과 리소스를 공유할 수 없습니다.
- 구매자 계정은 다른 구매자 계정과 리소스를 공유할 수 없습니다.
- 신뢰할 수 있는 계정과 공유된 리소스는 먼저 구매자의 홈 리전에 있는 구매자 계정에서 공유해야 합니다.
- 리소스를 공유 해제할 때는 약 15분 정도 기다렸다가 동일한 리소스를 동일한 신뢰할 수 있는 계정으로 다시 공유하는 것이 좋습니다.

공유 리소스 생성 및 사용에 대한 제한 사항

Oracle Database@AWS 리소스를 생성하거나 사용할 때는 다음 제한 사항에 유의하세요.

- 구매자 계정만 Exadata 인프라 및 ODB 네트워크 리소스를 생성할 수 있습니다. 구매자 계정은 Oracle Database@AWS 비공개 제안을 수락하는 계정입니다.
- 신뢰할 수 있는 계정은 구매자 계정에서 공유하는 Exadata 인프라에서만 리소스를 생성할 수 있습니다.
- 신뢰할 수 있는 계정은 공유 리소스를 사용하기 전에 계정에서 Oracle Database@AWS 서비스를 초기화해야 합니다.

공유 리소스 삭제에 대한 제한 사항

- 신뢰할 수 있는 계정에서 생성한 VM 클러스터가 있는 Exadata 인프라는 해당 VM 클러스터가 제거될 때까지 삭제할 수 없습니다.
- ODB 피어링 연결이 제거될 때까지 신뢰할 수 있는 계정에서 생성된 ODB 피어링 연결이 있는 ODB 네트워크를 삭제할 수 없습니다.
- 구매자 계정은 신뢰할 수 있는 계정에서 생성한 Oracle Database@AWS 리소스를 삭제할 수 없습니다.

- 신뢰할 수 있는 계정은 공유 리소스를 볼 수 있지만 구매자 계정이 소유한 Oracle Database@AWS 리소스는 수정하거나 삭제할 수 없습니다.

계정 간 Oracle Database@AWS 리소스 공유

비용을 최적화하면서 공동 작업을 활성화하려면 Oracle Database@AWS 리소스를 동일한 AWS 조직 내의 다른 AWS 계정와 공유합니다. 이 주제에서는 AWS Resource Access Manager(AWS RAM)를 사용하여 리소스를 공유하는 방법을 설명합니다.

주제

- 리소스 공유를 위한 사전 조건
- AWS RAM을 사용하여 Oracle Database@AWS 리소스를 다른 계정과 공유
- 리소스 공유 보
- AWS RAM을 사용하여 리소스 공유 업데이트 또는 삭제

리소스 공유를 위한 사전 조건

Oracle Database@AWS 리소스를 공유하기 전에 다음이 있는지 확인합니다.

- 활성 Oracle Database@AWS 구독(AWS Marketplace를 통해 비공개 제안을 수락한 구매자 계정이어야 함)
- Exadata 인프라 또는 ODB 네트워크와 같이 공유하려는 리소스의 ID 또는 이름
- 리소스를 공유하려는 조직 내 AWS 계정의 ID
- AWS RAM에서 리소스 공유를 생성하는 데 필요한 권한
- AWS RAM을 사용하여 AWS Organizations와 리소스를 공유하는 기능(자세한 내용은 AWS Resource Access Manager 사용 설명서의 AWS Organizations내에서 리소스 공유 활성화 참조)

AWS RAM을 사용하여 Oracle Database@AWS 리소스를 다른 계정과 공유

Exadata 인프라 또는 ODB 네트워크를 다른 AWS 계정과 공유하려면 AWS RAM을 사용하여 리소스 공유를 생성합니다. 이렇게 하면 신뢰할 수 있는 계정이 Exadata 인프라에서 VM 클러스터를 생성할 수 있습니다.

콘솔

1. AWS RAM 콘솔(https://console.aws.amazon.com/ram/)을 엽니다.

2. 리소스 공유 생성을 선택합니다.
3. 이름에 리소스 공유를 설명하는 이름을 입력합니다.
4. 리소스 유형 선택에서 다음 리소스 중 하나를 선택합니다.
   - Oracle Database@AWS ODB 네트워크
   - Oracle Database@AWS Exadata 인프라
5. 공유할 Exadata 인프라 리소스를 선택합니다. 위탁자에게 액세스 권한을 부여할 때까지 다음을 선택합니다.
6. 위탁자에서 AWS 계정을 선택한 다음 공유하려는 AWS 계정 ID를 입력합니다.
7. 관리형 권한에서 다음 권한을 선택하여 신뢰할 수 있는 계정이 공유 Exadata 인프라에서 VM 클러스터를 생성하도록 허용합니다.
   - AWSRAMDefaultPermissionODBNetwork
   - AWSRAMDefaultPermissionODBCloudExadataInfrastructure
8. 리소스 공유 생성을 선택합니다.

AWS CLI

AWS CLI를 사용하여 리소스를 공유하려면 `aws ram create-resource-share` 명령을 사용합니다. 다음 예제에서는 지정된 Exadata 인프라를 222222222222 계정과 공유하는 `ExadataInfraShare`라는 리소스 공유를 생성하여 이 계정이 공유 인프라에서 VM 클러스터를 생성할 수 있도록 합니다.

```
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
```

리소스 공유 보

공유한 리소스 및 이를 공유한 계정을 보려면:

콘솔

1. AWS RAM 콘솔(https://console.aws.amazon.com/ram/)을 엽니다.
2. 공유 리소스를 선택하여 다른 계정과 공유한 리소스를 봅니다.

3. 리소스 공유를 선택하여 공유된 리소스 및 공유된 위탁자를 포함한 세부 정보를 봅니다.

AWS CLI

AWS CLI를 사용하여 리소스 공유를 보려면 `get-resource-shares` 명령을 사용합니다.

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

특정 리소스 공유의 리소스를 보려면 `list-resources` 명령을 사용합니다.

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

리소스 공유가 공유되는 위탁자(계정)를 보려면 `list-principals` 명령을 사용합니다.

```
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 RAM을 사용하여 리소스 공유 업데이트 또는 삭제

AWS RAM을 사용하여 신뢰할 수 있는 계정과 리소스 공유를 중지하려면 다음 작업 중 하나를 수행합니다.

- 리소스 공유에서 리소스를 제거합니다.
- 리소스 공유에서 신뢰할 수 있는 계정을 제거합니다.
- 리소스 공유를 삭제합니다.

공유 리소스에 대한 액세스를 취소하거나 삭제하기 전에 다음 영향을 고려하세요.

- 신뢰할 수 있는 계정은 공유되지 않은 인프라에서 더 이상 새 리소스를 생성할 수 없습니다.
- 공유 Exadata 인프라의 신뢰할 수 있는 계정에서 생성된 기존 리소스는 계속 작동하며 해당 AWS 계정에 계속 액세스할 수 있습니다.
- 신뢰할 수 있는 계정에서 생성한 VM 클러스터가 있는 Exadata 인프라는 해당 VM 클러스터가 제거될 때까지 삭제할 수 없습니다.

리소스를 공유 해제하기 전에 신뢰할 수 있는 계정과 조정하여 원활한 전환을 보장하는 것이 좋습니다.

자세한 내용은 AWS Resource Access Manager 사용 설명서의 AWS RAM에서 리소스 공유 업데이트 및 AWS RAM에서 리소스 공유 삭제를 참조하세요.

신뢰할 수 있는 계정에서 Oracle Database@AWS 초기화

신뢰할 수 있는 계정은 리소스 공유를 수신할 수 있는 것으로 지정한 AWS 계정입니다. AWS 조직의 다른 개인 AWS 계정이어야 합니다. 신뢰할 수 있는 계정에서 공유 Oracle Database@AWS 리소스를 사용하려면 먼저 서비스를 초기화해야 합니다. 초기화는 필요한 메타데이터를 생성하고 AWS 계정과 Oracle Cloud Infrastructure 간의 연결을 설정합니다.

주제

- Oracle Database@AWS 초기화란 무엇입니까?
- 다음 단계

Oracle Database@AWS 초기화란 무엇입니까?

리소스가 계정과 공유된 후에는 Oracle Database@AWS 서비스를 초기화해야 공유 리소스에 액세스하거나 사용할 수 있습니다. 서비스를 먼저 초기화하지 않고 Oracle Database@AWS API를 사용하려고 하면 오류가 발생합니다.

초기화는 일회성 프로세스입니다. 필요한 메타데이터를 생성하고 AWS 계정과 Oracle Cloud Infrastructure 간에 연결을 설정합니다.

AWS Management Console 또는 AWS CLI를 사용하여 서비스를 초기화할 수 있습니다.

콘솔

1. https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 이 계정의 Oracle Database@AWS 콘솔에 처음 액세스하는 경우 시작 페이지가 표시됩니다.
3. 계정 활성화를 선택합니다.
4. 서비스 초기화 프로세스가 시작됩니다. 이 프로세스를 완료하는 데 몇 분이 걸릴 수 있습니다.
5. 계정 활성화 버튼이 대시보드 버튼으로 변경될 때까지 시작 페이지를 주기적으로 새로 고칩니다.
6. 대시보드를 선택하여 Oracle Database@AWS 사용을 시작합니다.

AWS CLI

AWS CLI를 사용하여 신뢰할 수 있는 계정에서 Oracle Database@AWS를 초기화하려면 `initialize-service` 명령을 사용합니다.

```
aws odb initialize-service
```

초기화 상태를 확인하려면 `get-oci-onboarding-status` 명령을 사용합니다.

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

초기화가 완료되면 출력에 `ACTIVE_LIMITED` 상태가 표시되며, 이는 계정이 공유 리소스에 액세스할 수 있지만 새 Exadata 인프라 또는 ODB 네트워크를 생성할 수 없음을 나타냅니다.

다음 단계

신뢰할 수 있는 계정에서 Oracle Database@AWS를 초기화한 후 다음을 수행할 수 있습니다.

- `list` 및 `get` 명령을 사용하거나 AWS 콘솔에서 공유 리소스를 봅니다.
- 공유 Exadata 인프라 및 ODB 네트워크에서 VM 클러스터와 Autonomous VM 클러스터를 생성합니다.
- 공유 ODB 네트워크에서 ODB 피어링 연결을 생성합니다.

공유 리소스 작업에 대한 자세한 내용은 신뢰할 수 있는 계정의 공유 Oracle Database@AWS 리소스 작업 섹션을 참조하세요.

신뢰할 수 있는 계정의 공유 Oracle Database@AWS 리소스 작업

리소스가 신뢰할 수 있는 계정과 공유되고 Oracle Database@AWS 서비스를 초기화한 후에는 공유 리소스를 보고 사용할 수 있습니다. 이 주제에서는 신뢰할 수 있는 계정에서 공유 리소스를 사용하는 방법을 설명합니다.

주제

- 신뢰할 수 있는 계정의 공유 리소스에 대한 제한 사항
- 공유 Exadata 인프라에서 VM 클러스터 생성
- 신뢰할 수 있는 계정에서 공유 리소스 보기
- 공유 ODB 네트워크를 사용한 ODB 피어링 설정

신뢰할 수 있는 계정의 공유 리소스에 대한 제한 사항

공유 Oracle Database@AWS 리소스로 작업할 때는 다음 제한 사항에 유의하세요.

- 리소스 공유는 동일한 AWS 조직 내에서만 지원됩니다.
- 구매자 계정(Oracle Database@AWS 비공개 제안을 수락하는 계정)만 Exadata 인프라 및 ODB 네트워크 리소스를 생성할 수 있습니다.
- 공유 인프라에서 필요한 권한이 있는 경우에만 리소스를 생성할 수 있습니다.
- 각 리소스 유형에 대한 특정 작업(관리형 권한)은 리소스 공유 생성 중에 자동으로 선택되며 수정할 수 없습니다.
- 다른 계정이 소유한 리소스는 수정하거나 삭제할 수 없습니다.
- 공유 인프라에서 생성하는 리소스는 계정이 소유하며 OCI 할당량에 포함됩니다. 상위 리소스에도 동일하게 적용됩니다.
- 소유자 계정이 리소스를 공유 해제하면 더 이상이 공유 인프라에서 새 리소스를 생성할 수 없습니다. 그러나 기존 리소스는 계속 작동합니다.
- 크로스 리전 공유는 지원되지 않습니다. 동일한 AWS 리전 내에서만 리소스를 공유할 수 있습니다.
- 신뢰할 수 있는 계정 리소스는 Oracle Database@AWS 구독 구매자에게 청구됩니다.
- 공유된 리소스를 사용할 때는 Amazon 리소스 이름(ARN)을 제공해야 합니다.

공유 Exadata 인프라에서 VM 클러스터 생성

신뢰할 수 있는 계정이 공유 Exadata 인프라 및 ODB 네트워크에 액세스할 수 있는 경우 이 인프라에서 Exadata VM 클러스터, Autonomous VM 클러스터 또는 ODB 피어링을 생성할 수 있습니다.

> **Note**
>
> 공유된 리소스를 사용할 때는 리소스 ID만 지정하는 대신 Amazon 리소스 이름(ARN)을 지정해야 합니다.

콘솔

1. https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 탐색 창에서 Exadata VM 클러스터 또는 Autonomous VM 클러스터를 선택합니다.
3. VM 클러스터 생성 또는 Autonomous VM 클러스터 생성을 선택합니다.

4. Exadata 인프라에서 VM 클러스터를 생성할 공유 Exadata 인프라를 선택합니다.
5. VM 클러스터 구성에 필요한 나머지 필드를 작성합니다.
6. VM 클러스터 생성 또는 Autonomous VM 클러스터 생성을 선택합니다.

AWS CLI

AWS CLI를 사용하여 공유 Exadata 인프라에서 VM 클러스터를 생성하려면 `create-cloud-vm-cluster` 명령을 사용합니다.

```
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 CLI를 사용하여 공유 Exadata 인프라에서 Autonomous VM 클러스터를 생성하려면 `create-cloud-vm-cluster` 명령을 사용합니다.

```
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 클러스터는 지정된 공유 Exadata 인프라에서 생성되며 신뢰할 수 있는 계정이 소유합니다.

신뢰할 수 있는 계정에서 공유 리소스 보기

AWS 관리 콘솔 또는 AWS CLI를 사용하여 계정과 공유된 리소스를 볼 수 있습니다.

콘솔

1. https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.

2. 탐색 창에서 보려는 리소스 유형인 Exadata 인프라 또는 ODB 네트워크를 선택합니다.
3. 콘솔에 공유된 리소스가 표시됩니다.
4. 공유 리소스를 선택하면 세부 정보를 볼 수 있습니다.

AWS CLI

AWS CLI를 사용하여 공유 리소스를 보려면 리소스 유형에 적합한 `list` 명령을 사용합니다. 예를 들어 Exadata 인프라를 나열하려면:

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

응답에는 공유된 리소스가 표시됩니다.

특정 공유 리소스에 대한 자세한 정보를 가져오려면 리소스 ID와 함께 적절한 `get` 명령을 사용합니다.

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

공유 ODB 네트워크를 사용한 ODB 피어링 설정

공유 ODB 네트워크의 애플리케이션과 데이터베이스 간에 통신을 활성화하려면 VPC와 공유 ODB 네트워크 간에 ODB 피어링을 설정할 수 있습니다. ODB 피어링에 대한 자세한 내용은 Oracle Database@AWS에서 ODB 피어링 연결 생성 섹션을 참조하세요.

콘솔

1. https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 탐색 창에서 ODB 피어링을 선택합니다.
3. ODB 네트워크 피어링 생성을 선택합니다.
4. ODB 네트워크의 경우 피어링할 공유 ODB 네트워크를 선택합니다.
5. 피어 네트워크에서 VPC를 선택합니다.
6. ODB 네트워크 피어링 생성을 선택합니다.

AWS CLI

AWS CLI를 사용하여 VPC와 공유 ODB 네트워크 간에 네트워크 피어링 연결을 생성하려면 `create-odb-peering-connection` 명령을 사용합니다.

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

피어링 연결을 생성한 후 피어링된 네트워크 간의 트래픽을 활성화하도록 라우팅 테이블을 업데이트합니다.

```
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 관리

리소스를 생성한 후 일부 Oracle Database@AWS 리소스를 수정하고 삭제할 수 있습니다.

Oracle Database@AWS에서 ODB 네트워크 업데이트

다음 ODB 네트워크 리소스를 업데이트할 수 있습니다.

- ODB 네트워크 이름
- ODB 네트워크에 대한 ODB 피어링 연결을 설정하는 데 사용할 Amazon VPC
- ODB 네트워크의 Exadata 리소스에 액세스할 수 있는 VPC CIDR 범위

> **Note**
>
> CIDR 범위를 지정하면 전체 VPC를 ODB 네트워크에서 사용할 수 있도록 하는 대신 필요한 VPC 서브넷에 대한 연결을 제한할 수 있습니다.

이 섹션에서는 1단계: Oracle Database@AWS에서 ODB 네트워크 생성에서 ODB 네트워크를 이미 생성했다고 가정합니다.

ODB 네트워크를 업데이트하려면

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 왼쪽 창에서 ODB 네트워크를 선택합니다.
3. 수정할 네트워크를 선택합니다.
4. 수정을 선택합니다.
5. (선택 사항) ODB 네트워크 이름에 새 네트워크 이름을 입력합니다. 이름은 1~255자여야 하며 영문자 또는 밑줄로 시작해야 합니다. 연속된 하이픈은 포함될 수 없습니다.
6. (선택 사항) 피어링된 CIDR 경우 ODB 네트워크에 연결해야 하는 피어링된 VPC의 CIDR 범위를 지정합니다. 액세스를 제한하려면 필요한 최소 CIDR 범위를 지정하는 것이 좋습니다.
7. (선택 사항) 서비스 통합 구성에서 Amazon S3 또는 제로 ETL을 선택하거나 선택 취소합니다.
8. 계속을 선택하고 수정을 선택합니다.

Oracle Database@AWS에서 ODB 네트워크 삭제

ODB 네트워크를 삭제할 수 있습니다. 이 섹션에서는 1단계: Oracle Database@AWS에서 ODB 네트워크 생성에서 ODB 네트워크를 이미 생성했다고 가정합니다. 현재 VM 클러스터에서 사용 중인 ODB 네트워크는 삭제할 수 없습니다.

ODB 네트워크를 삭제하려면

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 왼쪽 창에서 ODB 네트워크를 선택합니다.
3. 삭제할 네트워크를 선택합니다.
4. 삭제를 선택합니다.
5. (선택 사항) 연결된 OCI 리소스 삭제를 선택하여 ODB 네트워크와 함께 생성된 OCI 리소스를 삭제합니다.
6. 텍스트 상자에 **`delete me`**을 입력합니다.
7. 삭제를 선택합니다.

Oracle Database@AWS에서 VM 클러스터 삭제

Exadata VM 클러스터 또는 Autonomous VM 클러스터를 삭제할 수 있습니다. 이 섹션에서는 3단계: Oracle Database@AWS에서 Exadata VM 클러스터 또는 Autonomous VM 클러스터 생성에서 VM 클러스터를 이미 생성했다고 가정합니다.

VM 클러스터를 삭제하려면

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 왼쪽 창에서 Exadata VM 클러스터 또는 Autonomous VM 클러스터를 선택합니다.
3. 삭제할 VM 클러스터를 선택합니다.
4. 삭제를 선택합니다.
5. 메시지가 표시되면 **`delete me`**를 입력한 후 삭제를 선택합니다.

Oracle Database@AWS에서 Oracle Exadata 인프라 삭제

Oracle Exadata 인프라를 삭제할 수 있습니다. 이 섹션에서는 2단계: Oracle Database@AWS에서 Oracle Exadata 인프라 생성에서 Oracle Exadata 인프라를 이미 생성했다고 가정합니다. 현재 VM 클러스터에서 사용 중인 Exadata 인프라는 삭제할 수 없습니다.

Oracle Exadata 인프라를 삭제하려면

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 왼쪽 창에서 Exadata 인프라를 선택합니다.
3. 삭제할 Exadata 인프라를 선택합니다.
4. 삭제를 선택합니다.
5. 메시지가 표시되면 **`delete me`**를 입력한 후 삭제를 선택합니다.

ODB 피어링 연결 삭제

ODB 피어링 연결이 더 이상 필요하지 않으면 삭제할 수 있습니다. ODB 네트워크를 삭제하려면 먼저 모든 ODB 피어링 연결을 삭제해야 합니다.

콘솔

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 탐색 창에서 ODB 피어링 연결을 선택합니다.
3. 삭제할 ODB 피어링 연결을 선택합니다.
4. 삭제를 선택합니다.
5. 삭제를 확인하려면 **`delete me`**를 입력하고 삭제를 선택합니다.

AWS CLI

ODB 피어링 연결을 삭제하려면 `delete-odb-peering-connection` 명령을 사용합니다.

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

Oracle Database@AWS에 백업

Oracle Database@AWS는 Oracle 데이터베이스를 보호하기 위한 여러 백업 옵션을 제공합니다. Amazon S3와 원활하게 통합되는 Oracle 관리형 백업을 사용하거나 Oracle Recovery Manager(RMAN)를 사용하여 자체 사용자 관리형 백업을 생성할 수 있습니다.

Amazon S3에 대한 Oracle 관리형 백업

ODB 네트워크를 생성하면 Oracle Database@AWS가 Amazon S3에 대한 Oracle 관리형 백업의 네트워크 액세스를 자동으로 구성합니다. OCI는 필요한 DNS 항목과 보안 목록을 구성합니다. 이러한 구성은 OCI Virtual Cloud Network(VCN)와 Amazon S3 간의 트래픽을 허용합니다. ODB 네트워크는 자동 백업을 활성화하거나 제어하지 않습니다.

Oracle 관리형 백업은 OCI에서 완벽하게 관리합니다. Oracle Exadata 데이터베이스를 생성할 때 OCI 콘솔에서 자동 백업 활성화를 선택하여 자동 백업을 활성화할 수 있습니다. 다음 중 하나의 백업 대상을 선택합니다.

- Amazon S3
- OCI 객체 스토리지
- Autonomous Recovery Service

자세한 내용은 OCI 설명서의 Exadata 데이터베이스 백업을 참조하세요.

Oracle Database@AWS의 Amazon S3에 대한 사용자 관리형 백업

Oracle Database@AWS를 사용하면 전용 인프라의 Exadata Database Service를 사용하여 데이터베이스의 사용자 관리형 백업을 생성할 수 있습니다. Oracle Recovery Manager(RMAN)를 사용하여 데이터를 백업하고 Amazon S3 버킷에 저장합니다. Oracle Database@AWS의 관리형 서비스 이점을 유지하면서 백업 예약, 보존 정책 및 스토리지 비용을 완벽하게 제어할 수 있습니다.

> **Note**
>
> Oracle Database@AWS는 전용 인프라의 Autonomous 데이터베이스에 대한 사용자 관리형 백업을 지원하지 않습니다.

사용자 관리형 백업은 Oracle Database@AWS에서 제공하는 AWS 관리형 백업 솔루션을 보완합니다. 규정 준수 요구 사항, 리전 간 재해 복구 또는 기존 백업 관리 워크플로와의 통합에 수동 백업을 사용할 수 있습니다.

다음과 같은 사용자 관리형 백업 기술을 사용할 수 있습니다.

Oracle 안전 백업

최적의 성능으로 Amazon S3로 직접 백업을 스트리밍합니다.

Storage Gateway

NFS 공유를 사용하는 파일 기반 백업에는 Storage Gateway를 사용합니다.

S3 탑재 지점

파일 클라이언트를 사용하여 Amazon S3 버킷을 로컬 파일 시스템으로 탑재합니다.

Oracle Database@AWS의 Amazon S3에 대한 사용자 관리형 백업을 위한 사전 조건

Oracle Exadata 데이터베이스를 Amazon S3에 백업하려면 먼저 다음을 수행합니다.

1. ODB 네트워크에서 Amazon S3에 대한 직접 액세스를 활성화합니다.
2. Oracle Database@AWS와 Amazon S3 간의 네트워크 연결 및 라우팅을 구성합니다.

ODB 네트워크에서 Amazon S3로의 액세스 활성화

데이터베이스를 Amazon S3에 수동으로 백업하려면 ODB 네트워크에서 S3에 대한 직접 액세스를 활성화합니다. 이 기술을 사용하면 데이터베이스가 데이터 가져오기/내보내기 또는 사용자 관리형 백업과 같은 비즈니스 요구 사항에 맞게 Amazon S3에 액세스할 수 있습니다. 백업 스토리지의 대상을 완전히 제어할 수 있으며 정책을 사용하여 VPC Lattice를 사용한 Amazon S3에 대한 액세스를 제한할 수 있습니다.

ODB 네트워크에서 Amazon S3에 대한 직접 액세스는 기본적으로 활성화되어 있지 않습니다. ODB 네트워크를 생성하거나 수정할 때 S3 액세스를 활성화할 수 있습니다.

콘솔

ODB 네트워크에서 Amazon S3에 대한 직접 액세스를 활성화하려면

1. https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 탐색 창에서 ODB 네트워크를 선택합니다.
3. Amazon S3 액세스를 활성화하려는 ODB 네트워크를 선택합니다.
4. 수정을 선택합니다.
5. Amazon S3를 선택합니다.
6. (선택 사항) Amazon S3에 대한 액세스를 제어하도록 Amazon S3 정책 문서를 구성합니다. 정책을 지정하지 않으면 기본 정책에서 전체 액세스 권한을 부여합니다.
7. 계속을 선택하고 수정을 선택합니다.

AWS CLI

ODB 네트워크에서 직접 Amazon S3 액세스를 활성화하려면 `s3-access` 파라미터와 함께 `update-odb-network` 명령을 사용합니다.

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

Amazon S3 정책 문서를 구성하려면 `--s3-policy-document` 파라미터를 사용합니다.

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

Amazon S3 액세스가 활성화되면 리전 DNS `s3.region.amazonaws.com`을 사용하여 ODB 네트워크에서 Amazon S3에 액세스할 수 있습니다. OCI는 기본적으로 이 DNS 이름을 구성합니다. 사용자 지정 DNS 이름을 사용하려면 사용자 지정 DNS가 서비스 네트워크 엔드포인트의 IP 주소로 확인되도록 VCN DNS를 수정합니다.

Oracle Database@AWS와 Amazon S3 간의 네트워크 연결 구성

Amazon S3에 대한 사용자 관리형 백업을 허용하려면 VM이 S3 Amazon VPC 엔드포인트에 액세스할 수 있어야 합니다. OCI 콘솔에서 네트워크 보안 그룹(NSG)의 보안 규칙을 편집하여 수신 및 송신 트래픽을 제어할 수 있습니다. 사용자 관리형 백업의 경우 트래픽은 백업 서브넷이 아닌 클라이언트 서브넷

을 통해 흐릅니다. 다음 단계에서는 클라이언트 서브넷의 NSG를 업데이트하여 VPC 엔드포인트 IP 주소에 대한 송신 규칙을 추가합니다.

Amazon S3 엔드포인트에 대한 VM 액세스를 허용하려면

1. https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. ODB 네트워크를 선택합니다.
3. ODB 네트워크의 이름을 선택합니다.
4. OCI 리소스를 선택합니다.
5. 서비스 통합 탭을 선택합니다.
6. Amazon S3에서 다음 정보를 기록해 둡니다.
   - Amazon VPC S3 엔드포인트의 IPv4 주소입니다. 나중에 이 정보가 필요합니다. 예를 들어 IP 주소는 `192.168.12.223`일 수 있습니다.
   - Amazon VPC S3 엔드포인트의 도메인 이름입니다. 나중에 이 정보가 필요합니다. 예를 들어, 도메인 이름은 `s3.us-east-1.amazonaws.com`일 수 있습니다.
7. 왼쪽 탐색 창에서 Exadata VM 클러스터를 선택하고 VM 클러스터 이름을 선택합니다.
8. 페이지 상단에서 요약 탭을 선택합니다.
9. 가상 머신을 선택한 다음 VM의 이름을 선택합니다.
10. DNS 이름의 값을 기록해 둡니다. `ssh`를 사용하여 VM에 연결할 때 지정하는 호스트 이름입니다.
11. 오른쪽 상단에서 OCI에서 관리를 선택합니다. OCI 콘솔이 열립니다.
12. 가상 클라우드 네트워크 목록 페이지에서 ODB 네트워크 클라이언트 서브넷(`exa_static_nsg`)의 네트워크 보안 그룹(NSG)이 포함된 VCN을 선택합니다. 자세한 내용은 OCI 설명서의 NSG에 대한 보안 규칙 관리를 참조하세요.
13. 세부 정보 페이지에서 표시되는 옵션에 따라 다음 작업 중 하나를 수행합니다.
    - 보안 탭에서 네트워크 보안 그룹으로 이동합니다.
    - 리소스에서 네트워크 보안 그룹을 선택합니다.
14. 클라이언트 서브넷(`exa_static_nsg`)의 NSG를 선택합니다.
15. 앞서 기록한 VPC 엔드포인트 주소에 대한 송신 규칙을 추가합니다.

VM에서 S3에 대한 연결을 테스트하려면

1. `ssh`를 사용하여 이전에 DNS 이름을 얻은 VM에 `root`로 연결합니다. 연결할 때 SSH 키를 사용하여 `.pem` 파일을 지정합니다.

2. 다음 명령을 실행하여 VM이 Amazon S3 Amazon VPC 엔드포인트에 액세스할 수 있는지 확인합니다. 이전에 적어 둔 S3 도메인 이름을 사용합니다.

```
# 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 Backup을 사용하여 Amazon S3에 백업

Oracle Secure Backup은 Recovery Manager(RMAN)와 함께 사용할 수 있는 SBT 인터페이스 역할을 합니다. RMAN을 Oracle Secure Backup과 함께 사용하여 Oracle Database@AWS 데이터베이스를 Amazon S3에 직접 백업할 수 있습니다. Oracle Secure Backup은 다음과 같은 이점을 제공합니다.

- Oracle Secure Backup은 RMAN과 S3 간의 데이터 전송을 최적화합니다.
- 중간 백업 스토리지는 필요하지 않습니다.
- Oracle Secure Backup은 백업 미디어의 수명 주기를 관리합니다.

Oracle Secure Backup을 사용하여 Amazon S3에 백업하려면

1. Exadata VM 서버에 Oracle Secure Backup 모듈을 설치합니다. 자리 표시자 값을 AWS 액세스 키 및 시크릿 액세스 키로 바꿉니다. 자세한 내용은 Oracle Secure Backup Cloud Module을 사용하여 클라우드로 백업의 Oracle 설명서를 참조하세요.

```
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. RMAN에 연결하고 백업 채널과 기본 디바이스 유형을 구성합니다.

```
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. 구성을 확인합니다.

```
RMAN> SHOW ALL;
```

4. 데이터베이스를 백업합니다.

```
RMAN> BACKUP DATABASE;
```

5. 백업이 성공적으로 완료되었는지 확인합니다.

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

Amazon EC2에서 AWS Storage Gateway를 사용하여 Amazon S3에 백업

AWS Storage Gateway는 온프레미스 환경을 AWS 클라우드 스토리지 서비스에 연결하는 하이브리드 서비스입니다. Oracle Database@AWS 백업의 경우 Storage Gateway를 사용하여 Amazon S3에 직접 쓰는 파일 기반 백업 워크플로를 생성할 수 있습니다. Oracle Secure Backup 기술과 달리 백업의 수명 주기를 관리합니다.

이 솔루션에서는 Storage Gateway를 구성하기 위한 별도의 Amazon EC2 인스턴스를 생성합니다. 또한 Amazon EBS 볼륨을 추가하여 Amazon S3에 읽기 및 쓰기를 캐싱합니다.

이 기법은 다음과 같은 이점이 있습니다.

- Oracle Secure Backup과 같은 미디어 관리자는 필요하지 않습니다.
- 중간 백업 스토리지는 필요하지 않습니다.

Storage Gateway를 배포하고 파일 공유를 생성하려면

1. AWS Management Console(https://console.aws.amazon.com/storagegateway/home/)을 열고 게이트웨이를 생성할 AWS 리전을 선택합니다.
2. Amazon EC2 인스턴스를 허브로 사용하여 Amazon S3 파일 게이트웨이를 배포하고 활성화합니다. Storage Gateway 사용 설명서에 있는 S3 File Gateway용 사용자 지정 Amazon EC2 호스트 배포의 지침을 따릅니다.

   파일 게이트웨이를 구성할 때 다음을 수행해야 합니다.

   - 캐시 스토리지용으로 크기가 150GiB 이상인 Amazon EBS 볼륨을 하나 이상 추가합니다.

- 보안 그룹의 NFS 액세스를 위해 TCP/UDP 포트 2049를 엽니다. 이렇게 하면 NFS 파일 공유를 생성할 수 있습니다.
- 게이트웨이 활성화 중에 일회성 HTTP 액세스를 허용하기 위해 수신 트래픽에 대해 TCP 포트 80을 엽니다. 활성화한 후에는 이 포트를 닫을 수 있습니다.

3. ODB 네트워크와 Storage Gateway 간의 프라이빗 연결을 위한 Amazon VPC 엔드포인트를 생성합니다. 자세한 내용은 인터페이스 VPC 엔드포인트를 사용하여 AWS 서비스에 액세스를 참조하세요.
4. Storage Gateway 콘솔을 통해 Amazon S3 버킷에 대한 파일 공유를 생성합니다. 자세한 내용은 파일 공유 생성을 참조하세요.

Storage Gateway를 사용하여 데이터베이스를 Amazon S3에 백업하려면

1. 터미널에서 ssh를 사용하여 Exadata VM의 DNS 이름에 연결합니다. DNS 이름을 찾으려면 Oracle Database@AWS의 Amazon S3에 대한 사용자 관리형 백업을 위한 사전 조건 섹션을 참조하세요.
2. NFS 탑재를 위해 Exadata VM 클러스터 서버에 디렉터리를 생성합니다. 다음 예에서는 /home/oracle/sgw_mount/ 디렉터리를 생성합니다.

```
mkdir /home/oracle/sgw_mount/
```

3. 방금 생성한 디렉터리에 NFS 공유를 탑재합니다. 다음 예제에서는 /home/oracle/sgw_mount/ 디렉터리에 공유를 생성합니다. *SG-IP-address*를 Storage Gateway IP 주소로 바꾸고 *your-bucket-name*을 S3 버킷 이름으로 바꿉니다.

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

4. RMAN에 연결하고 데이터베이스를 탑재된 디렉터리에 백업합니다. 다음 예제에서는 rman_local_bkp 채널을 생성하고 탑재 지점 경로를 사용하여 백업 조각의 형식을 지정합니다.

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

5. 탑재 디렉터리에 백업 파일이 생성되었는지 확인합니다. 다음 예제에서는 두 개의 백업 조각을 보여줍니다.

```
$ 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 탑재 지점을 사용하여 Amazon S3에 백업

Amazon S3 탑재 지점을 사용하여 먼저 로컬에서 백업을 생성한 다음 Amazon S3에 복사할 수 있습니다. 이 기법은 로컬 스토리지에 백업을 생성한 다음 탑재 지점 인터페이스를 사용하여 Amazon S3로 전송합니다. 데이터를 두 번 백업해야 하므로 백업 시간이 다른 기법보다 깁니다.

> **Note**
>
> 스테이징 없이 탑재 지점을 사용하여 Amazon S3로 직접 백업하는 것은 지원되지 않습니다. RMAN에는 Amazon S3 탑재 지점 인터페이스와 호환되지 않는 특정 파일 시스템 권한이 필요합니다.

이 기법은 Oracle Secure Backup과 같은 미디어 관리자에 라이선스를 부여할 필요가 없습니다. 백업의 수명 주기를 관리합니다.

S3 탑재 지점을 사용하여 Amazon S3에 백업하려면

1. 터미널에서 `ssh`를 사용하여 Exadata VM의 DNS 이름에 연결합니다. DNS 이름을 찾으려면 Oracle Database@AWS의 Amazon S3에 대한 사용자 관리형 백업을 위한 사전 조건 섹션을 참조하세요.
2. Exadata VM 클러스터 서버에 Amazon S3 탑재 지점을 설치합니다. 설치 및 구성에 대한 자세한 내용은 Amazon S3 사용 설명서의 Mountpoint for Amazon S3를 참조하세요.

   ```
   $ sudo yum install ./mount-s3.rpm
   ```
3. 명령에서 `mount-s3`를 실행하여 설치를 확인합니다.

   ```
   $ mount-s3 --version
   mount-s3 1.19.0
   ```
4. Exadata VM 클러스터 서버 로컬 스토리지에 중간 백업 디렉터리를 생성합니다. 데이터베이스를 이 로컬 디렉터리에 백업한 다음 백업을 S3 버킷에 복사합니다. 다음 예에서는 `/u02/rman_bkp_local` 디렉터리를 생성합니다.

```
mkdir /u02/rman_bkp_local
```

5. Amazon S3 탑재 지점에 대한 디렉터리를 생성합니다. 다음 예에서는 /home/oracle/s3mount 디렉터리를 생성합니다.

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

6. 탑재 지점을 사용하여 Amazon S3 버킷을 탑재합니다. 다음 예제에서는 /home/oracle/s3mount 디렉터리에 S3 버킷을 탑재합니다. *your-s3-bucket-name*을 Amazon S3 버킷 이름으로 바꿉니다.

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

7. Amazon S3 버킷 콘텐츠에 액세스할 수 있는지 확인합니다.

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

8. RMAN을 대상 데이터베이스에 연결하고 로컬 스테이징 디렉터리에 백업합니다. 다음 예제에서는 rman_local_bkp 채널을 생성하고 /u02/rman_bkp_local/ 경로를 사용하여 백업 조각의 형식을 지정합니다.

```
$ rman TARGET /

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

9. 백업이 로컬 디렉터리에 생성되었는지 확인합니다.

```
$ 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. 로컬 스테이징 디렉터리에서 Amazon S3 탑재 지점으로 백업 파일을 복사합니다.

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

11. 파일을 Amazon S3에 성공적으로 복사했는지 확인합니다.

```
$ 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 S3에 대한 직접 액세스 비활성화

ODB 네트워크에서 Amazon S3에 더 이상 직접 액세스할 필요가 없는 경우 비활성화할 수 있습니다. S3에 대한 직접 네트워크 액세스를 활성화하거나 비활성화해도 Amazon S3에 대한 Oracle 관리형 백업에 대한 네트워크 액세스에는 영향을 주지 않습니다.

콘솔

Amazon S3에 대한 직접 액세스를 비활성화하려면

1. https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 탐색 창에서 ODB 네트워크를 선택합니다.
3. Amazon S3 액세스를 비활성화하려는 ODB 네트워크를 선택합니다.
4. 수정을 선택합니다.
5. S3 액세스 활성화 확인란의 선택을 취소합니다.
6. ODB 네트워크 수정을 선택합니다.

AWS CLI

`s3-access` 파라미터와 함께 `update-odb-network` 명령을 사용합니다.

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

Amazon S3 통합 문제 해결

Amazon S3에 대한 Oracle 관리형 백업 또는 Amazon S3에 대한 직접 액세스에 문제가 발생하는 경우 다음 문제 해결 단계를 고려하세요.

데이터베이스에서 Amazon S3에 액세스할 수 없음

다음을 확인하세요.

- ODB 네트워크에 대해 Amazon S3 액세스가 활성화되어 있는지 확인합니다. `GetOdbNetwork` 작업을 사용하여 `s3Access` 상태가 `Enabled`인지 확인합니다.
- 올바른 리전 DNS 이름인 `s3.region.amazonaws.com`을 사용하고 있는지 확인합니다.
- Oracle 데이터베이스에 Amazon S3에 액세스하는 데 필요한 권한이 있는지 확인합니다.

Oracle 관리형 백업 실패

다음을 확인하세요.

- Amazon S3에 대한 Oracle 관리형 백업은 기본적으로 활성화되어 있으며 비활성화할 수 없습니다. 백업이 실패하는 경우 Oracle 데이터베이스 로그에서 특정 오류 메시지를 확인합니다.
- 서비스 통합 리소스를 확인하여 Amazon VPC Lattice 리소스가 제대로 구성되어 있는지 확인합니다.
- Oracle 관리형 자동 백업 문제에 대한 지원은 Oracle Support에 문의하십시오. 자세한 내용은 Oracle Database@AWS에 대한 지원 받기 섹션을 참조하세요.

Amazon Redshift와 Oracle Database@AWS 제로 ETL 통합

제로 ETL 통합은 Amazon Redshift에서 여러 소스의 트랜잭션 및 운영 데이터를 사용할 수 있도록 하는 완전 관리형 솔루션입니다. 이 솔루션을 사용하면 Oracle Exadata에서 실행되는 Oracle 데이터베이스 또는 전용 Exadata 인프라의 Autonomous 데이터베이스에서 Amazon Redshift로 데이터를 복제할 수 있습니다. 자동 동기화는 기존 추출, 전환, 적재(ETL) 프로세스를 방지합니다. 또한 실시간 분석 및 AI 워크로드를 지원합니다. 자세한 내용은 Amazon Redshift 관리 안내서의 제로 ETL 통합을 참조하세요.

제로 ETL 통합은 다음을 제공합니다.

- 실시간 데이터 복제 - 지연 시간을 최소화하면서 Oracle 데이터베이스에서 Amazon Redshift로의 지속적인 데이터 동기화
- 복잡한 ETL 파이프라인 제거 - 사용자 지정 데이터 통합 솔루션을 구축하고 유지 관리할 필요가 없음
- 운영 오버헤드 감소 - AWS API를 통한 자동 설정 및 관리
- 간소화된 데이터 통합 아키텍처 - Oracle Database@AWS와 AWS 분석 서비스 간의 원활한 통합
- 보안 강화 - 기본 제공 암호화 및 AWS IAM 액세스 제어

Amazon Redshift는 Oracle Database@AWS와의 제로 ETL 통합에 대해 추가 요금을 부과하지 않습니다. 제로 ETL 통합의 일부로 생성된 변경 데이터를 생성하고 처리하는 데 사용되는 기존 Amazon Redshift 리소스에 대해 요금이 청구됩니다. 자세한 내용은 Amazon Redshift 요금을 참조하세요.

Oracle Database@AWS에서 제로 ETL 통합을 지원하는 데이터베이스 버전

제로 ETL 통합은 다음 Oracle 데이터베이스 버전을 지원합니다.

- Oracle Exadata – Oracle Database 19c
- 전용 인프라의 Autonomous 데이터베이스 - Oracle Database 19c 및 23ai

Oracle Database@AWS에서 제로 ETL 통합이 작동하는 방식

제로 ETL 통합을 통해 Oracle Database@AWS는 Amazon Redshift에 데이터를 복제할 수 있습니다. 통합에서는 Amazon VPC Lattice를 활용하여 보안 네트워크 연결을 생성합니다. 변경 데이터 캡처(CDC) 기술은 실시간 데이터 동기화를 보장합니다. AWS Glue API를 통해 통합을 관리합니다.

제로 ETL 통합 아키텍처에는 다음이 포함됩니다.

- 보안 연결 - 데이터 전송을 위해 TLS 포트 2484를 통한 SSL/TLS 암호화 사용
- AWS Secrets Manager - AWS Key Management Service를 사용하여 데이터베이스 자격 증명 및 인증서를 안전하게 저장
- AWS Glue 통합 - 제로 ETL 통합을 위한 통합 관리 인터페이스 제공

복제는 다음 단계를 진행합니다.

1. 포트 2484에서 SSL을 사용하여 Oracle 데이터베이스에 대한 보안 연결 설정
2. 선택한 데이터베이스, 스키마 및 테이블의 초기 전체 덤프 수행
3. 지속적인 실시간 복제를 위한 변경 데이터 캡처(CDC) 설정
4. 복제된 데이터를 대상 Amazon Redshift 클러스터에 쓰기

> **Important**
>
> 제로 ETL 통합은 기본적으로 활성화되어 있지 않습니다. AWS Glue API를 사용하여 구성해야 합니다. Oracle Database@AWS API를 사용하여 제로 ETL 통합을 직접 설정할 수 없습니다.

Oracle Database@AWS에서 제로 ETL 통합을 위한 사전 조건

제로 ETL 통합을 설정하기 전에 다음 사전 조건을 충족하는지 확인합니다.

일반적인 사전 요구 사항

- Oracle Database@AWS 설정 - 프로비저닝되고 실행 중인 VM 클러스터가 하나 이상 있는지 확인합니다.
- 제로 ETL이 활성화된 통합 - VM 클러스터 또는 Autonomous VM 클러스터가 제로 ETL이 활성화된 ODB 네트워크와 연결되어 있는지 확인합니다.

- 지원되는 Oracle 데이터베이스 버전 - Oracle Database 19c(Oracle Exadata) 또는 Oracle Database 19c/23ai(전용 인프라의 Autonomous 데이터베이스)를 사용해야 합니다.
- 동일한 AWS 리전 - 소스 Oracle 데이터베이스와 대상 Amazon Redshift 클러스터가 동일한 AWS 리전에 있어야 합니다.

Oracle 데이터베이스 사전 조건

다음 설정으로 Oracle 데이터베이스를 구성할 수 있습니다.

복제 사용자 설정

복제하려는 각 플러그형 데이터베이스(PDB)에 전용 복제 사용자를 생성합니다.

- Oracle Exadata의 경우 - 보안 암호로 `ODBZEROETLADMIN` 사용자를 생성합니다.
- 전용 인프라의 Autonomous 데이터베이스의 경우 - 기존 `GGADMIN` 사용자를 사용합니다.

복제 사용자에게 다음 권한을 부여합니다.

```
-- 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";
```

보충 로깅

Oracle 데이터베이스에서 보충 로깅을 활성화하여 변경 데이터를 캡처합니다.

```
-- 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@AWS와 Amazon Redshift 간에 제로 ETL 통합을 설정하려면 SSL을 구성해야 합니다.

Oracle Exadata 데이터베이스의 경우

포트 2484에서 SSL을 수동으로 구성해야 합니다. 이 작업에는 다음이 포함됩니다.

- `listener.ora`에서 `(PROTOCOL=tcps)(PORT=2484)` 구성
- `sqlnet.ora`를 사용하여 Wallet 설정
- SSL 인증서 생성 및 구성(My Oracle Support 설명서의 Exadata Cloud Database(ExaCC/ExaCS)용 SSL/TCPS 구성 방법(문서 ID 2947301.1) 참조)

Autonomous 데이터베이스의 경우

포트 2484의 SSL은 기본적으로 활성화됩니다. 추가 구성은 필요하지 않습니다.

> **Important**
>
> SSL 포트는 2484로 고정됩니다.

AWS 서비스 사전 조건

제로 ETL 통합을 설정하기 전에 AWS Secrets Manager를 설정하고 IAM 권한을 구성합니다.

AWS Secrets Manager 설정

다음과 같이 AWS Secrets Manager에 Oracle 데이터베이스 자격 증명을 저장합니다.

1. AWS Key Management Service에서 고객 관리형 키(CMK)를 생성합니다.
2. CMK를 사용하여 AWS Secrets Manager에 데이터터베이스 자격 증명을 저장합니다.
3. Oracle Database@AWS 액세스를 허용하도록 리소스 정책을 구성합니다.

TDE 키 ID와 암호를 가져오려면 Oracle을 AWS Database Migration Service의 소스로 사용하기 위해 지원되는 암호화 방법에 설명된 기술을 사용합니다. 다음 명령은 base64 wallet을 생성합니다.

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

다음 예제에서는 Oracle Exadata의 보안 암호를 보여줍니다. *asm_service_name*의 경우 *111.11.11.11*은 VM 노드의 가상 IP를 나타냅니다. ASM 리스너를 SCAN에 등록할 수도 있습니다.

```
{
  "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"
  }
}
```

다음 예제에서는 전용 인프라의 Autonomous 데이터베이스에 대한 보안 암호를 보여줍니다.

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

```
      "certificateWallet": "base64_encoded_wallet_content"
    }
  ]
}
```

IAM 권한 구성

제로 ETL 통합 작업을 허용하는 IAM 정책을 생성합니다. 다음 예제 정책은 Exadata VM 클러스터에 대한 설명, 생성, 업데이트 및 삭제 작업을 허용합니다. Autonomous VM 클러스터의 경우 리소스 ARN에 대해 `cloud-vm-cluster` 대신 `cloud-autonomous-vm-cluster` 값을 사용합니다.

Oracle Database@AWS의 제로 ETL 통합 고려 사항

Oracle Database@AWS와 Amazon Redshift 간의 제로 ETL 통합을 설정할 때는 다음 지침을 고려하세요.

초기 데이터 로드 시간

초기 전체 로드 시간은 데이터베이스 크기에 따라 달라집니다. 대규모 데이터베이스는 초기 동기화를 완료하는 데 몇 시간 또는 며칠이 걸릴 수 있습니다.

Oracle 데이터베이스 성능

변경 데이터 캡처는 특히 트랜잭션 볼륨이 많은 경우 Oracle 데이터베이스 성능에 영향을 미칠 수 있습니다. 제로 ETL 통합을 활성화한 후 데이터베이스 성능을 모니터링합니다.

스키마 변경

소스 Oracle 데이터베이스의 데이터 정의 언어(DDL)를 변경하려면 수동으로 개입하여 통합을 다시 생성해야 할 수 있습니다. 스키마 변경 사항을 신중하게 계획합니다.

일반적인 고려 사항은 Amazon Redshift와 제로 ETL 통합을 사용할 때 고려할 사항을 참조하세요.

Oracle Database@AWS의 제로 ETL 통합에 대한 제한 사항

다음과 같은 일반적인 제한 사항에 유의하세요.

통합당 단일 PDB

각 제로 ETL 통합은 하나의 플러그형 데이터베이스(PDB)에서만 데이터를 복제할 수 있습니다. `include: pdb1.*.*, include: pdb2.*.*`와 같은 데이터 필터는 지원되지 않습니다.

Autonomous 데이터베이스 또는 Exadata 인프라당 단일 통합

각 제로 ETL 통합은 전용 인프라의 단일 Autonomous 데이터베이스에서만 데이터를 복제할 수 있습니다.

고정 SSL 포트

SSL 연결은 포트 2484를 사용해야 합니다.

동일한 리전 요구 사항

소스 Oracle Database@AWS VM 클러스터와 대상 Amazon Redshift 클러스터는 동일한 AWS 리전에 있어야 합니다. 교차 리전 복제는 지원되지 않습니다.

mTLS 지원 없음

상호 TLS(mTLS)는 지원되지 않습니다. OCI 데이터베이스에 mTLS가 활성화된 경우 제로 ETL 통합을 사용하도록 비활성화해야 합니다.

변경할 수 없는 통합 설정

통합과 연결된 보안 암호 ARN 또는 KMS 키를 생성한 후에는 수정할 수 없습니다. 이러한 설정을 변경하려면 통합을 삭제하고 다시 생성해야 합니다.

TDE 열 수준 암호화

Oracle Exadata 데이터베이스에서는 열 수준 투명한 데이터 암호화(TDE)가 지원되지 않습니다. 테이블스페이스 수준 TDE만 지원됩니다.

데이터 형식 지원

일부 Oracle 관련 데이터 형식은 완전히 지원되지 않거나 복제 중에 변환이 필요할 수 있습니다. 데이터베이스를 프로덕션에 배포하기 전에 특정 데이터 유형을 철저히 테스트합니다.

Amazon Redshift와 Oracle Database@AWS 통합 설정

Oracle 데이터베이스와 Amazon Redshift 간에 제로 ETL 통합을 설정하려면 다음 단계를 완료하세요.

1. ODB 네트워크에서 제로 ETL을 활성화합니다.
2. Oracle 데이터베이스 사전 조건을 구성합니다.
3. AWS Secrets Manager 및 AWS Key Management Service를 설정합니다.
4. IAM 권한을 구성합니다.
5. Amazon Redshift 리소스 정책을 설정합니다.

6. 제로 ETL 통합을 생성합니다.
7. Amazon Redshift에서 대상 테이블을 생성합니다.

1단계: ODB 네트워크에 대한 제로 ETL 활성화

소스 VM 클러스터와 연결된 ODB 네트워크에 대해 제로 ETL 통합을 활성화할 수 있습니다. 기본적으로는 이 통합이 비활성화되어 있습니다.

콘솔

제로 ETL 통합을 활성화하려면

1. https://console.aws.amazon.com/odb/에서 Oracle Database@AWS 콘솔을 엽니다.
2. 탐색 창에서 ODB 네트워크를 선택합니다.
3. 제로 ETL 통합을 활성화하려는 ODB 네트워크를 선택합니다.
4. 수정을 선택합니다.
5. 제로 ETL을 선택합니다.
6. 계속을 선택하고 수정을 선택합니다.

AWS CLI

제로 ETL 통합을 활성화하려면 `--zero-etl-access` 파라미터와 함께 `update-odb-network` 명령을 사용합니다.

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

소스 VM 클러스터와 연결된 ODB 네트워크에 대해 제로 ETL 통합을 활성화하려면 `update-odb-network` 명령을 사용합니다. 이 명령은 제로 ETL 통합에 필요한 네트워크 인프라를 구성합니다.

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

2단계: Oracle 데이터베이스 구성

사전 조건에 설명된 대로 Oracle 데이터베이스 구성을 완료합니다.

- 복제 사용자를 생성하고 필요한 권한을 부여합니다.
- 보관된 다시 실행 로그를 활성화합니다.
- SSL을 구성합니다(Oracle Exadata만 해당).
- 해당하는 경우 ASM 사용자를 설정합니다(Oracle Exadata만 해당).

3단계: AWS Secrets Manager 및 AWS Key Management Service 설정

고객 관리형 키(CMK)를 생성하고 데이터베이스 자격 증명을 저장합니다.

1. `create-key` 명령을 사용하여 AWS Key Management Service에서 CMK를 생성합니다.

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

2. AWS Secrets Manager에 데이터베이스 자격 증명을 저장합니다.

```
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. 보안 암호에 리소스 정책을 연결하여 Oracle Database@AWS 액세스를 허용합니다.

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

앞의 명령에서 `secret-resource-policy.json`에는 다음 JSON이 포함되어 있습니다.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": "zetl.odb.amazonaws.com"
      },
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": "*"
    }
  ]
}
```

4. CMK에 리소스 정책을 연결합니다. CMK 리소스 정책에는 암호화된 제로 ETL 통합을 지원하기 위해 Oracle Database@AWS 서비스 위탁자와 Amazon Redshift 서비스 위탁자 모두에 대한 권한이 포함되어야 합니다.

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

`cmk-resource-policy.json` 파일에는 다음 정책 문이 포함되어야 합니다. 첫 번째 문은 Oracle Database@AWS 서비스 액세스를 허용하고 두 번째 문은 Amazon Redshift가 암호화된 데이터 작업을 위해 KMS 키에 대한 권한 부여를 생성하도록 허용합니다.

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"
          ]
        }
      }
    }
  ]
}
```

4단계: IAM 권한 구성

제로 ETL 통합 작업을 허용하는 IAM 정책을 생성하고 연결합니다.

```
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
```

다음 정책은 필요한 권한을 부여합니다.

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": "*"
    }
  ]
}
```

5단계: Amazon Redshift 리소스 정책 구성

Amazon Redshift 클러스터에 리소스 정책을 설정하여 인바운드 통합을 승인합니다.

```
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**
>
> 또는 AWS 콘솔에서 나를 위해 수정 옵션을 사용할 수 있습니다. 이 옵션은 수동으로 수행할 필요 없이 필요한 Amazon Redshift 정책을 자동으로 구성합니다.

6단계: AWS Glue를 사용하여 제로 ETL 통합 생성

AWS Glue `create-integration` 명령을 사용하여 제로 ETL 통합을 생성합니다. 이 명령에서는 소스 VM 클러스터와 대상 Amazon Redshift 네임스페이스를 지정합니다.

다음 예제에서는 Exadata VM 클러스터에서 실행되고 있는 pdb1이라는 PDB와의 통합을 생성합니다. 소스 ARN에서 `cloud-vm-cluster`를 `cloud-autonomous-vm-cluster`로 대체하여 Autonomous VM 클러스터를 생성할 수도 있습니다. KMS 키 지정은 선택 사항입니다. 키를 지정하면 3단계: AWS Secrets Manager 및 AWS Key Management Service 설정에서 생성한 키와 다를 수 있습니다.

```
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"
```

명령은 통합 ARN을 반환하고 상태를 creating으로 설정합니다. describe-integrations 명령을 사용하여 통합 상태를 모니터링할 수 있습니다.

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

> **Important**
>
> 통합당 하나의 PDB만 지원됩니다. 데이터 필터는 include: pdb1.*.*와 같은 단일 PDB를 지정해야 합니다. 소스는 통합이 생성되는 동일한 AWS 리전 및 계정에 있어야 합니다.

7단계: Amazon Redshift에서 대상 데이터베이스 생성

통합이 활성화되면 Amazon Redshift 클러스터에 대상 데이터베이스를 생성합니다.

```
-- 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";
```

대상 데이터베이스를 생성한 후 복제된 데이터를 쿼리할 수 있습니다.

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

-- Connect to the new database
\c target_database_name

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

제로 ETL 통합 확인

AWS Glue에서 통합 상태를 쿼리하고 Oracle 변경 사항이 Amazon Redshift에 복제되고 있는지 확인하여 통합이 작동하는지 확인합니다.

제로 ETL 통합이 올바르게 작동하는지 확인하려면

1. 통합 상태를 확인합니다.

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

   상태는 ACTIVE 또는 REPLICATING이어야 합니다.

2. Oracle 데이터베이스를 변경하고 Amazon Redshift에 표시되는지 확인하여 데이터 복제를 확인합니다.
3. Amazon CloudWatch에서 복제 지표를 모니터링합니다(사용 가능한 경우).

Oracle Database@AWS에서 제로 ETL 통합의 데이터 필터링

Oracle Database@AWS 제로 ETL 통합에서는 데이터 필터링을 지원합니다. 이를 사용하여 소스 Oracle Exadata 데이터베이스가 대상 데이터 웨어하우스에 복제하는 데이터를 제어할 수 있습니다. 전체 데이터베이스를 복제하는 대신 하나 이상의 필터를 적용하여 특정 테이블을 선택적으로 포함하거나 제외할 수 있습니다. 이렇게 하면 관련 데이터만 전송되도록 하여 스토리지 및 쿼리 성능을 최적화할 수 있습니다. 필터링은 데이터베이스 및 테이블 수준으로 제한됩니다. 열 수준 및 행 수준 필터링은 지원되지 않습니다.

Oracle Database와 Amazon Redshift는 객체 이름 대소문자를 다르게 처리하여 데이터 필터 구성과 대상 쿼리 모두에 영향을 줍니다. 다음 사항에 유의하세요.

- Oracle Database는 CREATE 문에 명시적으로 인용되지 않는 한 데이터베이스, 스키마 및 객체 이름을 대문자로 저장합니다. 예를 들어 mytable(따옴표 없음)을 생성하면 Oracle 데이터 사전은 테이블 이름을 MYTABLE로 저장합니다. 객체 생성 문에서 객체 이름을 따옴표로 묶으면 Oracle 데이터 사전은 대소문자를 유지합니다.
- 제로 ETL 데이터 필터는 대/소문자를 구분하며 Oracle 데이터 사전에 표시된 객체 이름의 정확한 대/소문자와 일치해야 합니다. 예를 들어 Oracle 사전이 스키마와 테이블 이름 REINVENT.MYTABLE을 저장하는 경우 include: ORCL.REINVENT.MYTABLE을 사용하여 필터를 생성합니다.

- Amazon Redshift 쿼리는 명시적으로 인용되지 않는 한 기본적으로 소문자 객체 이름으로 설정됩니다. 예를 들어 MYTABLE(따옴표 없음)의 쿼리는 mytable을 검색합니다.

Amazon Redshift 필터를 생성하고 데이터를 쿼리할 때의 사례 차이점에 유의하세요. Oracle Database@AWS에 대한 필터링 고려 사항은 Amazon RDS for Oracle과 동일합니다. Oracle 데이터베이스에서 대소문자가 데이터 필터에 어떤 영향을 미치는 지에 대한 예는 Amazon Relational Database Service 사용 설명서의 RDS for Oracle 예제를 참조하세요.

제로 ETL 통합 모니터링

제로 ETL 통합을 정기적으로 모니터링하면 최적의 성능을 보장하고 문제를 조기에 식별하는 데 도움이 됩니다.

통합 상태 모니터링

Glue API를 사용하여 AWS 제로 ETL 통합의 상태를 모니터링합니다.

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

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

통합 상태는 다음과 같습니다.

- creating - 통합 설정 중
- active - 통합이 실행 중이고 데이터 복제 중
- modifying - 통합 구성 업데이트 중
- needs_attention – 통합에 수동 개입 필요
- failed - 통합에 오류가 발생
- deleting - 통합 제거 중

성능 모니터링

제로 ETL 통합 성능의 다음 측면을 모니터링합니다.

- 복제 지연 - Oracle에서 변경이 발생하는 시점과 Amazon Redshift에 나타나는 시점 간의 시간 차이
- 데이터 처리량 - 시간 단위당 복제되는 데이터의 양
- 오류율 - 복제 오류 또는 실패 빈도
- 리소스 사용률 - 소스 시스템과 대상 시스템 모두에서 CPU, 메모리 및 네트워크 사용량

Amazon CloudWatch를 사용하여 이러한 지표를 모니터링하고 중요한 임계값에 대한 경보를 설정합니다.

Oracle Database@AWS에서 제로 ETL 통합 관리

제로 ETL 통합을 생성한 후 통합 수정 및 삭제를 비롯한 다양한 관리 작업을 수행할 수 있습니다. 이 섹션에서는 제로 ETL 통합의 지속적인 관리를 다룹니다.

제로 ETL 통합 수정

지원되는 데이터 웨어하우스에서 제로 ETL 통합의 이름, 설명 및 데이터 필터링 옵션만 수정할 수 있습니다. 통합을 암호화하는 데 사용된 AWS Key Management Service 키나 소스 또는 대상 데이터베이스는 수정할 수 없습니다.

통합 수정을 위한 사전 조건

제로 ETL 통합을 수정하기 전에 다음이 있는지 확인합니다.

- 필수 권한 - IAM 사용자 또는 역할에는 표준 AWS Glue 권한 외에도 `odb:UpdateOutboundIntegration` 권한이 있어야 합니다.
- 활성 상태의 통합 - 통합은 `CREATING`, `MODIFYING`, `DELETING` 또는 `FAILED` 상태가 아닌 `ACTIVE` 상태여야 합니다.
- 유효한 데이터 필터 구문 - 새 데이터 필터는 지원되는 포함/제외 패턴 구문을 따라야 합니다.

데이터 필터 수정

데이터 필터를 수정하여 복제할 테이블 또는 스키마를 변경할 수 있습니다. 이렇게 하면 전체 통합을 다시 생성하지 않고도 복제에서 데이터베이스 객체를 추가하거나 제거할 수 있습니다.

통합에 대한 데이터 필터를 수정하려면 `modify-integration` 명령을 사용합니다.

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

통합 이름과 설명을 동시에 수정할 수도 있습니다. 다음 예제에서는 pdb1에서 두 스키마의 통합 이름, 설명 및 필터를 수정합니다.

```
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

데이터 필터를 수정하면 통합이 `modifying` 상태로 전환되고 데이터의 재동기화를 수행합니다. 통합은 복제를 중지하고, 새 필터 설정을 적용하고, 재로드 대상 작업으로 복제를 재개합니다. 통합 상태를 모니터링하여 수정이 성공적으로 완료되었는지 확인합니다.

제로 ETL 통합에 대한 데이터 필터 수정 시 고려 사항

데이터 필터를 수정할 때는 다음 사항을 고려하세요.

- 단일 PDB 제한 - 통합당 하나의 플러그형 데이터베이스(PDB)만 지정할 수 있습니다. `include: pdb1.*.*, include: pdb2.*.*`와 같은 데이터 필터는 지원되지 않습니다.
- 복제 중단 - 수정 프로세스 중에 데이터 복제가 중지되고 새 필터가 적용된 후 재개됩니다.
- 데이터 재로드 - 통합은 새 필터 기준과 일치하는 데이터의 전체 재로드를 수행합니다.
- 성능 영향 - 대규모 데이터 필터 변경을 완료하는 데 상당한 시간이 걸릴 수 있으며 다시 로드하는 동안 소스 데이터베이스 성능에 영향을 미칠 수 있습니다.

제로 ETL 통합 설정 수정에 대한 제한 사항

제로 ETL 통합을 생성한 후에는 다음 설정을 수정할 수 없습니다.

- 보안 암호 ARN - 데이터베이스 보안 자격 증명이 포함된 AWS Secrets Manager 보안 암호
- KMS 키: 암호화에 사용된 고객 관리형 키

- 소스 ARN - Oracle Database@AWS VM 클러스터
- 대상 ARN - Amazon Redshift 클러스터 또는 네임스페이스

이러한 설정을 변경하려면 기존 제로 ETL 통합을 삭제하고 새 통합을 생성합니다.

제로 ETL 통합 삭제

제로 ETL 통합이 더 이상 필요하지 않은 경우 이를 삭제하여 복제를 중지하고 연결된 리소스를 정리할 수 있습니다.

AWS Glue를 사용한 삭제

AWS Glue API를 사용하여 제로 ETL 통합을 삭제할 수 있습니다.

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

다음 상태에서 통합을 삭제할 수 있습니다.

- 활성화
- needs_attention
- "failed"
- syncing

삭제의 영향

제로 ETL 통합을 삭제할 때는 다음 효과를 고려하세요.

복제가 중지됩니다.

Oracle Database@AWS는 Amazon Redshift의 새 변경 사항을 복제하지 않습니다.

기존 데이터는 보존됩니다.

Amazon Redshift에 이미 복제된 데이터는 계속 사용할 수 있습니다.

대상 데이터베이스는 그대로 유지됩니다.

통합에서 생성된 Amazon Redshift 데이터베이스는 자동으로 삭제되지 않습니다.

> **Important**
>
> 삭제하면 되돌릴 수 없습니다. 삭제 후 복제를 재개해야 하는 경우 전체 초기 로드를 수행하는 새 통합을 생성합니다.

제로 ETL 관리 모범 사례

제로 ETL 통합의 성능, 보안 및 비용 효율성을 최적화하려면 다음 모범 사례를 따르세요.

운영 모범 사례

이러한 운영 관행은 안정적이고 효율적인 제로 ETL 통합을 유지하는 데 도움이 됩니다.

정기 모니터링

CloudWatch 경보를 설정하여 통합 상태 및 성능 지표를 모니터링합니다.

자격 증명 교체

데이터베이스 암호를 정기적으로 교체하고 AWS Secrets Manager에서 업데이트합니다.

백업 확인

Oracle 데이터베이스 백업에 재해 복구에 필요한 구성 요소가 포함되어 있는지 정기적으로 확인합니다.

성능 테스트

특히 사용량이 가장 많은 기간 동안 제로 ETL 통합이 Oracle 데이터베이스 성능에 미치는 영향을 테스트합니다.

스키마 변경 계획

프로덕션에 적용하기 전에 개발 환경에서 스키마 변경 사항을 계획하고 테스트합니다.

보안 모범 사례

이러한 보안 조치를 구현하여 제로 ETL 통합 및 데이터를 보호합니다.

최소 권한 액세스

복제 사용자 및 AWS IAM 역할에 필요한 최소 권한만 부여합니다.

네트워크 보안

보안 그룹 및 NACL을 사용하여 네트워크 액세스를 필요한 포트 및 소스로만 제한합니다.

저장 시 암호화

Oracle 데이터베이스와 Amazon Redshift 클러스터가 모두 저장된 암호화를 사용하는지 확인합니다.

감사 로깅

Oracle과 Amazon Redshift 모두에서 감사 로깅을 활성화하여 데이터 액세스 및 변경 사항을 추적합니다.

보안 암호 관리

가능하면 AWS Secrets Manager 자동 교체 기능을 사용합니다.

비용 최적화

이러한 전략을 적용하여 비용을 최적화하는 동시에 효과적인 제로 ETL 통합 성능을 유지합니다.

데이터 필터링

정확한 데이터 필터를 사용하여 필요한 데이터만 복제하여 스토리지 및 컴퓨팅 비용을 절감합니다.

Amazon Redshift 최적화

적절한 Amazon Redshift 노드 유형을 사용하고 데이터 압축을 구현하여 비용을 최적화합니다.

사용 모니터링

AWS Cost Explorer를 통해 제로 ETL 통합 사용량 및 비용을 정기적으로 검토합니다.

미사용 통합 정리

지속적인 요금을 방지하기 위해 더 이상 필요하지 않은 통합을 삭제합니다.

제로 ETL 통합 문제 해결

이 섹션에서는 제로 ETL 통합과 관련된 일반적인 문제를 해결하기 위한 지침을 제공합니다.

제로 ETL 통합 설정 실패

인증 실패 횟수

- 복제 사용자가 존재하고 AWS Secrets Manager에 올바른 암호가 있는지 확인합니다.
- 복제 사용자에게 필요한 모든 권한이 부여되었는지 확인합니다.
- Oracle Database@AWS에서 보안 암호 ARN이 올바르고 액세스할 수 있는지 확인합니다.
- CMK 리소스 정책이 Oracle Database@AWS 서비스 위탁자의 액세스를 허용하는지 확인합니다.

네트워크 연결 문제

- ODB 네트워크에 제로 ETL 통합이 활성화되어 있는지 확인합니다.
- 포트 2484에 SSL이 올바르게 구성되어 있는지 확인합니다(Exadata만 해당).
- Oracle 데이터베이스 리스너가 실행 중이고 연결을 수락하고 있는지 확인합니다.
- 보안 그룹 및 NACL이 포트 2484에서 트래픽을 허용하는지 확인합니다.
- 보안 암호의 서비스 이름이 실제 Oracle 서비스 이름과 일치하는지 확인합니다.

권한 오류

- IAM 사용자 또는 역할에 AWS Glue 통합 작업에 필요한 권한이 있는지 확인합니다.
- Amazon Redshift 리소스 정책이 VM 클러스터의 인바운드 통합을 허용하는지 확인합니다.
- Oracle Database@AWS에 보안 암호 및 AWS Key Management Service 키에 대한 액세스 권한이 부여되었는지 확인합니다.

복제 문제

초기 로드 실패

- Oracle 데이터베이스에 전체 로드 작업을 지원하기에 충분한 리소스가 있는지 확인합니다.
- 소스 데이터베이스에서 추가 로깅이 활성화되어 있는지 확인합니다.
- 데이터 추출을 방해할 수 있는 테이블 수준 잠금 또는 제약 조건이 있는지 확인합니다.

변경 데이터 캡처 문제

- Oracle 데이터베이스에 적절한 다시 실행 로그 스페이스 및 보존이 있는지 확인합니다.
- 복제 사용자가 아카이브된 다시 실행 로그에 액세스할 수 있는지 확인합니다.
- ASM 지원 시스템의 경우 ASM 사용자가 올바르게 구성되었는지 확인합니다.
- Oracle 데이터베이스 성능을 모니터링하여 CDC가 리소스 경합을 일으키지 않는지 확인합니다.

높은 복제 지연

- CloudWatch에서 복제 지연 지표를 모니터링합니다.
- 소스 데이터베이스에서 트랜잭션 볼륨이 많거나 트랜잭션이 큰지 확인합니다.
- Amazon Redshift 클러스터에 수신 데이터를 처리할 수 있는 적절한 용량이 있는지 확인합니다.

데이터 일관성 문제

누락되거나 불완전한 데이터

- 데이터 필터에 필요한 모든 스키마와 테이블이 포함되어 있는지 확인합니다.
- 복제 실패를 일으킬 수 있는 지원되지 않는 데이터 형식이 있는지 확인합니다.
- 복제 사용자에게 필요한 모든 테이블에 대한 SELECT 권한이 있는지 확인합니다.

데이터 유형 변환 오류

- Oracle과 Redshift 간에 지원되는 데이터 형식 매핑을 검토합니다.
- 사용자 지정 처리가 필요할 수 있는 Oracle 관련 데이터 유형을 확인합니다.
- 더 호환되는 데이터 형식을 사용하도록 Oracle 스키마를 수정하는 것이 좋습니다.

모니터링 및 디버깅

다음 접근 방식을 사용하여 제로 ETL 통합 문제를 모니터링하고 디버깅합니다.

- 통합 상태 모니터링 - `aws glue describe-integrations`를 사용하여 통합 상태를 정기적으로 확인합니다.
- CloudWatch 지표 - 사용 가능한 CloudWatch 지표에서 복제 성능 및 오류를 모니터링합니다.
- Oracle 데이터베이스 모니터링 - Oracle 데이터베이스 성능 및 리소스 사용률을 모니터링합니다.
- Redshift 모니터링 - Amazon Redshift 클러스터 성능 및 스토리지 사용률을 모니터링합니다.

이 문제 해결 안내서를 사용하여 해결할 수 없는 복잡한 문제의 경우 다음 정보를 사용하여 AWS Support에 문의하세요.

- 통합 ARN 및 현재 상태입니다.
- 통합의 오류 메시지에서 작업을 설명합니다.
- Oracle 데이터베이스 및 Amazon Redshift 클러스터 구성.
- 문제가 발생하기 시작한 시점의 타임라인입니다.

Oracle Database@AWS의 보안

AWS에서 클라우드 보안은 가장 중요합니다. AWS 고객은 보안에 가장 보안에 민감한 조직의 요구 사항에 부합하도록 빌드된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 AWS, OCI 및 사용자 간의 공동 책임입니다. 공동 책임 모델은 이를 클라우드의 보안과 클라우드 내 보안으로 설명합니다.

- 클라우드의 보안 - AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호합니다. AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다.
- 클라우드 내 보안 – 귀하의 책임은 귀하가 사용하는 AWS 서비스에 따라 결정됩니다. 또한 데이터의 민감도, 조직의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Oracle Database@AWS 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 또한 Oracle Database@AWS 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스 사용 방법을 알아봅니다.

Oracle Database@AWS 리소스에 대한 액세스를 관리할 수 있습니다. 액세스를 관리하는 데 사용되는 방법은 사용자가 Oracle Database@AWS를 사용하여 수행해야 하는 작업 유형에 따라 다릅니다.

- Oracle Database@AWS 리소스를 관리할 수 있는 사용자를 결정하는 권한을 지정하려면 AWS Identity and Access Management(IAM) 정책을 사용합니다. 예를 들면, IAM을 사용하여 Exadata 인프라, VM 클러스터 또는 태그 리소스를 생성, 설명, 수정 및 삭제할 수 있는 사용자를 결정할 수 있습니다.
- Oracle 데이터베이스 엔진의 보안 기능을 사용하여 DB 인스턴스에 있는 데이터베이스에 로그인할 수 있는 사용자를 제어합니다. 이러한 보안 기능은 데이터베이스가 마치 로컬 네트워크에 있는 것처럼 실행됩니다.
- Exadata 데이터베이스와 함께 Secure Socket Layer(SSL) 또는 Transport Layer Security(TLS) 연결을 사용합니다. 자세한 내용은 TLS Walletless 연결 준비를 참조하세요.
- Oracle Database@AWS는 인터넷에서 즉시 액세스할 수 없으며 AWS의 프라이빗 서브넷에만 배포됩니다.
- Oracle Database@AWS는 다양한 작업에 많은 기본 TCP(Transmission Control Protocol) 포트를 사용합니다. 포트의 전체 목록은 기본 포트 할당을 참조하세요.

- 기본적으로 활성화된 Transparent Data Encryption(TDE)를 사용하여 키를 저장하고 관리하기 위해 Oracle Database@AWS는 OCI 볼트 또는 Oracle Key Vault를 사용합니다. Oracle Database@AWS는 AWS Key Management Service를 지원하지 않습니다.
- 기본적으로 데이터베이스는 Oracle 관리형 암호화 키를 사용하여 구성됩니다. 데이터베이스는 고객 관리형 키도 지원합니다.
- 데이터 보호를 개선하려면 Oracle Data Safe를 Oracle Database@AWS와 함께 사용합니다.

다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 Oracle Database@AWS를 구성하는 방법을 보여줍니다.

주제

- 의 데이터 보호Oracle Database@AWS
- Oracle Database@AWS의 Identity and Access Management(IAM)
- Oracle Database@AWS에 대한 규정 준수 검증
- Oracle Database@AWS의 복원성
- Oracle Database@AWS에 서비스 연결 역할 사용
- AWS 관리형 정책으로 Oracle Database@AWS 업데이트

의 데이터 보호Oracle Database@AWS

데이터를 보호하려면 AWS 계정자격 증명을 보호하고 AWS IAM Identity Center또는 AWS Identity and Access Management(IAM)를 통해 개별 사용자 계정을 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS리소스와 통신하세요. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- AWS CloudTrail으로 API 및 사용자 활동 로깅을 설정하세요. AWS 활동 캡처에 CloudTrail 추적을 사용하는 방법에 대한 자세한 내용은 AWS CloudTrail사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- AWS 암호화 솔루션을 AWS 서비스내의 모든 기본 보안 컨트롤과 함께 사용하세요.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.

- 명령줄 인터페이스 또는 API를 통해 AWS에 액세스할 때 FIPS 140-3 검증된 암호화 모듈이 필요한 경우, FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Oracle Database@AWS 또는 기타 AWS 서비스에서 콘솔, API, AWS CLI 또는 AWS SDK를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

데이터 암호화

Exadata 데이터베이스는 Oracle Transparent Data Encryption(TDE)을 사용하여 데이터를 암호화합니다. 또한 데이터는 임시 테이블스페이스, 실행 취소 세그먼트, 다시 실행 로그 및 JOIN 및 SORT와 같은 내부 데이터베이스 작업 중에 보호됩니다. 자세한 내용은 데이터 보안을 참조하세요.

전송 중 암호화

Exadata 데이터베이스는 기본 Oracle Net Services 암호화 및 무결성 기능을 사용하여 데이터베이스에 대한 연결을 보호합니다. 자세한 내용은 전송 중 데이터의 보안을 참조하세요.

키 관리

Transparent Data Encryption에는 마스터 암호화 키를 안전하게 저장하는 키 스토어와 키 스토어를 안전하고 효율적으로 관리하고 키 유지 관리 작업을 수행하는 관리 프레임워크가 포함됩니다. 자세한 내용은 Vault 암호화 키 관리를 참조하세요.

Oracle Database@AWS의 Identity and Access Management(IAM)

AWS Identity and Access Management(IAM)은 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 지원하는 AWS 서비스입니다. IAM 관리자는 어떤 사용자가 Oracle Database@AWS 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

주제

- 대상

- ID를 통한 인증
- 정책을 사용하여 액세스 관리
- Oracle Database@AWS에서 IAM을 사용하는 방식
- Oracle Database@AWS에 대한 ID 기반 정책
- AWS의 관리형 정책Oracle Database@AWS
- OCI에서 Oracle Database@AWS 인증 및 권한 부여
- Oracle Database@AWS ID 및 액세스 문제 해결

대상

AWS Identity and Access Management(IAM)를 사용하는 방법은 역할에 따라 다릅니다.

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청(참조Oracle Database@AWS ID 및 액세스 문제 해결)
- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출(Oracle Database@AWS에서 IAM을 사용하는 방식 참조)
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성(Oracle Database@AWS에 대한 ID 기반 정책 참조)

ID를 통한 인증

인증은 ID 자격 증명을 사용하여 AWS에 로그인하는 방식입니다. AWS 계정 루트 사용자이나 IAM 사용자로, 또는 IAM 역할을 수임하여 인증(에 로그인)받아야 합니다.

AWS IAM Identity Center(IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. 로그인하는 방법에 대한 자세한 내용은 AWS 로그인사용 설명서의 AWS 계정에 로그인하는 방법 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해 AWS는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 제공합니다. 자세한 내용은 IAM 사용 설명서의 API 요청용 AWS Signature Version 4 섹션을 참조하세요.

AWS 계정 루트 사용자

AWS 계정을 생성하는 경우에는 모든 AWS 서비스 서비스와 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 루트 사용자라는 단일 로그인 ID로 시작합니다. 일상적인 태스크에 루트 사용자를 사용

하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명이 필요한 작업은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 작업 섹션을 참조하세요.

페더레이션 ID

가장 좋은 방법은 인간 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명으로 AWS 서비스에 액세스하도록 하는 것입니다.

페더레이션 ID는 엔터프라이즈 사용자 디렉터리, 웹 ID 제공업체 또는 Directory Service의 사용자로, ID의 자격 증명을 사용하여 AWS 서비스에 액세스합니다. 페더레이션 ID는 임시 자격 증명을 제공하는 역할을 수임합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 추천합니다. 자세한 정보는 AWS IAM Identity Center사용 설명서의 What is IAM Identity Center?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명이 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서에서 임시 자격 증명을 사용하여 AWS에 액세스하려면 인간 사용자가 ID 제공업체와의 페더레이션을 사용하도록 요구를 참조하세요.

IAM 그룹은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자 사용 사례 섹션을 참조하세요.

IAM 역할

IAM 역할은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. 사용자에서 IAM 역할(콘솔)로 전환하거나 AWS CLI 또는 AWS API 작업을 직접적으로 호출하여 역할을 수임할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

정책을 사용하여 액세스 관리

정책을 생성하고 AWS ID 또는 리소스에 연결하여 AWS에서 내 액세스를 제어합니다. 정책은 자격 증명이나 리소스와 연결될 때 해당 권한을 정의합니다. AWS는 보안 주체가 요청을 보낼 때 이러한 정책

을 평가합니다. 대부분의 정책은 AWS에 JSON 문서로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

ID 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택 섹션을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS관리형 정책을 사용할 수 없습니다.

기타 정책 유형

AWS는 이러한 정책 타입이 부여하는 최대 권한을 설정할 수 있는 추가 정책 타입을 지지합니다.

- 권한 경계 - ID 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 자세한 정보는 IAM 사용 설명서의 IAM 엔터티의 권한 범위를 참조하세요.
- 서비스 제어 정책(SCP) - AWS Organizations내 조직 또는 조직 단위에 대한 최대 권한을 지정합니다. 자세한 내용은 AWS Organizations사용 설명서의 서비스 제어 정책을 참조하세요.

- 리소스 제어 정책(RCP) – 계정의 리소스에 사용할 수 있는 최대 권한을 설정합니다. 자세한 내용은 AWS Organizations사용 설명서의 리소스 제어 정책(RCP)을 참조하세요.
- 세션 정책 – 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련될 때 AWS가 요청을 허용할지 여부를 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

Oracle Database@AWS에서 IAM을 사용하는 방식

IAM을 사용하여 Oracle Database@AWS에 대한 액세스를 관리하기 전에 Oracle Database@AWS와 함께 사용할 수 있는 IAM 기능을 알아보세요.

IAM 특성	Oracle Database@AWS 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACL	아니요
ABAC(정책 내 태그)	부분
임시 자격 증명	예
엔터티 권한	예
서비스 역할	아니요
서비스 연결 역할	예

Oracle Database@AWS 및 기타 AWS 서비스에서 대부분의 IAM 기능을 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 IAM으로 작동하는 AWS 서비스를 참조하세요.

Oracle Database@AWS에 대한 ID 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Oracle Database@AWS에 대한 ID 기반 정책 예제

Oracle Database@AWS ID 기반 정책 예제를 보려면 Oracle Database@AWS에 대한 ID 기반 정책 섹션을 참조하세요.

Oracle Database@AWS 내 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 위탁자에는 계정, 사용자, 역할, 페더레이션 사용자 또는 AWS 서비스가 포함될 수 있습니다.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

Oracle Database@AWS 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

Oracle Database@AWS 작업 목록을 보려면 Service Authorization Reference의 Oracle Database@AWS에서 정의한 작업을 참조하세요.

Oracle Database@AWS의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
odb
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다.

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

Oracle Database@AWS ID 기반 정책 예제를 보려면 Oracle Database@AWS에 대한 ID 기반 정책 섹션을 참조하세요.

Oracle Database@AWS 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

Oracle Database@AWS 리소스 유형 및 해당 ARN의 목록을 보려면 서비스 승인 참조의 Oracle Database@AWS에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 Oracle Database@에서 정의한 작업AWS을 참조하세요.

Oracle Database@AWS ID 기반 정책 예제를 보려면 Oracle Database@AWS에 대한 ID 기반 정책 섹션을 참조하세요.

Oracle Database@AWS 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

Oracle Database@AWS 조건 키 목록을 보려면 서비스 승인 참조의 Oracle Database@AWS에 대한 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 Oracle Database@AWS에서 정의한 작업을 참조하세요.

Oracle Database@AWS ID 기반 정책 예제를 보려면 Oracle Database@AWS에 대한 ID 기반 정책 섹션을 참조하세요.

Oracle Database@AWS의 ACL

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Oracle Database@AWS를 사용한 ABAC

ABAC 지원(정책의 태그): 부분적

속성 기반 액세스 제어(ABAC)는 태그라고 불리는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM 엔터티 및 AWS 리소스에 태그를 연결하면 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계할 수 있습니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*또는 `aws:TagKeys`조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Oracle Database@AWS에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명은 AWS리소스에 대한 단기 액세스를 제공하며 페더레이션 또는 전환 역할을 사용할 때 자동으로 생성됩니다. AWS에서는 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 내용은 IAM 사용 설명서의 IAM의 임시 보안 자격 증명 및 IAM으로 작업하는 AWS 서비스 섹션을 참조하세요.

Oracle Database@AWS의 서비스 간 엔터티 권한

전달 액세스 세션(FAS) 지원: 예

전달 액세스 세션(FAS)은 AWS 서비스를 직접적으로 호출하는 위탁자의 권한과 요청하는 AWS 서비스를 함께 사용하여 다운스트림 서비스에 대한 요청을 수행합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Oracle Database@AWS의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Oracle Database@AWS 기능이 중단될 수 있습니다. Oracle Database@AWS이 그 일을 하라는 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

Oracle Database@AWS에 대한 서비스 연결 역할

서비스 연결 역할 지원: 예

서비스 연결 역할은 AWS서비스에 연결된 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 AWS 계정에 나타나고, 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

Oracle Database@AWS 서비스 연결 역할을 생성 또는 관리하는 방법에 대한 자세한 내용은 Oracle Database@AWS에 서비스 연결 역할 사용을 참조하세요.

Oracle Database@AWS에 대한 ID 기반 정책

기본적으로 사용자 및 역할에는 Oracle Database@AWS 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 Oracle Database@AWS에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 인증 참조에서 Oracle Database@AWS에 대한 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- Oracle Database@AWS 콘솔 사용
- 사용자가 Oracle Database@AWS 리소스를 프로비저닝하도록 허용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Oracle Database@AWS 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책으로 시작하고 최소 권한을 향해 나아가기 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반 사용 사례에 대한 권한을 부여하는 AWS관리형 정책을 사용합니다. AWS 계정에서 사용할 수 있습니다. 사용 사례에 고유한 AWS고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS직무에 대한 관리형 정책을 참조하세요.

- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. CloudFormation과 같이, 특정 AWS 서비스를 통해 사용되는 경우에만 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 – AWS 계정에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우, 추가 보안을 위해 MFA를 설정합니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

Oracle Database@AWS 콘솔 사용

Oracle Database@AWS 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은 AWS 계정에서 Oracle Database@AWS 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 직접적으로 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요가 없습니다. 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자가 Oracle Database@AWS 리소스를 프로비저닝하도록 허용

이 정책은 Oracle Database@AWS 리소스를 프로비저닝할 수 있는 완전한 액세스 권한을 사용자에게 허용합니다. VPC에서 DNS 확인을 설정하려면 아웃바운드 Route 53 해석기를 생성하고 OCI 도메인 이름을 사용하여 DNS 트래픽을 OCI DNS 리스너 IP로 전달하는 규칙을 추가합니다.

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": "*"
        }
    ]
}
```

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI나 AWS API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "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": "*"
        }
    ]
}
```

AWS의 관리형 정책Oracle Database@AWS

권한 세트 및 역할에 권한을 추가하려면 정책을 직접 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 편리합니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하려면 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용하면 됩니다. 이 정책은 일반적인 사용 사례를 다루며 사용자의 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 정보는 IAM 사용 설명서에서 AWS 관리형 정책을 참조하세요.

AWS 서비스는 AWS 관리형 정책을 유지하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스는 때때로 추가 권한을 AWS관리형 정책에 추가하여 새로운 기능을 지원합니다. 이 유형의 업데이트는 정책이 연결된 모든 자격 증명(권한 세트 및 역할)에 적용됩니다. 서비스는 새로운 기능이 시작되거나 새 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않기 때문에 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한 AWS는 여러 서비스의 직무에 대한 관리형 정책을 지원합니다. 예를 들어 `ReadOnlyAccess` AWS 관리형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스 권한을 제공합니다. 서비스에서 새 기능을 시작하면 AWS가 새 작업 및 리소스에 대한 읽기 전용 권한을 추가합니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한 AWS 관리형 정책을 참조하세요.

주제

- AWS 관리형 정책: AmazonODBServiceRolePolicy

AWS 관리형 정책: AmazonODBServiceRolePolicy

`AmazonODBServiceRolePolicy` 정책을 IAM 엔터티에 연결할 수 없습니다. 이 정책은 Oracle Database@AWS이(가) 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 자세한 내용은 Oracle Database@AWS에 서비스 연결 역할 사용 섹션을 참조하세요.

최신 버전의 JSON 정책 문서를 비롯하여 정책에 대한 추가 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 AmazonODBServiceRolePolicy를 참조하세요.

OCI에서 Oracle Database@AWS 인증 및 권한 부여

AWS API를 사용하여 Oracle Database@AWS에 대한 리소스를 생성하면 해당 리소스는 연결된 Oracle Cloud Infrastructure(OCI) 테넌시에 논리적으로 상주합니다. 이러한 리소스를 배포하기 위해 AWS는 사용자를 대신하여 OCI API와 통신합니다. 혼동된 대리자 문제를 완화하기 위해 OCI 및 Oracle Database@AWS는 AWS STS를 신뢰할 수 있는 엔터티로 사용하고 액세스 세션을 전달하여 연결된 테넌시에서 OCI API를 사용할 의도를 승인합니다. 따라서 이벤트는 AWS CloudTrail 추적 및 이벤트 기록에 OCI IP 스페이스의 `sts:getCallerIdentity` API에 대해 기록됩니다. Oracle Database@AWS API를 사용할 때 다음과 같은 이벤트가 발생할 수 있습니다.

Oracle Database@AWS ID 및 액세스 문제 해결

다음 정보를 사용하여 Oracle Database@AWS 및 IAM에서 작업할 때 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- Oracle Database@AWS에서 작업을 수행할 권한이 없음
- iam:PassRole을 수행하도록 인증되지 않음
- 내 AWS 계정 외부의 사람이 내 Oracle Database@AWS 리소스에 액세스할 수 있게 허용하기를 원합니다.

Oracle Database@AWS에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 표시되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 odb:*GetWidget* 권한이 없을 때 발생합니다.

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

이 경우, odb:*GetWidget* 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam:PassRole을 수행하도록 인증되지 않음

iam:PassRole 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Oracle Database@AWS에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스에서는 새로운 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 해당 서비스에 기존 역할을 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 Oracle Database@AWS에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

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

이 경우, Mary가 iam:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 AWS 계정 외부의 사람이 내 Oracle Database@AWS 리소스에 액세스할 수 있게 허용하기를 원합니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- Oracle Database@AWS에서 이러한 기능을 지원하는지 여부를 알아보려면 Oracle Database@AWS에서 IAM을 사용하는 방식 섹션을 참조하세요.
- 소유하고 있는 AWS 계정의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 자신이 소유한 다른 AWS 계정의 IAM 사용자에 대한 액세스 권한 제공을 참조하세요.
- 리소스에 대한 액세스 권한을 서드 파티 AWS 계정에게 제공하는 방법을 알아보려면 IAM 사용 설명서의 서드 파티가 소유한 AWS 계정에 대한 액세스 제공을 참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

Oracle Database@AWS에 대한 규정 준수 검증

Oracle Database@AWS 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률 및 규정에 따라 결정됩니다. 클라우드의 규정 준수에 대한 Oracle 설명서는 Oracle 웹 사이트에서 확인할 수 있습니다.

Oracle Database@AWS의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전에서는 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며 이러한 가용 영역은 짧은 대기 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크에 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 정보는 AWS 글로벌 인프라를 참조하세요.

AWS 글로벌 인프라뿐만 아니라 Oracle Database@AWS도 데이터 복원력과 백업 요구 사항을 지원하는 다양한 기능을 제공합니다.

Oracle Database@AWS에 서비스 연결 역할 사용

Oracle Database@AWS는 AWS Identity and Access Management(IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Oracle Database@AWS에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Oracle Database@AWS에서 사전 정의하며 서비스에서 다른 AWS 서비스를 직접적으로 호출하기 위해 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 통해 Oracle Database@AWS 사용이 쉬워지는데 필요한 권한을 수동으로 추가할 필요가 없기 때문입니다. Oracle Database@AWS에서 서비스 연결 역할 권한을 정의하므로, 달리 정의되지 않은 한 Oracle Database@AWS에서만 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 역할의 관련 리소스를 삭제해야만 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 Oracle Database@AWS 리소스가 보호됩니다.

Oracle Database@AWS에 대한 서비스 연결 역할 권한

Oracle Database@AWS에서는 AWSServiceRoleForODB라는 서비스 연결 역할을 사용하여 사용자의 리소스 대신 Oracle Database@AWS에서 AWS 서비스를 직접적으로 호출할 수 있도록 허용합니다.

AWSServiceRoleForODB 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

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

이 서비스 연결 역할에는 계정에서 운영할 수 있는 권한을 부여하는 `AmazonODBServiceRolePolicy`라는 권한 정책이 연결되어 있습니다. 자세한 내용은 AWS 관리형 정책: AmazonODBServiceRolePolicy 섹션을 참조하세요.

> **Note**
>
> IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 다음 오류 메시지가 표시되는 경우:

리소스를 만들 수 없습니다. 서비스 연결 역할을 생성할 권한이 있는지 확인합니다. 그렇지 않은 경우 기다렸다가 나중에 다시 시도하십시오.
다음 권한이 활성화되어 있는지 확인하십시오.

```
{
    "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"
        }
    }
}
```

자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

Oracle Database@AWS에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. Exadata 데이터베이스를 생성하면 Oracle Database@AWS에서 서비스 연결 역할을 대신 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. Exadata 데이터베이스를 생성하면 Oracle Database@AWS에서 서비스 연결 역할을 대신 생성합니다.

Oracle Database@AWS에 대한 서비스 연결 역할 편집

Oracle Database@AWS는 AWSServiceRoleForODB 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 그러나 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 설명 편집을 참조하세요.

Oracle Database@AWS에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제할 것을 권합니다. 그렇게 하면 적극적으로 모니터링하거나 유지 관리하지 않은 미사용 엔터티가 없습니다. 그러나 서비스 연결 역할을 삭제하려면 먼저 모든 리소스를 삭제해야 합니다.

Oracle Database@AWS에 대한 서비스 연결 역할 정리

IAM을 사용하여 서비스 연결 역할을 삭제하기 전에 먼저 역할에 활성 세션이 없는지 확인하고 역할에서 사용되는 리소스를 모두 제거해야 합니다.

IAM 콘솔에서 서비스 연결 역할에 활성 세션이 있는지 확인하려면

1. AWS Management Console에 로그인하여 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할(Roles)을 선택합니다. 그런 다음 AWSServiceRoleForODB 역할의 이름(확인란 아님)을 선택합니다.
3. 선택한 역할의 요약 페이지에서 Access Advisor(액세스 관리자) 탭을 선택합니다.
4. [Access Advisor] 탭에서 서비스 연결 역할의 최근 활동을 검토합니다.

> **Note**
>
> Oracle Database@AWS에서 AWSServiceRoleForODB 역할을 사용하는지 잘 모를 경우에는 역할을 삭제해 볼 수 있습니다. 서비스가 역할을 사용 중인 경우 삭제가 실패하며 역할이 사용되고 있는 AWS 리전을 볼 수 있습니다. 역할이 사용 중인 경우에는 세션이 종료될 때까지 기다렸다가 역할을 삭제해야 합니다. 서비스 연결 역할에 대한 세션은 취소할 수 없습니다.

AWSServiceRoleForODB 역할을 제거하려면 먼저 모든 Oracle Database@AWS 리소스를 삭제해야 합니다.

Oracle Database@AWS 서비스 연결 역할이 지원되는 리전

Oracle Database@AWS에서는 서비스를 사용할 수 있는 모든 AWS 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS 리전 및 엔드포인트를 참조하세요.

AWS 관리형 정책으로 Oracle Database@AWS 업데이트

이 서비스가 이러한 변경 내용을 추적하기 시작한 이후부터 Oracle Database@AWS의 AWS 관리형 정책 업데이트에 관한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 Oracle Database@AWS 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경	설명	날짜
Oracle Database@AWS에 대한 서비스 연결 역할 권한 - 기존 정책에 대한 업데이트	Oracle Database@AWS는 `AWSServiceRoleForODB` 서비스 연결 역할의 `AmazonODBServiceRolePolicy` 에 새로운 권한을 추가했습니다. 이러한 권한은 Oracle Database@AWS에서 다음을 수행하도록 허용합니다. • Amazon VPC Transit Gateway Attachment 설명 • Amazon EC2 연결 설명 • Amazon EventBridge 소스 활성화 자세한 내용은 Oracle Database@AWS에 대한 서비스 연결 역할 권한 섹션을 참조하세요.	2025년 6월 30일
Oracle Database@AWS에 대한 서비스 연결 역할 권한 - 기존 정책에 대한 업데이트	Oracle Database@AWS는 `AWSServiceRoleForODB` 서비스 연결 역할의 `AmazonODBServiceRolePolicy` 에 새로운 권한을 추가했습니다. 이러한 권한은 Oracle Database@AWS에서 다음을 수행하도록 허용합니다. • Amazon EventBridge 소스 설명 • 이벤트 버스 설명 및 생성 자세한 내용은 Oracle Database@AWS에 대한 서비스 연결 역할 권한 섹션을 참조하세요.	2025년 6월 26일
AWS 관리형 정책: AmazonODBServiceRolePolicy - 새로운 서비스 연결 역할 정책	Oracle Database@AWS가 `AWSServiceRoleForODB` 서비스 연결 역할에 대한 `AmazonODBServiceRolePolicy` 를 추가했습니다. 자세한 내용은 AWS 관리형 정책: AmazonODBServiceRolePolicy 섹션을 참조하세요.	2024년 12월 2일
Oracle Database@AWS에서 변경 사항 추적 시작	Oracle Database@AWS에서 AWS 관리형 정책에 대한 변경 내용 추적을 시작했습니다.	2024년 12월 2일

Oracle Database@AWS 모니터링

Oracle Database@AWS 및 다른 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하려면 모니터링이 중요합니다. AWS는 Oracle Database@AWS를 모니터링하고, 이상이 있을 때 이를 보고하고, 필요한 경우 자동 조치를 취할 수 있도록 다음과 같은 모니터링 도구를 제공합니다.

- Amazon CloudWatch는 AWS에서 실행하는 AWS 리소스와 애플리케이션을 실시간으로 모니터링합니다. 지표를 수집 및 추적하고, 사용자 지정 대시보드를 생성할 수 있으며, 지정된 지표가 지정한 임곗값에 도달하면 사용자에게 알리거나 조치를 취하도록 경보를 설정할 수 있습니다. 예를 들어 CloudWatch에서 Amazon EC2 인스턴스의 CPU 사용량 또는 기타 지표를 추적하고 필요할 때 자동으로 새 인스턴스를 시작할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하세요.
- Amazon CloudWatch Logs로 Amazon EC2 인스턴스, CloudTrail, 기타 소스의 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다. CloudWatch Logs는 로그 파일의 정보를 모니터링하고 특정 임계값에 도달하면 사용자에게 알릴 수 있습니다. 또한 매우 내구성이 뛰어난 스토리지에 로그 데이터를 저장할 수 있습니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서를 참조하세요.
- Amazon EventBridge를 사용하면 AWS 서비스를 자동화하고 애플리케이션 가용성 문제나 리소스 변경 같은 시스템 이벤트에 자동으로 대응할 수 있습니다. AWS 서비스의 이벤트는 거의 실시간으로 EventBridge로 전송됩니다. 원하는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동화 작업을 지정할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하세요.
- AWS CloudTrail은 직접 수행하거나 AWS 계정을 대신하여 수행한 API 직접 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 어떤 사용자 및 계정이 AWS를 직접적으로 호출했는지, 어떤 소스 IP 주소에 직접 호출이 이루어졌는지, 언제 직접 호출이 발생했는지 확인할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

Amazon CloudWatch를 사용한 Oracle Database@AWS 모니터링

원시 데이터를 수집하여 읽기 가능한 실시간에 가까운 지표로 처리하는 CloudWatch를 사용하여 Oracle Database@AWS를 모니터링할 수 있습니다. 이러한 통계는 15개월간 보관되므로 기록 정보에 액세스하고 웹 애플리케이션 또는 서비스가 어떻게 실행되고 있는지 전체적으로 더 잘 파악할 수 있습니다. 특정 임곗값을 주시하다가 해당 임곗값이 충족될 때 알림을 전송하거나 조치를 취하도록 경보를 설정할 수도 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하세요.

Oracle Database@AWS에 대한 Amazon CloudWatch 지표

이 Oracle Database@AWS 서비스는 VM 클러스터, 컨테이너 데이터베이스 및 플러그형 데이터베이스의 AWS/ODB 네임스페이스에 있는 Amazon CloudWatch에 지표를 보고합니다.

주제

- 클라우드 VM 클러스터에 대한 지표
- 컨테이너 데이터베이스에 대한 지표
- 플러그형 데이터베이스에 대한 지표

클라우드 VM 클러스터에 대한 지표

Oracle Database@AWS 서비스는 클라우드 VM 클러스터의 AWS/ODB 네임스페이스에서 다음과 같은 지표를 보고합니다.

지표	설명	단위
ASMDiskgroupUtilization	디스크 그룹에서 사용되는 사용 가능한 스페이스의 백분율입니다. 사용 가능한 스페이스는 증가에 사용할 수 있는 스페이스입니다. 데이터 디스크 그룹은 Oracle 데이터베이스 파일을 저장합니다. RECO 디스크 그룹에는 아카이브 및 플래시백 로그와 같은 복구용 데이터베이스 파일이 포함되어 있습니다.	백분율
CpuUtilization	CPU 사용률(%)입니다.	백분율
FilesystemUtilization	프로비저닝된 파일 시스템의 사용률입니다.	백분율
LoadAverage	5분 동안의 시스템 로드 평균입니다.	Integer

지표	설명	단위
MemoryUtilization	스와핑 없이 새 애플리케이션을 시작하는 데 사용할 수 있는 메모리의 백분율. 사용 가능한 메모리는 cat /proc/meminfo 명령을 통해 얻을 수 있습니다.	백분율
NodeStatus	호스트에 연결할 수 있는지 여부를 나타냅니다.	Integer
OcpusAllocated	할당된 OCPU 수입니다.	Integer
SwapUtilization	총 스왑 스페이스의 사용률입니다.	백분율

컨테이너 데이터베이스에 대한 지표

Oracle Database@AWS 서비스는 컨테이너 데이터베이스의 AWS/ODB 네임스페이스에서 다음과 같은 지표를 보고합니다.

지표	설명	단위
BlockChanges	초당 변경된 평균 블록 수입니다.	초당 변경
CpuUtilization	모든 소비자 그룹에 걸쳐 집계된 백분율로 표시되는 CPU 사용률입니다. 사용률은 데이터베이스가 사용할 수 있는 CPU 수를 기준으로 보고되며, 이는 OCPU 수의 두 배입니다.	백분율
CurrentLogons	선택한 간격 동안 성공한 로그온 수입니다.	개수

지표	설명	단위
ExecuteCount	선택한 간격 동안 SQL 문을 실행한 사용자 및 재귀 직접 호출 수입니다.	개수
ParseCount	선택한 간격 동안 하드 및 소프트 구문 분석의 수입니다.	개수
StorageAllocated	수집 시 데이터베이스에 할당된 총 스토리지 스페이스 크기입니다.	GB
StorageAllocatedByTablespace	수집 시 테이블스페이스에 할당된 총 스토리지 스페이스 크기입니다. 컨테이너 데이터베이스의 경우 이 지표는 루트 컨테이너 테이블스페이스를 제공합니다.	GB
StorageUsed	수집 시 데이터베이스에서 사용하는 총 스토리지 스페이스 크기입니다.	GB
StorageUsedByTablespace	수집 시 테이블스페이스에서 사용하는 총 스토리지 스페이스 크기입니다. 컨테이너 데이터베이스의 경우 이 지표는 루트 컨테이너 테이블스페이스를 제공합니다.	GB
StorageUtilization	현재 사용 중인 프로비저닝된 스토리지 용량의 백분율입니다. 모든 테이블스페이스에 할당된 총 스페이스를 나타냅니다.	백분율

지표	설명	단위
StorageUtilizationByTablespace	이는 수집 시 테이블스페이스에서 사용하는 스토리지 스페이스의 비율을 나타냅니다. 컨테이너 데이터베이스의 경우 이 지표는 루트 컨테이너 테이블스페이스를 제공합니다.	백분율
TransactionCount	선택한 간격 동안 사용자 커밋 및 사용자 롤백의 총 수입니다.	개수
UserCalls	선택한 간격 동안 로그온, 구문 분석 및 실행 직접 호출의 결합된 수입니다.	개수

플러그형 데이터베이스에 대한 지표

Oracle Database@AWS 서비스는 플러그형 데이터베이스의 AWS/ODB 네임스페이스에서 다음과 같은 지표를 보고합니다.

지표	설명	단위
AllocatedStorageUtilizationByTablespace	할당된 모든 스페이스 중 테이블스페이스에서 사용하는 스페이스의 백분율입니다. 컨테이너 데이터베이스의 경우 이 지표는 루트 컨테이너 테이블스페이스에 대한 데이터를 제공합니다. (통계: 평균, 간격: 30분)	%
AvgGCCRBlockReceiveTime	평균 전역 캐시 CR(일관된 읽기) 블록 수신 시간입니다. RAC/클러스터 데이터베이스 전용입니다. (통계: 평균, 간격: 5분)	밀리초

지표	설명	단위
AvgGCCurrentBlockReceiveTime	평균 글로벌 캐시 현재 블록 수신 시간입니다. 통계는 평균값을 보고합니다. Real Application Cluster(RAC) 데이터베이스 전용입니다. (통계: 평균, 간격: 5분)	밀리초
BlockChanges	초당 변경된 평균 블록 수입니다. (통계: 평균, 간격: 1분)	초당 변경
BlockingSessions	현재 차단 세션입니다. 컨테이너 데이터베이스에는 적용되지 않습니다. (통계: 최대, 간격: 15분)	개수
CPUTimeSeconds	시간 간격 동안 데이터베이스 인스턴스의 포그라운드 세션별 CPU 시간 누적의 평균 비율입니다. 평균 활성 세션의 CPU 시간 구성 요소입니다. (통계: 평균, 간격: 1분)	초당 초 수
CpuCount	선택한 간격 동안의 CPU 수입니다.	개수
CpuUtilization	모든 소비자 그룹에 걸쳐 집계된 백분율로 표시되는 CPU 사용률입니다. 사용률은 데이터베이스가 사용할 수 있는 CPU 수를 기준으로 보고되며, 이는 OCPU 수의 두 배입니다. (통계: 평균, 간격: 1분)	%
CurrentLogons	선택한 간격 동안 성공한 로그온 수입니다. (통계: 합계, 간격: 1분)	개수

지표	설명	단위
DBTimeSeconds	시간 간격 동안 데이터베이스 인스턴스의 포그라운드 세션별 데이터베이스 시간 누적(CPU + 대기)의 평균 비율입니다. 평균 활성 세션이라고도 합니다. (통계: 평균, 간격: 1분)	초당 초 수
DbmgmtJobExecutionsCount	단일 관리형 데이터베이스 또는 데이터베이스 그룹에서의 SQL 작업 실행 수와 해당 상태입니다. 상태 차원 값은 "Succeeded", "Failed", "InProgress"일 수 있습니다. (통계: 합계, 간격: 1분)	개수
ExecuteCount	선택한 간격 동안 SQL 문을 실행한 사용자 및 재귀 직접 호출 수입니다. (통계: 합계, 간격: 1분)	개수
FRASpaceLimit	플래시 복구 영역 스페이스 제한입니다. 플러그형 데이터베이스에는 적용되지 않습니다. (통계: 최대, 간격: 15분)	GB
FRAUtilization	플래시 복구 영역 사용률입니다. 플러그형 데이터베이스에는 적용되지 않습니다. (통계: 평균, 간격: 15분)	%
GCCRBlocksReceived	초당 수신된 전역 캐시 CR(일관된 읽기) 블록입니다. RAC/클러스터 데이터베이스 전용입니다. (통계: 평균, 간격: 5분)	초당 블록 수

지표	설명	단위
GCCurrentBlocksReceived	초당 수신된 글로벌 캐시 현재 블록을 나타냅니다. 통계는 평균값을 보고합니다. Real Application Cluster(RAC) 데이터베이스 전용입니다. (통계: 평균, 간격: 5분)	초당 블록 수
IOPS	초당 입/출력 평균 작업 수입니다. (통계: 평균, 간격: 1분)	초당 연산 수
IOThroughputMB	초당 MB 단위의 평균 처리량입니다. (통계: 평균, 간격: 1분)	초당 MB
InterconnectTrafficMB	평균 노드 간 데이터 전송 속도입니다. RAC/클러스터 데이터베이스 전용입니다. (통계: 평균, 간격: 5분)	초당 MB
InvalidObjects	데이터베이스 객체 수가 잘못되었습니다. 컨테이너 데이터베이스에는 적용되지 않습니다. (통계: 최대, 간격: 24시간)	개수
LogicalBlocksRead	초당 SGA/메모리(버퍼 캐시)에서 읽은 평균 블록 수입니다. (통계: 평균, 간격: 1분)	초당 읽기 수
MaxTablespaceSize	가능한 최대 테이블스페이스 크기입니다. 컨테이너 데이터베이스의 경우 이 지표는 루트 컨테이너 테이블스페이스에 대한 데이터를 제공합니다. (통계: 최대, 간격: 30분)	GB
MemoryUsage	메모리 풀 총 크기(MB)입니다. (통계: 평균, 간격: 15분)	MB

지표	설명	단위
MonitoringStatus	리소스의 모니터링 상태입니다. 지표 수집이 실패하면 이 지표에 오류 정보가 캡처됩니다. (통계: 평균, 간격: 5분)	해당 사항 없음
NonReclaimableFRA	회수할 수 없는 빠른 복구 영역입니다. 플러그형 데이터베이스에는 적용되지 않습니다. (통계: 평균, 간격: 15분)	%
OcpusAllocated	선택한 시간 간격 동안 서비스에 의해 할당된 실제 OCPU 수입니다. (통계: 개수, 간격: 1분)	Integer
ParseCount	선택한 간격 동안 하드 및 소프트 구문 분석의 수입니다. (통계: 합계, 간격: 1분)	개수
ParsesByType	초당 하드 또는 소프트 구문 분석 수입니다. (통계: 평균, 간격: 1분)	초당 구문 분석 수
ProblematicScheduledDBMSJobs	문제가 있는 예약된 데이터베이스 작업 수입니다. 컨테이너 데이터베이스에는 적용되지 않습니다. (통계: 최대, 간격: 15분)	개수
ProcessLimitUtilization	프로세스 제한 사용률입니다. 플러그형 데이터베이스에는 적용되지 않습니다. (통계: 평균, 간격: 1분)	%

지표	설명	단위
Processes	데이터베이스 프로세스 수입니다. 플러그형 데이터베이스에는 적용되지 않습니다. (통계: 최대, 간격: 1분)	개수
ReclaimableFRA	회수할 수 있는 빠른 복구 영역입니다. 플러그형 데이터베이스에는 적용되지 않습니다. (통계: 평균, 간격: 15분)	%
ReclaimableFRASpace	플래시 복구 영역 회수 가능 스페이스입니다. 플러그형 데이터베이스에는 적용되지 않습니다. (통계: 평균, 간격: 15분)	GB
RedoSizeMB	생성된 재실행의 평균 양으로, 초당 MB입니다. (통계: 평균, 간격: 1분)	초당 MB
SessionLimitUtilization	세션 제한 사용률입니다. 플러그형 데이터베이스에는 적용되지 않습니다. (통계: 평균, 간격: 1분)	%
Sessions	데이터베이스의 세션 수입니다. (통계: 평균, 간격: 1분)	개수
StorageAllocated	간격 동안 테이블스페이스에 의해 할당된 최대 스페이스 크기입니다. 컨테이너 데이터베이스의 경우 이 지표는 루트 컨테이너 테이블스페이스에 대한 데이터를 제공합니다. (통계: 최대, 간격: 30분)	GB

지표	설명	단위
StorageAllocatedByTablespace	간격 동안 테이블스페이스에 의해 할당된 최대 스페이스 크기입니다. 컨테이너 데이터베이스의 경우 이 지표는 루트 컨테이너 테이블스페이스에 대한 데이터를 제공합니다. (통계: 최대, 간격: 30분)	GB
StorageUsed	간격 동안 사용되는 최대 스페이스 크기입니다. (통계: 최대, 간격: 30분)	GB
StorageUsedByTablespace	간격 동안 테이블스페이스에서 사용하는 최대 스페이스 크기입니다. 컨테이너 데이터베이스의 경우 이 지표는 루트 컨테이너 테이블스페이스에 대한 데이터를 제공합니다. (통계: 최대, 간격: 30분)	GB
StorageUtilization	현재 사용 중인 프로비저닝된 스토리지 용량의 백분율입니다. 모든 테이블스페이스에 할당된 총 스페이스를 나타냅니다. (통계: 평균, 간격: 30분)	%
StorageUtilizationByTablespace	테이블스페이스별로 사용된 스페이스의 백분율입니다. 컨테이너 데이터베이스의 경우 이 지표는 루트 컨테이너 테이블스페이스에 대한 데이터를 제공합니다. (통계: 평균, 간격: 30분)	%

지표	설명	단위
TransactionCount	선택한 간격 동안 사용자 커밋 및 사용자 롤백의 총 수입니다. (통계: 합계, 간격: 1분)	개수
TransactionsByStatus	커밋 또는 롤백된 초당 트랜잭션의 수입니다. (통계: 평균, 간격: 1분)	초당 트랜잭션 수
UnusableIndexes	데이터베이스 스키마에서 사용할 수 없는 인덱스 수입니다. 컨테이너 데이터베이스에는 적용되지 않습니다. (통계: 최대, 간격: 24시간)	개수
UsableFRA	사용 가능한 빠른 복구 영역입니다. 플러그형 데이터베이스에는 적용되지 않습니다. (통계: 평균, 간격: 15분)	%
UsedFRASpace	플래시 복구 영역 스페이스 사용량입니다. 플러그형 데이터베이스에는 적용되지 않습니다. (통계: 최대, 간격: 15분)	GB
UserCalls	선택한 간격 동안 로그온, 구문 분석 및 실행 직접 호출의 결합된 수입니다. (통계: 합계, 간격: 1분)	개수
WaitTimeSeconds	시간 간격 동안 데이터베이스 인스턴스의 포그라운드 세션별 유휴가 아닌 대기 시간의 평균 누적 속도입니다. 평균 활성 세션의 대기 시간 구성 요소입니다. (통계: 평균, 간격: 5분)	초당 초 수

Oracle Database@AWS에 사용되는 Amazon CloudWatch 차원

다음 표의 차원을 사용하여 Oracle Database@AWS 지표 데이터를 필터링할 수 있습니다.

측정 기준	다음에 대해 요청된 데이터를 필터링합니다.
cloudVmClusterId	VM 클러스터의 식별자입니다.
cloudExadataInfrastructureId	Exadata 인프라의 식별자입니다.
collectionName	컬렉션의 이름입니다.
deploymentType	인프라 유형입니다.
diskgroupName	디스크 그룹의 이름
errorCode	오류 코드입니다.
errorSeverity	오류의 심각도입니다.
filesystemName	파일 시스템의 이름입니다.
hostName	호스트 기기의 이름입니다.
instanceName	데이터베이스 인스턴스의 이름입니다.
instanceNumber	데이터베이스 인스턴스의 인스턴스 번호입니다.
ioType	I/O 작업의 유형입니다.
jobId	작업의 고유 식별자입니다.
managedDatabaseGroupId	Managed Database Group의 식별자입니다.
managedDatabaseId	Managed Database의 식별자입니다.
memoryPool	메모리 풀의 유형입니다.
memoryType	메모리 유형입니다.

측정 기준	다음에 대해 요청된 데이터를 필터링합니다.
ociCloudVmClusterId	VM 클러스터의 OCI 식별자입니다.
ociCloudExadataInfrastructureId	Exadata 인프라의 OCI 식별자입니다.
parseType	구문 분석의 유형입니다.
resourceId	리소스의 식별자입니다.
resourceId_Database	데이터베이스의 식별자입니다.
resourceId_DbNode	데이터베이스 노드의 식별자입니다.
resourceName	리소스의 이름.
resourceName_Database	데이터베이스의 이름입니다.
resourceName_DbNode	데이터베이스 노드의 이름입니다.
resourceType	데이터베이스의 형식입니다.
schemaName	스키마의 이름입니다.
status	데이터베이스의 상태입니다.
tablespaceContents	테이블스페이스의 콘텐츠입니다.
tablespaceName	테이블스페이스의 이름입니다.
tablespaceType	테이블스페이스의 유형입니다.
transactionStatus	트랜잭션의 상태입니다.
waitClass	대기 이벤트의 클래스입니다.

Amazon EventBridge에서 Oracle Database@AWS 이벤트 모니터링

사용자는 애플리케이션 및 AWS 서비스의 실시간 데이터 스트림을 제공하는 EventBridge의 Oracle Database@AWS 이벤트를 모니터링할 수 있습니다. EventBridge는 해당 데이터를 AWS Lambda, Amazon SNS(Simple Notification Service) 등의 대상으로 라우팅합니다.

> **Note**
>
> 이전에는 EventBridge를 Amazon CloudWatch Events라고 했습니다. 자세한 내용은 Amazon EventBridge 사용 설명서의 EventBridge는 Amazon CloudWatch Events의 진화를 참조하세요.

Oracle Database@AWS 이벤트 개요

Oracle Database@AWS 이벤트는 리소스 수명 주기의 변경을 나타내는 구조화된 메시지입니다. 이벤트 버스는 이벤트를 수신하여 0개 이상의 목적지 또는 대상에 전달하는 라우터입니다. Oracle Database@AWS 이벤트는 다음 소스에서 생성될 수 있습니다.

AWS의 이벤트

이러한 이벤트는 AWS 측의 Oracle Database@AWS API에서 생성되며 AWS 계정의 기본 이벤트 버스로 전달됩니다.

OCI의 이벤트

Oracle Exadata 인프라 또는 VM 클러스터와 관련된 이벤트와 같은 이러한 이벤트는 OCI에서 직접 생성됩니다. Oracle Database@AWS를 구독하면 `aws.partner/odb/` 접두사가 있는 이벤트 버스가 AWS 계정에 생성되어 OCI에서 이벤트를 수신합니다.

AWS의 Oracle Database@AWS 이벤트

AWS의 Oracle Database@AWS 이벤트에는 생성 및 삭제 중 ODB 네트워크와 관련된 수명 주기 변경 사항이 포함됩니다. 이러한 이벤트는 AWS 계정의 기본 이벤트 버스로 전달됩니다. 전송 유형은 최선의 작업입니다.

ODB 네트워크 이벤트

Event	이벤트 ID	메시지
생성	ODB-EVENT-0001	ODB 네트워크 odbnet_ID를 성공적으로 생성함
생성 실패	ODB-EVENT-0011	ODB 네트워크 odbnet_ID 생성 실패
삭제	ODB-EVENT-0002	ODB 네트워크 odbnet_ID를 성공적으로 삭제함
삭제 실패함	ODB-EVENT-0012	ODB 네트워크 odbnet_ID를 삭제하지 못함

예: ODB 네트워크 생성 이벤트

다음 예제에서는 성공적인 ODB 네트워크 생성에 대한 이벤트를 보여줍니다.

```
{
  "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"
  }
}
```

OCI의 Oracle Database@AWS 이벤트

대부분의 이벤트는 OCI에서 직접 생성됩니다. Oracle Database@AWS는 AWS 계정에 `aws.partner/odb/` 접두사가 있는 이벤트 버스를 생성하여 OCI로부터 이벤트를 수신합니다. 이 이벤트 버스를 삭제하지 않는 것이 좋습니다.

OCI는 다음을 포함한 포괄적인 이벤트 유형을 제공합니다.

- Oracle Exadata 인프라
- VM 클러스터 이벤트
- CDB 이벤트
- PDB 이벤트

OCI가 지원하는 특정 이벤트 유형 및 세부 정보에 대한 자세한 내용은 Oracle Exadata Database Service on Dedicated Infrastructure Events 및 Events for Autonomous Database on Dedicated Exadata Infrastructure를 참조하세요.

Oracle Database@AWS 이벤트 필터링

Amazon EventBridge의 이벤트 버스에서 이벤트 버스 설정에 대한 EventBridge 권장 모범 사례를 따를 수 있습니다. 사용 사례에 따라 EventBridge 규칙을 설정하여 이벤트를 필터링하고 이벤트를 수신 및 사용할 대상을 필터링할 수 있습니다.

AWS에서 ODB 네트워크 이벤트 필터링

AWS의 ODB 네트워크 이벤트의 경우 다음 이벤트 패턴을 사용하여 필터링할 수 있습니다.

```
{
  "source": ["aws.odb"],
  "detail-type": ["ODB Network Event"]
}
```

기본 이벤트 버스와 함께 EventBridge `put-rule` API를 사용하여 이 패턴을 적용할 수 있습니다. 자세한 내용은 Amazon EventBridge API 참조의 PutRule을 참조하세요.

OCI에서 Oracle Database@AWS 이벤트 필터링

OCI의 Oracle Database@AWS 이벤트의 경우 Amazon EventBridge API 참조의 PutRule 예제와 유사한 명령을 사용하여 규칙을 설정할 수 있습니다. 다음 지침을 참고하세요.

- 필터링하려는 이벤트 유형에 따라 사용자 지정 이벤트 패턴을 사용합니다.
- EventBusName을 Oracle Database@AWS에서 생성한 버스의 이름으로 설정합니다.

이벤트를 필터링하고 계정 간에 EventBridge 대상을 설정하는 방법에 대한 자세한 내용은 Amazon EventBridge에서 AWS 계정간 이벤트 전송 및 수신을 참조하세요.

Oracle Database@AWS 이벤트 문제 해결

이벤트 전송 또는 이벤트 콘텐츠에 문제가 발생하면 다음을 수행합니다.

- ODB 네트워크 이벤트의 경우 AWS Support에 문의하세요.
- ODB 네트워크 이벤트 이외의 Oracle Database@AWS 이벤트는 Oracle Cloud Support에 문의하세요.

자세한 내용은 Oracle Database@AWS에 대한 지원 받기 섹션을 참조하세요.

Oracle Database@AWS을 사용하여 AWS CloudTrail API 직접 호출 로깅

Oracle Database@AWS는 사용자, 역할 또는 AWS 서비스가 수행한 작업의 레코드를 제공하는 서비스인 AWS CloudTrail과 통합됩니다. CloudTrail은 Oracle Database@AWS에 대한 모든 API 직접 호출을 이벤트로 캡처합니다. 캡처되는 직접 호출에는 Oracle Database@AWS 콘솔로부터의 직접 호출과 Oracle Database@AWS API 작업에 대한 코드 직접 호출이 포함됩니다. CloudTrail에서 수집한 정보를 사용하여 Oracle Database@AWS에 수행된 요청, 요청이 수행된 IP 주소, 요청이 수행된 시간, 추가 세부 정보를 확인할 수 있습니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 관한 정보가 포함됩니다. 자격 증명을 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트 사용자로 했는지 사용자 보안 인증으로 했는지 여부.
- IAM Identity Center 사용자를 대신하여 요청이 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자에 대한 임시 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부

> **Note**
>
> Oracle Database@AWS는 CloudTrail 로그에 AWS Security Token Service(STS)의 `GetCallerIdentity` API 직접 호출을 기록합니다. 이러한 STS API 직접 호출은 사용자를 대신하여 OCI와 상호 작용할 때 Oracle Database@AWS의 ID를 확인합니다. 이는 AWS 작업의 정상적이고 안전한 부분이며 민감한 정보를 노출하지 않습니다.

계정을 생성할 때 AWS 계정에서 CloudTrail이 활성 상태이며, CloudTrail 이벤트 기록에 자동으로 액세스할 수 있습니다. CloudTrail 이벤트 기록은 지난 90일 간 AWS 리전의 관리 이벤트에 대해 보기, 검색 및 다운로드가 가능하고, 수정이 불가능한 레코드를 제공합니다. 자세한 설명은 AWS CloudTrail 사용 설명서의 CloudTrail 이벤트 기록 작업을 참조하세요. 이벤트 기록 보기는 CloudTrail 요금이 부과되지 않습니다.

지난 90일 동안 AWS 계정에서 진행 중인 이벤트 기록을 보려면 추적 또는 CloudTrail Lake 이벤트 데이터 스토어를 생성합니다.

CloudTrail 추적

CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. AWS Management Console을 사용하여 만든 추적은 모두 다중 리전입니다. AWS CLI를 사용하여 단일 리전 또는 다중 리전 추적을 생성할 수 있습니다. 계정의 모든 AWS 리전에서 활동을 캡처하므로, 다중 리전 추적 생성이 권장됩니다. 단일 리전 추적을 생성하는 경우 추적의 AWS 리전에 로깅된 이벤트만 볼 수 있습니다. 추적에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 AWS 계정에 대한 추적 생성 및 조직에 대한 추적 생성을 참조하세요.

CloudTrail에서 추적을 생성하여 진행 중인 관리 이벤트의 사본 하나를 Amazon S3 버킷으로 무료로 전송할 수는 있지만, Amazon S3 스토리지 요금이 부과됩니다. CloudTrail 요금에 관한 자세한 내용은 AWS CloudTrail 요금을 참조하세요. Amazon S3 요금에 관한 자세한 내용은 Amazon S3 요금을 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어

CloudTrail Lake를 사용하면 이벤트에 대해 SQL 기반 쿼리를 실행할 수 있습니다. CloudTrail Lake는 행 기반 JSON 형식의 기존 이벤트를 Apache ORC 형식으로 변환합니다. ORC는 빠른 데이터 검색에 최적화된 열 기반 스토리지 형식입니다. 이벤트는 이벤트 데이터 스토어로 집계되며, 이벤트 데이터 스토어는 고급 이벤트 선택기를 적용하여 선택한 기준을 기반으로 하는 변경 불가능한 이벤트 컬렉션입니다. 이벤트 데이터 스토어에 적용하는 선택기는 어떤 이벤트가 지속되고 쿼리에 사용 가능한지를 제어합니다. CloudTrail Lake에 관한 자세한 내용은 AWS CloudTrail 사용 설명서의 AWS CloudTrail Lake 작업을 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어 및 쿼리에는 비용이 발생합니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 요금에 관한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

CloudTrail의 Oracle Database@AWS 관리 이벤트

관리 이벤트는 AWS 계정의 리소스에 대해 수행되는 관리 작업에 관한 정보를 제공합니다. 이를 컨트롤 플레인 작업이라고도 합니다. 기본적으로 CloudTrail은 관리 이벤트를 로깅합니다.

Oracle Database@AWS는 모든 Oracle Database@AWS 컨트롤 플레인 작업을 관리 이벤트로 로깅합니다.

Oracle Database@AWS 이벤트 예제

이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청된 API 작업, 작업 날짜와 시간, 요청 파라미터 등에 관한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 추적이 아니므로 이벤트가 특정 순서로 표시되지 않습니다.

다음 예제는 `CreateOdbNetwork` 작업을 시연하는 CloudTrail 이벤트를 보여줍니다.


```
{
    "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 레코드 콘텐츠에 관한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 레코드 콘텐츠를 참조하세요.

Oracle Database@AWS 문제 해결

다음 섹션을 사용하여 Oracle Database@AWS에서 발생할 수 있는 네트워킹 문제를 해결할 수 있습니다.

주제

- ODB 네트워크 생성 실패
- VPC와 ODB 네트워크 또는 VM 클러스터 간의 연결 문제
- VPC에서 VM 클러스터의 확인할 수 없는 호스트 이름 또는 스캔 이름
- Oracle Database@AWS에 대한 지원 받기

ODB 네트워크 생성 실패

ODB 네트워크를 생성할 수 없는 경우 일반적인 원인은 다음과 같습니다.

제한된 CIDR 범위

ODB 네트워크는 클라이언트 및 백업 서브넷에 대해 특정 CIDR 범위를 사용합니다. 이러한 서브넷에 대해 선택한 CIDR 범위가 제한되거나 예약된 IP 주소 범위와 겹치지 않는지 확인합니다.

다음 CIDR 범위는 예약되어 있으며 ODB 네트워크에 사용할 수 없습니다.

- Oracle 클라우드 예약 범위: 169.254.0.0/16
- 예약 클래스 D: 224.0.0.0 - 239.255.255.255
- 예약 클래스 E: 240.0.0.0 - 255.255.255.255
- 향후 OCI 사용: 100.105.0.0/16

VPC 설명서에 설명된 CIDR 범위에 대한 EC2 규칙을 따릅니다. 자세한 내용은 CIDR 블록 연결 제한을 참조하세요.

또한 지정된 CIDR 범위와 ODB 네트워크에 대한 VPC 연결에 사용되는 범위 간의 중복을 방지합니다.

중첩 VPC CIDR

ODB 네트워크에 대해 지정한 CIDR 범위는 기존 VPC에서 사용하는 CIDR 범위와 겹치지 않아야 합니다. CIDR 범위가 겹치면 라우팅 충돌이 발생하여 ODB 네트워크가 성공적으로 생성되지 않을

수 있습니다. ODB 피어링 VPC의 CIDR 범위를 확인하고 ODB 네트워크 CIDR이 고유하고 중복되지 않는지 확인합니다.

VPC 소유권

연결하려는 ODB 네트워크와 VPC는 동일한 AWS 계정이 소유해야 합니다. ODB 네트워크를 다른 계정이 소유한 VPC에 피어링하려고 하면 생성이 실패합니다. ODB 네트워크와 VPC를 모두 동일한 AWS 계정에서 소유하고 있는지 확인합니다.

전송 게이트웨이 부족

전송 게이트웨이를 VPC에 연결하지 않고 ODB 네트워크 피어링된 CIDR 목록에 CIDR 범위를 추가하면 생성 또는 업데이트 작업이 실패합니다. 연결이 사용되는 CIDR 범위에 대한 요구 사항은 없습니다.

VPC와 ODB 네트워크 또는 VM 클러스터 간의 연결 문제

VPC에서 ODB 네트워크 또는 ODB 네트워크 내의 VM 클러스터에 연결할 수 없는 경우 일반적인 원인은 다음과 같습니다.

- VPC 구성 확인 - Oracle Database@AWS 콘솔에서 ODB 네트워크와 피어링된 VPC를 찾습니다. VPC ID가 ODB 네트워크 세부 정보에 표시된 것과 일치하는지 확인합니다.
- 라우팅 테이블 검사 - Amazon VPC 콘솔에서 애플리케이션이 실행 중인 서브넷에 연결된 라우팅 테이블을 찾습니다. ODB 네트워크의 클라이언트 서브넷 CIDR과 일치하는 대상 CIDR이 있는 경로를 확인합니다. 이 라우팅이 올바른 ODB 네트워크 ARN을 가리키는지 확인합니다. 경로가 누락된 경우 ODB 네트워크의 클라이언트 서브넷 CIDR에 새 경로를 추가합니다.
- 피어링된 CIDR 검증 - ODB 네트워크 세부 정보의 `Peered CIDRs` 섹션을 검토합니다. VPC의 모든 관련 CIDR 블록이 나열되었는지 확인합니다. 필수 CIDR이 누락된 경우 피어링된 CIDR을 업데이트합니다.
- 보안 그룹 규칙 확인 - Amazon EC2 콘솔에서 VPC의 리소스에 대한 보안 그룹을 찾습니다. 인바운드 및 아웃바운드 규칙을 검토하고 필요한 트래픽을 허용하도록 필요에 따라 업데이트합니다.
- 가용 영역(AZ) 확인 - Amazon VPC 콘솔에서 서브넷의 가용 영역(AZ)을 식별합니다. ODB 네트워크도 서브넷과 동일한 AZ에 배포되었는지 확인합니다.
- 여러 ODB 네트워크 피어링 연결 방지 - Oracle Database@AWS 콘솔에서 VPC 피어링 연결을 확인합니다. ODB 네트워크에 대한 활성 연결이 하나뿐인지 확인합니다. ODB 네트워크 피어링이 두 개 이상 표시되면 추가 ODB 네트워크 피어링을 제거합니다.

VPC에서 VM 클러스터의 확인할 수 없는 호스트 이름 또는 스캔 이름

VPC에서 VM 클러스터의 호스트 이름 또는 스캔 이름을 확인할 수 없는 경우 VPC 및 다음 리소스에서 DNS 전달을 구성하여 ODB 네트워크에서 호스팅되는 DNS 레코드를 확인합니다.

- ODB 네트워크에 DNS 쿼리를 전송하는 아웃바운드 엔드포인트입니다. 자세한 내용은 Oracle Database@AWS의 ODB 네트워크에서 아웃바운드 엔드포인트 구성 섹션을 참조하세요.
- 해석기가 ODB 네트워크용 DNS로 전달하는 DNS 쿼리의 도메인 이름을 지정하는 해석기 규칙입니다. 자세한 내용은 Oracle Database@AWS에서 해석기 규칙 구성 섹션을 참조하세요.

Oracle Database@AWS에 대한 지원 받기

Oracle Database@AWS에 대한 정보와 지원을 받는 방법을 알아봅니다.

Oracle 지원 범위 및 연락처 정보

Oracle Cloud Support는 모든 Oracle Database@AWS 질문에 대한 1차 지원 라인입니다. 지원팀에 문의하려면 Oracle Cloud Infrastructure(OCI) 콘솔에 로그인한 다음 구명 보트 아이콘을 선택합니다. My Oracle Cloud Support 계정이 없는 경우 My Oracle Cloud Support 계정 및 액세스 섹션을 참조하세요.

Oracle Support에서 도움이 될 수 있는 문제의 예는 다음과 같습니다.

- 데이터베이스 연결 문제(Oracle TNS)
- Oracle Database 성능 문제
- Oracle Database 오류 해결
- 서비스와 연결된 OCI 테넌시와의 통신과 관련된 네트워킹 문제
- 더 많은 용량을 받기 위한 할당량(한도) 증가(자세한 내용은 데이터베이스 리소스에 대한 한도 증가 요청 참조)
- Oracle Database 인프라에 더 많은 컴퓨팅 및 스토리지 용량을 추가하기 위한 규모 조정
- 차세대 하드웨어 업그레이드
- AWS Marketplace 요금과 관련된 결제 문제

OCI 콘솔 외부에서 Oracle Support에 문의해야 하는 경우 Oracle Database@AWS와 관련된 문제임을 Oracle Support 에이전트에게 알립니다. 이는 이 서비스에 대한 요청이 이러한 배포를 전문으로 하는 OCI 지원 팀에서 처리되기 때문입니다.

전화로 Oracle Support에 문의

1. 1-800-223-1711로 전화하세요. 미국 외부에 있는 경우 Oracle Support 연락처 글로벌 디렉터리를 방문하여 해당 국가 또는 리전의 연락처 정보를 찾아보세요.
2. 옵션 "2"를 선택하여 새 서비스 요청(SR)을 엽니다.
3. "확실하지 않음"의 경우 옵션 "4"를 선택합니다.
4. 에이전트에게 멀티 클라우드 시스템과 제품 이름에 문제가 있음을 알립니다. 사용자를 대신하여 내부 서비스 요청이 열리고 OCI 지원 엔지니어가 직접 연락을 드릴 것입니다.

Oracle의 Cloud Customer Connect 커뮤니티의 멀티 클라우드 포럼에 질문을 제출할 수도 있습니다. 모든 고객이 이 옵션을 사용할 수 있습니다.

My Oracle Cloud Support 계정 및 액세스

My Oracle Cloud Support 서비스 요청 티켓을 생성하려면 조직의 Oracle Database@AWS 서비스 관리자가 요청을 승인해야 합니다. Oracle Database@AWS 관리자인 경우 Oracle Database@AWS 서비스 활성화 이메일에 포함된 My Oracle Cloud Support 온보딩 지침을 완료합니다.

다음 주제에서 My Oracle Cloud Support를 통한 온보딩 지침을 확인할 수 있습니다.

- Oracle 지원 계정 구성
- 지원 요청 생성

사용자를 승인하여 My Oracle Cloud Support 지원 요청을 여는 방법에 대한 지침은 Administrator Tasks for Support를 참조하세요.

AWS Support 범위 및 연락처 정보

AWS Support는 모든 AWS 관련 문제 및 질문에 대한 1차 지원 라인입니다. 다른 AWS 서비스와 마찬가지로 문제에 대한 AWS Support 사례를 생성합니다. AWS Support 팀은 필요에 따라 OCI Support와 협업합니다.

AWS Support가 도움을 줄 수 있는 Oracle Database@AWS 문제의 예는 다음과 같습니다.

- 네트워크 주소 변환(NAT), 방화벽, DNS 및 트래픽 관리, AWS 서브넷과 관련된 문제를 포함한 가상 네트워킹 문제
- 데이터베이스 호스트 연결, 소프트웨어 설치, 지연 시간 및 호스트 성능을 포함한 배스천 및 가상 머신(VM) 문제
- Amazon CloudWatch 내의 Exadata VM 클러스터 지표 보고
- AWS 서비스와 관련된 결제 문제

AWS Support에 대한 자세한 내용은 AWS Support 시작하기를 참조하세요.

Oracle 서비스 수준 계약

Oracle Database@AWS 서비스 수준 계약(SLA)에 대한 질문이 있거나 SLA 위반에 대한 서비스 크레딧을 요청하려면 Oracle 계정 관리자에게 문의하세요. 자세한 내용은 서비스 수준 계약을 참조하세요.

Oracle Database@AWS 할당량

Oracle Database@AWS는 멀티 클라우드 상품입니다. AWS는 Oracle Database@AWS 리소스에 대한 할당량을 설정하거나 적용하지 않습니다. 할당량은 Oracle Cloud Infrastructure(OCI)에서 적용됩니다. OCI 할당량에 대한 자세한 내용은 Oracle Cloud Infrastructure 설명서의 할당량 및 서비스 제한을 참조하세요.

Oracle Database@AWS 사용 설명서 기록

다음 표에서는 Oracle Database@AWS에 대한 문서 릴리스를 설명합니다.

변경 사항	설명	날짜
Oracle Database@AWS는 아시아 태평양(시드니) 리전 및 캐나다(중부) 리전을 지원합니다	이러한 리전에서 Oracle Database@AWS 리소스를 생성할 수 있습니다. 자세한 내용은 Oracle Database@AWS의 지원되는 리전을 참조하세요.	2026년 2월 2일
Oracle Database@AWS는 아시아 태평양(도쿄) 리전, 미국 동부(오하이오) 리전, 유럽(프랑크푸르트) 리전을 지원합니다.	이러한 리전에서 Oracle Database@AWS 리소스를 생성할 수 있습니다. 자세한 내용은 Oracle Database@AWS의 지원되는 리전을 참조하세요.	2025년 12월 22일
Oracle Database@AWS는 AWS 계정에서 권한 공유를 지원합니다	이제 AWS License Manager를 사용하여 동일한 AWS 조직의 AWS 계정에서 Oracle Database@AWS에 대한 AWS Marketplace 권한을 공유할 수 있습니다. 자세한 내용은 Oracle Database@AWS의 권한 공유를 참조하세요.	2025년 12월 19일
Oracle Database@AWS는 제로 ETL 통합 데이터 필터 수정을 지원합니다	Oracle Database@AWS는 Amazon Redshift와의 기존 제로 ETL 통합을 위한 데이터 필터 수정을 지원합니다. 데이터 필터 패턴을 업데이트하여 데이터 복제에서 지정된 스키마 및 테이블을 포함하거나 제외할 수 있습니다. 자세한 내용은 제로 ETL 통합 관리를 참조하세요.	2025년 10월 15일

Oracle Database@AWS는 피어링 연결을 위한 피어 네트워크 CIDR 관리를 지원합니다	ODB 피어링 연결을 생성하거나 업데이트할 때 피어 네트워크 CIDR을 지정할 수 있습니다. 피어 VPC에서 ODB 네트워크에 액세스할 수 있는 서브넷을 제어합니다. VPC 계정은 ODB 네트워크를 소유하지 않고도 CIDR 범위를 업데이트할 수 있습니다. 자세한 내용은 Oracle Database@AWS의 Amazon VPC에 대한 ODB 피어링 구성을 참조하세요.	2025년 10월 10일
Oracle Database@AWS는 Amazon Redshift와의 제로 ETL 통합을 지원합니다	Oracle Database@AWS가 이제 VPC Lattice와 통합되어 Amazon Redshift와의 제로 ETL 통합을 활성화합니다. 자세한 내용은 Oracle Database@AWS에 대한 서비스 통합을 참조하세요.	2025년 7월 2일
IAM 서비스 연결 역할 권한 업데이트	이제 `AmazonODBServiceRolePolicy` 정책은 VPC Transit Gateway Attachment를 설명하고, Amazon EC2 서브넷을 설명하고, Amazon EventBridge 소스를 활성화할 수 있는 추가 권한을 부여합니다. 자세한 내용은 AWS 관리형 정책에 대한 Oracle Database@AWS 업데이트를 참조하세요.	2025년 6월 30일

IAM 서비스 연결 역할 권한 업데이트	이제 `AmazonODBServiceRolePolicy` 정책은 Amazon EventBridge Scheduler의 이벤트를 설명하고 이벤트 버스를 생성하거나 설명할 수 있는 추가 권한을 부여합니다. 자세한 내용은 AWS 관리형 정책에 대한 Oracle Database@AWS 업데이트를 참조하세요.	2025년 6월 26일
Oracle Database@AWS는 미국 서부(오리건) 리전을 지원합니다	미국 서부(오리건) 리전에서 Oracle Database@AWS 리소스를 생성할 수 있습니다. 지원되는 물리적 AZ ID는 `usw2-az3` 및 `usw2-az4`입니다. 자세한 내용은 Oracle Database@AWS의 지원되는 리전을 참조하세요.	2025년 6월 26일
Oracle Database@AWS는 AWS 계정에서 리소스 공유를 지원합니다	이제 AWS Resource Access Manager(AWS RAM)를 사용하여 Exadata 인프라 및 VM 클러스터를 조직 내 다른 AWS 계정와 공유할 수 있습니다. 인프라를 한 번 프로비저닝하고 여러 계정에서 공유하여 비용을 절감하는 동시에 책임을 분리할 수 있습니다. 자세한 내용은 Oracle Database@AWS의 리소스 공유를 참조하세요.	2025년 6월 26일

Oracle Database@AWS는 Amazon EventBridge의 이벤트를 지원합니다	Oracle Database@AWS는 리소스 수명 주기 변경을 모니터링하기 위해 Amazon EventBridge에 이벤트를 전송합니다. 이벤트는 AWS 및 OCI 소스 모두에서 생성되므로 ODB 네트워크, Exadata 인프라, VM 클러스터 및 데이터베이스에 대한 변경 사항을 추적할 수 있습니다. 자세한 내용은 Amazon EventBridge에서 Oracle Database@AWS 이벤트 모니터링을 참조하세요.	2025년 6월 26일
Oracle Database@AWS는 리전 간 구독을 지원합니다	Oracle Database@AWS는 리전 간 구독을 지원하므로 한 번 구독하고 사용 가능한 모든 AWS 리전에서 서비스를 사용할 수 있습니다. 자세한 내용은 여러 리전에서 Oracle Database@AWS 구독을 참조하세요.	2025년 6월 26일
Oracle Database@AWS는 ODB 피어링 연결을 별도의 리소스로 지원합니다	이제 ODB 피어링 연결은 피어링 연결을 생성, 보기 및 삭제하기 위한 전용 API가 있는 별도의 리소스입니다. ODB 네트워크와 동일한 계정 또는 다른 계정의 Amazon VPC 간에 피어링 연결을 생성할 수 있습니다. 자세한 내용은 ODB 피어링 연결로 작업하기 섹션을 참조하세요.	2025년 6월 26일

Oracle Database@AWS는 ODB 네트워크를 Amazon S3와 통합합니다	Oracle Database@AWS는 이제 VPC Lattice와 통합되어 Amazon S3에 대한 Oracle 관리형 백업을 활성화하고 Amazon S3에 대한 ODB 네트워크 액세스를 지시합니다. 자세한 내용은 Oracle Database@AWS에 대한 서비스 통합을 참조하세요.	2025년 6월 26일
Oracle Database@AWS는 Autonomous VM 클러스터를 지원합니다	이제 Exadata 인프라에서 Autonomous VM 클러스터를 생성할 수 있습니다. Autonomous VM 클러스터는 기계 학습 및 AI를 사용하여 키 관리 작업을 자동화하는 완전 관리형 데이터베이스입니다. 자세한 내용은 3단계: Oracle Database@AWS에서 Exadata VM 클러스터 또는 Autonomous VM 클러스터 생성을 참조하세요.	2025년 5월 28일
Oracle Database@AWS는 사용자 지정 가능한 유지 관리 기간을 지원합니다	이제 Oracle 관리형 또는 고객 관리형 일정 옵션을 사용하여 Exadata 인프라에 대한 유지 관리 기간을 구성할 수 있습니다. 패치 모드(롤링 또는 비롤링)를 선택하고 유지 관리 타이밍 기본 설정을 지정할 수도 있습니다. 자세한 내용은 Oracle Database@AWS에서 Oracle Exadata 인프라 생성을 참조하세요.	2025년 5월 1일

Oracle Database@AWS는 새 가용 영역(AZ)을 지원합니다	이제 물리적 ID `use1-az4` 또는 `use1-az6`를 사용하여 AZ에서 ODB 네트워크를 생성할 수 있습니다. 자세한 내용은 Oracle Exadata 인프라를 참조하세요.	2025년 3월 26일
Oracle Database@AWS는 Amazon VPC Transit Gateway를 지원합니다	전송 게이트웨이를 ODB 네트워크에 피어링된 VPC에 연결하는 경우 여러 VPC를 이 게이트웨이에 연결할 수 있습니다. 이러한 VPC에서 실행되는 애플리케이션은 ODB 네트워크에서 실행되는 Exadata VM 클러스터에 액세스할 수 있습니다. 자세한 내용은 Oracle Database@AWS에 대한 Amazon VPC Transit Gateway 구성을 참조하세요.	2025년 3월 26일
Oracle Database@AWS는 Exadata X11M에 대한 데이터베이스 및 스토리지 서버 유형을 지원합니다	Exadata X11M을 사용하여 인프라를 생성할 때 데이터베이스 서버 유형과 스토리지 서버 유형을 지정할 수 있습니다. 자세한 내용은 Oracle Database@AWS에서 Oracle Exadata 인프라 생성을 참조하세요.	2025년 2월 4일
새로운 서비스 연결 역할 정책	Oracle Database@AWS는 `AWSServiceRoleForODB` 서비스 연결 역할에 대한 새 정책 `AmazonODBServiceRolePolicy` 를 추가했습니다. 자세한 내용은 AWS 관리형 정책에 대한 Oracle Database@AWS 업데이트를 참조하세요.	2024년 12월 2일

최초 릴리스입니다.	Oracle Database@AWS 사용 설명서의 최초 릴리스입니다.	2024년 12월 2일