Oracle Database@AWS Benutzerleitfaden

Oracle Database@AWS

Oracle Database@AWS: Oracle Database@AWS Benutzerleitfaden

Table of Contents

Was ist Oracle Database@AWS? 1
Features 1
Zugehörige Services 2
Zugriff 3
Preisgestaltung 3
Als nächstes 4
Funktionsweise 5
Untergeordnete OCI-Sites 5
Oracle Exadata-Infrastruktur 6
ODB-Netzwerk 6
Virtual Private Cloud (VPC) 8
ODB-Peering 8
Erstellung einer ODB-Peering-Verbindung 9
AWS Service-Integrationen 10
Weiterleitung von Datenverkehr von mehreren VPCs 11
AWS Transit Gateway 11
AWS Cloud-WAN 11
Exadata-VM-Cluster 12
Autonome VM-Cluster 12
Oracle Exadata-Datenbanken 13
Onboarding 14
Melden Sie sich an für ein AWS-Konto 14
Erstellen eines Benutzers mit Administratorzugriff 14
Fordern Sie ein privates Angebot an 16
Abonnieren Sie in mehreren Regionen 17
Erste Schritte 19
Voraussetzungen 19
Unterstützte OCI-Dienste 19
Unterstützte Regionen 20
Planung des IP-Adressraums 21
Einschränkungen für IP-Adressen im ODB-Netzwerk 21
CIDR-Anforderungen für das Client-Subnetz 22
CIDR-Anforderungen für Backup-Subnetze 23
IP-Verbrauchsszenarien 23

Schritt 1: Erstellen Sie ein ODB-Netzwerk ... 25
Schritt 2: Erstellen Sie eine Oracle Exadata-Infrastruktur ... 27
Schritt 3: Erstellen Sie einen VM-Cluster ... 29
Schritt 4: Erstellen Sie Oracle Exadata-Datenbanken ... 34
ODB-Peering ... 35
ODB-Peering einrichten ... 35
ODB-Peering wird aktualisiert ... 37
Konfiguration von VPC-Routentabellen für ODB-Peering ... 38
DNS konfigurieren ... 39
Wie funktioniert DNS in Oracle Database@AWS ... 39
Konfiguration eines ausgehenden Endpunkts ... 40
Konfiguration einer Resolver-Regel ... 41
Testen Sie Ihre DNS-Konfiguration ... 43
Konfiguration von Amazon VPC Transit Gateways für Oracle Database@AWS ... 44
Voraussetzungen ... 44
Einschränkungen ... 45
Einrichtung und Konfiguration eines Transit-Gateways ... 45
Konfiguration von AWS Cloud WAN für Oracle Database@AWS ... 46
Teilung von Ansprüchen ... 49
Freigabemethoden ... 49
Teilen von Rechten mit AWS License Manager ... 49
Gemeinsame Nutzung von Ressourcen mit AWS Resource Access Manager ()AWS RAM ... 49
Einschränkungen ... 50
Rechte kontenübergreifend teilen ... 50
Voraussetzungen für die gemeinsame Nutzung von Berechtigungen ... 50
Für die gemeinsame Nutzung von Ansprüchen sind Berechtigungen erforderlich ... 51
Rechte teilen ... 51
Freigabe von Ressourcen ... 52
AWS RAM Integration ... 52
Vorteile ... 53
Wie funktioniert die gemeinsame Nutzung von Ressourcen ... 53
Berechtigungen für gemeinsam genutzte Ressourcen ... 54
Einschränkungen ... 55
Einschränkungen beim Teilen von Ressourcen ... 55
Einschränkungen bei der Erstellung und Verwendung gemeinsam genutzter Ressourcen ... 56
Einschränkungen beim Löschen gemeinsam genutzter Ressourcen ... 56

Ressourcen über Konten hinweg teilen ... 57
Voraussetzungen für die gemeinsame Nutzung von Ressourcen ... 57
Freigabe von Ressourcen ... 58
Ihre Ressourcenfreigaben anzeigen ... 59
Ressourcenfreigaben aktualisieren oder löschen ... 60
Der Dienst wird initialisiert ... 60
Was ist Dienstinitialisierung? ... 61
Nächste Schritte ... 62
Arbeiten mit gemeinsam genutzten Ressourcen in einem vertrauenswürdigen Konto ... 62
Einschränkungen in einem vertrauenswürdigen Konto ... 63
VM-Cluster erstellen ... 64
Geteilte Ressourcen anzeigen ... 65
ODB-Peering mit gemeinsam genutzten ODB-Netzwerken einrichten ... 66
Verwalten ... 68
Aktualisierung eines ODB-Netzwerks ... 68
Löschen eines ODB-Netzwerks ... 69
Löschen eines VM-Clusters ... 69
Löschen einer Exadata-Infrastruktur ... 70
Löschen einer ODB-Peering-Verbindung ... 70
Sicherung erstellen ... 72
Von Oracle verwaltete Backups ... 72
Benutzerverwaltete Backups ... 72
Voraussetzungen ... 73
Oracle Secure Backup ... 76
Storage Gateway ... 77
S3-Bereitstellungspunkt ... 79
Deaktivierung des Zugriffs auf S3 ... 82
Fehlerbehebung bei der Amazon S3 S3-Integration ... 82
Zero-ETL-Integration mit Redshift ... 84
Unterstützte Datenbankversionen ... 84
Funktionsweise ... 85
Voraussetzungen ... 85
Allgemeine Voraussetzungen ... 86
Voraussetzungen für die Datenbank ... 86
Überlegungen ... 90
Einschränkungen ... 91

Einrichtung ... 92
Schritt 1: Aktivieren Sie Zero-ETL für Ihr ODB-Netzwerk ... 93
Schritt 2: Konfigurieren Sie Ihre Oracle-Datenbank ... 93
Schritt 3: AWS Secrets Manager und AWS Key Management Service einrichten ... 94
Schritt 4: IAM-Berechtigungen konfigurieren ... 96
Schritt 5: Amazon Redshift Redshift-Ressourcenrichtlinien konfigurieren ... 99
Schritt 6: Erstellen Sie die Zero-ETL-Integration mit AWS Glue ... 100
Schritt 7: Erstellen Sie eine Zieldatenbank in Amazon Redshift ... 101
Überprüfen Sie die Zero-ETL-Integration ... 102
Datenfilterung ... 102
Überwachen ... 103
Überwachung des Integrationsstatus ... 103
Überwachung der Leistung ... 104
Verwalten ... 104
Ändern von Null-ETL-Integrationen ... 104
Löschen von Null-ETL-Integrationen ... 106
Best Practices ... 108
Fehlerbehebung ... 110
Fehler bei der Einrichtung der Integration ... 110
Probleme bei der Replikation ... 111
Probleme mit der Datenkonsistenz ... 111
Überwachung und Debugging ... 112
Sicherheit ... 113
Datenschutz ... 114
Datenverschlüsselung ... 115
Verschlüsselung während der Übertragung ... 115
Schlüsselverwaltung ... 116
Identity and Access Management ... 116
Zielgruppe ... 116
Authentifizierung mit Identitäten ... 117
Verwalten des Zugriffs mit Richtlinien ... 118
Wie Oracle Database@AWS funktioniert mit IAM ... 120
Identitätsbasierte Richtlinien ... 126
AWS verwaltete Richtlinien ... 131
Oracle Database@AWS Authentifizierung und Autorisierung in OCI ... 132
Fehlerbehebung ... 132

Compliance-Validierung 134
Ausfallsicherheit 134
Service-verknüpfte Rollen 135
Dienstbezogene Rollenberechtigungen für Oracle Database@AWS 135
Unterstützte Regionen für Oracle Database@AWS serviceverknüpfte Rollen 138
Richtlinienaktualisierungen 138
Überwachen 141
Überwachung mit CloudWatch 142
CloudWatch Metriken 142
CloudWatch Abmessungen 157
Überwachung von Ereignissen 159
Überblick der Ereignisse 160
Ereignisse von AWS 160
Ereignisse von OCI 161
Filtern von Ereignissen 162
Fehlerbehebung bei Oracle Database@AWS Ereignissen 162
CloudTrail protokolliert 163
Oracle Database@AWS Management-Ereignisse in CloudTrail 165
Oracle Database@AWS Beispiele für Ereignisse 165
Fehlerbehebung 167
Das ODB-Netzwerk kann nicht erstellt werden 167
Behebung von Verbindungsproblemen zwischen Ihrer VPC und Ihrem ODB-Netzwerk oder Ihren VM-Clustern 168
Unauflösbare Hostnamen oder Scannamen von VM-Clustern aus VPC 169
Unterstützung für Oracle Database@ erhalten AWS 169
Umfang und Kontaktinformationen des Oracle-Supports 169
Meine Oracle Cloud Support-Konten und mein Zugriff 170
AWS Support Umfang und Kontaktinformationen 171
Service Level Agreements von Oracle 171
Kontingente 172
Dokumentverlauf 173
..... clxxxii

Was ist Oracle Database@AWS?

Oracle Database@AWS ist ein Angebot, das Ihnen den Zugriff auf die von Oracle Cloud Infrastructure (OCI) verwaltete Oracle Exadata-Infrastruktur innerhalb AWS von Rechenzentren ermöglicht. Sie können Ihre Oracle Exadata-Workloads migrieren, Verbindungen mit niedriger Latenz für Anwendungen einrichten, auf denen sie ausgeführt werden, und Services integrieren. AWS AWS Sie erhalten eine einzige Rechnung AWS Marketplace, die auf AWS Verpflichtungen und Oracle Support-Prämien angerechnet wird.

Das folgende Diagramm zeigt einen allgemeinen Überblick über eine OCI-Region, die an ein AWS Rechenzentrum gebunden ist, das die Oracle Exadata-Infrastruktur hostet. Innerhalb einer AWS Availability Zone (AZ) können Sie eine Amazon VPC per Peering mit einem privaten Netzwerk verbinden, das mit dem Rechenzentrum verbunden ist. Durch das Peering dieser Netzwerke können Anwendungsserver in der VPC auf Oracle-Datenbanken zugreifen, die auf der Oracle Exadata-Infrastruktur ausgeführt werden.

Funktionen von Oracle Database@AWS

Mit Oracle Database@AWS profitieren Sie von den folgenden Funktionen:

Migration von Oracle Exadata-Datenbank-Workloads zu AWS

Mit Oracle Database@AWS können Sie Ihre Oracle Exadata-Workloads ganz einfach zu Oracle Exadata Database Service on Dedicated Infrastructure oder Oracle Autonomous Database on Dedicated Exadata Infrastructure innerhalb migrieren. AWS Die Migration bietet minimale Änderungen, volle Funktionsverfügbarkeit, Architekturkompatibilität und dieselbe Leistung wie Exadata-Bereitstellungen vor Ort. Sie können Standard-Oracle-Datenbankmigrationstools wie Recovery Manager (RMAN), Oracle Data Guard, transportable Tablespaces, Oracle Data Pump, Oracle, AWS Database Migration Service und Oracle GoldenGate Zero Downtime Migration verwenden.

Reduzierte Anwendungslatenz

Sie können eine Konnektivität mit niedriger Latenz zwischen Oracle Exadata und Anwendungen einrichten, auf denen sie ausgeführt werden. AWS Die Nähe zu den gehosteten Anwendungen AWS gewährleistet minimale Netzwerkverzögerungen und eine verbesserte Leistung.

Innovation durch Datenvereinheitlichung

Sie können tiefere Einblicke gewinnen und neue Innovationen entwickeln, indem Sie Zero-ETL-Integrationen verwenden, um Ihre Daten in Oracle zu vereinheitlichen und AWS für Analysen, maschinelles Lernen und generative KI zu nutzen. Mit der Zero-ETL-Integration mit Amazon Redshift können Sie Analysen und maschinelles Lernen (ML) für Transaktionsdaten, die in gespeichert sind, nahezu in Echtzeit durchführen. Oracle Database@AWS

Vereinfachtes Management und vereinfachter Betrieb

Sie können von einer einheitlichen Erfahrung zwischen Oracle und der Zusammenarbeit AWS bei Support, Einkauf, Management und Betrieb profitieren. Ihre Nutzung der Oracle Database-Dienste berechtigt zu Ihren bestehenden AWS Verpflichtungen und Oracle-Lizenzvorteilen, wie z. B. Oracle Support Rewards. Sie können vertraute AWS Tools und Benutzeroberflächen verwenden, um Ihre Oracle Database@AWS Ressourcen zu erwerben, bereitzustellen und zu verwalten. Sie können Ihre Ressourcen mithilfe von AWS APIs CLI oder bereitstellen und verwalten SDKs. AWS APIs Rufen Sie die entsprechende OCI auf, die für die Bereitstellung und Verwaltung der Ressourcen APIs erforderlich ist.

Nahtlose Integration mit Diensten AWS

Sie können andere AWS Dienste und Anwendungen integrieren, die in derselben Umgebung ausgeführt werden. Oracle Database@AWS Integriert sich beispielsweise in Amazon EC2, Amazon VPC und IAM. Sie können auch AWS Dienste wie Amazon CloudWatch für die Überwachung und Amazon EventBridge für das Eventmanagement integrieren Oracle Database@AWS . Für Datenbank-Backups können Sie Amazon S3 verwenden, das auf eine Haltbarkeit von mehr als 11 9 Sekunden ausgelegt ist.

Verwandt AWS-Services

Oracle Database@AWS arbeitet mit den folgenden Diensten zusammen, um die Verfügbarkeit und Skalierbarkeit Ihrer Oracle-Datenbankanwendungen zu verbessern:

- Amazon EC2 — Stellt virtuelle Server bereit, die als Oracle-Anwendungsserver fungieren. Sie können Ihren Load Balancer so konfigurieren, dass er den Datenverkehr an Ihre EC2 Anwendungsserver weiterleitet. Weitere Informationen finden Sie im EC2 Amazon-Benutzerhandbuch.
- Amazon Virtual Private Cloud (VPC) — Ermöglicht es Ihnen, AWS Ressourcen in einem logisch isolierten virtuellen Netzwerk zu starten, das Sie definiert haben. Die Oracle Exadata-Infrastruktur

befindet sich in einem speziellen Netzwerk, dem sogenannten ODB-Netzwerk, das Sie per Peering mit einer VPC verbinden können. Sie können dann Anwendungsserver in Ihrer VPC ausführen und auf Ihre Exadata-Datenbanken zugreifen. Weitere Informationen finden Sie im Amazon VPC-Benutzerhandbuch.

- Amazon VPC Lattice — Bietet systemeigenen Zugriff auf AWS Services wie Amazon S3 und von Oracle verwaltete Backups aus dem ODB-Netzwerk. Weitere Informationen finden Sie unter Was ist Amazon VPC Lattice? .
- Amazon CloudWatch — Bietet einen Überwachungsservice für Oracle Database@AWS. OCI sammelt metrische Daten über Ihr Oracle Exadata-System und sendet sie an. CloudWatch Weitere Informationen finden Sie unter Überwachung Oracle Database@AWS mit Amazon CloudWatch.
- AWS Identity and Access Management (IAM) — Hilft Ihnen, den Zugriff Ihrer Benutzer auf Ressourcen sicher zu Oracle Database@AWS kontrollieren. Verwenden Sie IAM, um zu kontrollieren, wer Ihre AWS Ressourcen nutzen kann (Authentifizierung) und welche Ressourcen Benutzer auf welche Weise verwenden können (Autorisierung). Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Oracle Database@AWS.
- AWS Analysedienste — Stellen Sie eine breite und kostengünstige Palette von Analysediensten bereit, mit denen Sie schneller Erkenntnisse aus Ihrer Exadata-Datenbank gewinnen können. Jeder Service wurde speziell für eine Vielzahl von Analyse-Anwendungsfällen wie interaktive Analysen, Big-Data-Verarbeitung, Data Warehousing, Echtzeitanalysen, Betriebsanalysen, Dashboards und Visualisierungen entwickelt. Weitere Informationen finden Sie unter Analytics auf. AWS

Zugreifen Oracle Database@AWS

Sie können Oracle Database@AWS mit dem erstellen, darauf zugreifen und verwalten AWS-Managementkonsole. Es bietet eine Weboberfläche, über die Sie darauf zugreifen können Oracle Database@AWS.

Preisgestaltung für Oracle Database@AWS

Sie können Oracle Database@AWS Angebote von erwerben AWS Marketplace. Sie wenden sich zunächst an einen Vertriebsmitarbeiter von Oracle. Oracle stellt Ihnen das Angebot dann auf der AWS Marketplace Grundlage der privaten Preisvereinbarung zur Verfügung. In Ihrer AWS Rechnung werden Gebühren ausgewiesen, die auf Ihrer Nutzung basieren.

Es fallen keine Datenübertragungsgebühren an, wenn Ihre Oracle-Anwendung und Ihre Oracle-Datenbank in derselben Availability Zone (AZ) gehostet werden. Für die Kommunikation zwischen fallen die üblichen Datenübertragungsgebühren an AZs.

Wenn Sie Oracle Database@AWS verwaltete Integrationen wie Zero-ETL, von Oracle verwaltete Backups und Amazon S3 verwenden, fallen die üblichen Datenverarbeitungsgebühren für die gemeinsame Nutzung und den Zugriff auf Ressourcen über VPC Lattice an. Für verwaltete Integrationen fallen keine Stundengebühren an. Oracle Database@AWS Weitere Informationen finden Sie unter Amazon VPC Lattice — Preise.

Als nächstes

Sie sind jetzt bereit, mit der Erstellung Ihrer Oracle Database@AWS Ressourcen zu beginnen.

1. Erfahren Sie, wie das Oracle Database@AWS funktioniert. Weitere Informationen finden Sie unter Wie Oracle Database@AWS funktioniert.

   > **Note**
   >
   > Wenn Sie mit AWS Oracle Exadata vertraut sind und sofort loslegen möchten, überspringen Sie diesen Schritt.

2. Fordern Sie Oracle Database@AWS über das ein privates Angebot an und nehmen Sie das AWS-Managementkonsole Angebot dann an. Weitere Informationen finden Sie unter Fordern Sie ein privates Angebot für Oracle Database@ an AWS.

   > **Note**
   >
   > Um in dieser Vorschau ein privates Angebot anzufordern, müssen Sie sich an uns wenden AWS , damit Ihr Angebot zu einer Zulassungsliste AWS-Konto hinzugefügt wird.

3. Erstellen Sie Ihr ODB-Netzwerk, Ihre Oracle Exadata-Infrastruktur und Ihre Exadata-VM-Cluster mithilfe der Konsole. AWS Erstellen Sie Ihre Exadata-Datenbanken mithilfe von OCI-Tools. Weitere Informationen finden Sie unter Erste Schritte mit Oracle Database@AWS.
4. Teilen Sie Ihre Ressourcen kontenübergreifend mit AWS Resource Access Manager ().AWS RAM Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten Oracle Database@AWS Ressourcen in einem vertrauenswürdigen Konto.

Wie Oracle Database@AWS funktioniert

Oracle Database@AWS integriert Oracle Cloud Infrastructure (OCI) mit der. AWS Cloud In den folgenden Abschnitten erfahren Sie mehr über die wichtigsten Komponenten dieser Multicloud-Architektur.

Oracle Exadata Database Service on Dedicated Infrastructure ist ein OCI-Service, der Exadata Database Machine bereitstellt. Oracle Exadata Database Machine ist eine integrierte, vorkonfigurierte und vorab getestete Full-Stack-Plattform für den Einsatz in Unternehmensrechenzentren. Sie können die Oracle Exadata-Infrastruktur und VM-Cluster in einer AWS Availability Zone (AZ) mithilfe der AWS Konsole, CLI oder erstellen. APIs

Nachdem Sie Ihre Ressourcen in erstellt haben, verwenden Sie OCI AWS, um Oracle APIs Exadata-Datenbanken zu erstellen und zu verwalten. Ein ODB-Netzwerk, das Sie mit einer Amazon VPC verbinden, ermöglicht EC2 Amazon-Anwendungsservern den Zugriff auf Ihre Exadata-Datenbanken. Auf diese Weise werden Oracle Exadata-Datenbanken in die Umgebung integriert. AWS

Das folgende Diagramm zeigt die Oracle Database@AWS Architektur.

Untergeordnete OCI-Sites

Die Oracle Cloud Infrastructure wird in OCI-Regionen und Verfügbarkeitsdomänen gehostet. Eine OCI-Region besteht aus OCI-Verfügbarkeitsdomänen (ADs), bei denen es sich um isolierte Rechenzentrumscluster innerhalb einer OCI-Region handelt. Ein untergeordneter OCI-Site ist ein Rechenzentrum, das eine OCI-Verfügbarkeitsdomäne auf eine Availability Zone (AZ) in einer Region erweitert. AWS Die Exadata-Infrastruktur befindet sich logischerweise in einer OCI-Region und physisch in einer Region. AWS

Der untergeordnete OCI-Site für befindet sich Oracle Database@AWS physisch in einem AWS Rechenzentrum. AWS hostet die Exadata-Infrastruktur, und OCI stellt die Exadata-Infrastrukturhardware im Rechenzentrum bereit und wartet sie. Sie können die Exadata-Infrastruktur, das private Netzwerk und die VM-Cluster mithilfe der AWS Konsole, CLI oder konfigurieren. APIs Sie können AWS Dienste wie Amazon EC2 und Amazon VPC verwenden, um Anwendungen den Zugriff auf Oracle Exadata-Datenbanken zu ermöglichen, die in der Infrastruktur ausgeführt werden.

Oracle Exadata-Infrastruktur

Die Oracle Exadata-Infrastruktur ist die zugrunde liegende Architektur von Datenbankservern und Speicherservern, auf der Oracle Exadata-Datenbanken ausgeführt werden. Die Infrastruktur befindet sich in einer AWS Availability Zone (AZ). Um VM-Cluster auf der Exadata-Infrastruktur zu erstellen, verwenden Sie die AWS Konsole, CLI oder. APIs

Die Oracle Exadata-Infrastruktur ist auf physische Maschinen verteilt, die als Datenbankserver bezeichnet werden. Diese Server stellen die Rechenressourcen bereit, ähnlich den EC2 dedizierten Servern von Amazon. Jeder Datenbankserver hostet eine oder mehrere virtuelle Maschinen (VMs), die auf einem Hypervisor laufen. Architekturdiagramme, die diese Zusammenhänge veranschaulichen, finden Sie unter Exadata Database Service on Dedicated Infrastructure Technical Architecture.

Wenn Sie eine Exadata-Infrastruktur in Oracle Database@ erstellen AWS, geben Sie Informationen wie die folgenden an:

- Die Gesamtzahl der Datenbankserver
- Die Gesamtzahl der Speicherserver
- Das Exadata-Systemmodell (X11M)
- Die AZ, die die Infrastruktur hostet (siehe) Unterstützte Regionen für Oracle Database@AWS

Informationen zum Erstellen einer Oracle Exadata-Infrastruktur finden Sie unter. Schritt 2: Erstellen Sie eine Oracle Exadata-Infrastruktur in Oracle Database@AWS

ODB-Netzwerk

Ein ODB-Netzwerk ist ein privates isoliertes Netzwerk, das die OCI-Infrastruktur in einer AWS Availability Zone (AZ) hostet. Das ODB-Netzwerk besteht aus einem CIDR-Bereich von IP-Adressen. Das ODB-Netzwerk ist direkt dem Netzwerk zugeordnet, das sich innerhalb des untergeordneten OCI-Sites befindet, und dient somit als Kommunikationsmittel zwischen und OCI. AWS Sie müssen ein ODB-Netzwerk angeben, wenn Sie Ihre Exadata-VM-Cluster erstellen (siehe). Schritt 3: Erstellen Sie einen Exadata-VM-Cluster oder einen Autonomous VM-Cluster in Oracle Database@AWS

Sie stellen Ressourcen in einem ODB-Netzwerk mithilfe von Oracle Database@ bereit.AWS APIs Das ODB-Netzwerk wird von verwaltet AWS, aber Sie können eine ODB-Peering-Verbindung

einrichten, um eine Amazon-VPC mit dem ODB-Netzwerk zu verbinden. Weitere Informationen finden Sie unter de. ODB-Peering

Wenn Sie ein ODB-Netzwerk erstellen, geben Sie Informationen wie die folgenden an:

- Availability Zone — Das ODB-Netzwerk ist spezifisch für eine AZ.

  Sie können Folgendes AWS-Regionen verwenden Oracle Database@AWS :

  USA Ost (Nord-Virginia)

  Sie können das AZs mit dem physischen IDs `use1-az4` und verwenden`use1-az6`.

  USA West (Oregon)

  Sie können das AZs mit dem physischen IDs `usw2-az3` und verwenden`usw2-az4`.

  Asien-Pazifik (Tokio)

  Sie können das AZs mit dem physischen IDs `apne1-az1` und verwenden`apne1-az4`.

  USA Ost (Ohio)

  Sie können das AZs mit dem physischen IDs `use2-az1` und verwenden`use2-az2`.

  Europa (Frankfurt)

  Sie können das AZs mit dem physischen IDs `euc1-az1` und verwenden`euc1-az2`.

  Kanada (Zentral)

  Sie können die AZ mit der physischen ID verwenden`cac1-az4`.

  Asien-Pazifik (Sydney)

  Sie können die AZ mit der physischen ID verwenden`apse2-az4`.

  Führen Sie den folgenden Befehl aus, um die logischen AZ-Namen in Ihrem Konto zu finden IDs, die der vorherigen physischen AZ zugeordnet sind.

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

- Client-CIDR-Adressen — Das ODB-Netzwerk benötigt ein Client-Subnetz-CIDR für Exadata-VM-Cluster und Autonomous VM-Cluster.

- CIDR-Adressen Backup — Das ODB-Netzwerk benötigt ein Backup-Subnetz CIDR für verwaltete Datenbanksicherungen von VM-Clustern. Das Backup-Subnetz ist für Exadata-VM-Cluster optional.
- AWS Serviceintegrationen — Sie können einen Netzwerkpfad für AWS Serviceintegrationen wie Amazon S3 und Zero-ETL mit Amazon Redshift konfigurieren. Weitere Informationen finden Sie unter AWS Service-Integrationen.

Weitere Informationen finden Sie unter Schritt 1: Erstellen Sie ein ODB-Netzwerk in Oracle Database@AWS.

Virtual Private Cloud (VPC)

Eine Virtual Private Cloud (VPC) ist ein virtuelles Netzwerk, das Sie in der AWS Cloud erstellen. Es ist logisch von anderen virtuellen Netzwerken in der AWS Cloud isoliert und bietet Ihnen die vollständige Kontrolle über die virtuelle Netzwerkumgebung, einschließlich der Auswahl Ihres eigenen IP-Adressbereichs, der Erstellung von Subnetzen und der Konfiguration von Routentabellen und Netzwerk-Gateways. Weitere Informationen finden Sie unter Was ist Amazon VPC?

Sie können EC2 Amazon-Instances in Ihrer Amazon VPC starten. Die EC2 Instances können Anwendungsserver hosten, die mit Oracle Exadata-Datenbanken kommunizieren. Sie können die Anwendungsserver wie alle anderen EC2 Instances in Ihrer VPC verwalten und starten. Weitere Informationen finden Sie unter Was ist Amazon EC2?

Standardmäßig hat das ODB-Netzwerk keine Konnektivität zu VPCs. Um das ODB-Netzwerk mit Ihrer vorhandenen AWS Infrastruktur zu verbinden, erstellen Sie eine Peering-Verbindung zwischen dem ODB-Netzwerk und einer VPC. Sie können die VPC angeben, wenn Sie das ODB-Netzwerk erstellen. Weitere Informationen finden Sie unter Schritt 1: Erstellen Sie ein ODB-Netzwerk in Oracle Database@AWS.

ODB-Peering

ODB-Peering ist eine vom Benutzer erstellte Netzwerkverbindung, mit der der Datenverkehr privat zwischen einer Amazon VPC und einem ODB-Netzwerk weitergeleitet werden kann. Es besteht eine 1:1 -Beziehung zwischen einer VPC und einem ODB-Netzwerk. Nach dem Peering kann eine EC2 Amazon-Instance innerhalb der VPC mit einer Oracle Exadata-Datenbank im ODB-Netzwerk kommunizieren, als ob sie sich im selben Netzwerk befände.

> **Note**
>
> ODB-Peering unterscheidet sich vom VPC-Peering, bei dem es sich um eine Peering-Verbindung zwischen zwei Personen handelt, die den Verkehr zwischen ihnen weiterleitet VPCs .

Sie können ein ODB-Netzwerk in einem Konto und eine VPC in einem anderen Konto miteinander verbinden, indem Sie. AWS RAM Wenn Sie ein ODB-Netzwerk mit einem anderen Konto gemeinsam nutzen, kann das Vertrauenskonto das Peering direkt initiieren. Das Konto, das die ODB-Peering-Verbindung initiiert, besitzt und verwaltet die Verbindung.

Sie können ein Peer-Netzwerk angeben CIDRs , wenn Sie ODB-Peering-Verbindungen erstellen oder aktualisieren. Auf diese Weise kontrollieren Sie, welche Subnetze in der Peer-VPC Zugriff auf Ihr ODB-Netzwerk haben. Ein VPC-Konto kann die CIDR-Bereiche aktualisieren, ohne auch das ODB-Netzwerk zu besitzen. Weitere Informationen finden Sie unter Konfiguration von ODB-Peering für eine Amazon VPC in. Oracle Database@AWS

Ressourcen in einer VPC können sich über Availability Zones (AZs) erstrecken. In einem ODB-Netzwerk sind Ressourcen an eine einzige AZ gebunden. Sie definieren diese AZ, wenn Sie das ODB-Netzwerk erstellen.

Erstellung einer ODB-Peering-Verbindung

Eine ODB-Peering-Verbindung ist kein Merkmal eines ODB-Netzwerks, sondern eine unabhängige Ressource mit eigener ID (Präfix) und eigenem Lebenszyklus. `odbpcx-` Sie verwalten eine Peering-Verbindung mit einer Reihe von dedizierten. APIs Beispielsweise erstellen Sie mithilfe der Oracle AWS Database@-Konsole oder der API eine ODB-Peering-Verbindung zu einem vorhandenen ODB-Netzwerk. `CreateOdbPeeringConnection` Weitere Informationen finden Sie unter Eine ODB-Peering-Verbindung in Oracle Database@ erstellen AWS.

Wenn Sie eine ODB-Peering-Verbindung erstellen, führt Oracle Database@ die folgenden Aktionen automatisch aus:AWS

1. Validiert die Netzwerkkonfigurationen, einschließlich der Prüfung auf überlappende CIDR-Blöcke mit dem Oracle VCN CIDR
2. Richtet die zugrunde liegende Netzwerk-Peering-Infrastruktur ein

3. Konfiguriert die Routing-Tabellen des ODB-Netzwerks (nicht der VPC) mit den VPC-CIDR-Adressen

Nachdem Sie Ihre ODB-Peering-Verbindung hergestellt haben, aktualisieren Sie Ihre VPC-Routing-Tabellen manuell mit dem Amazon-Befehl. EC2 `create-route` Weitere Informationen finden Sie unter Konfiguration von VPC-Routentabellen für ODB-Peering.

AWS Service-Integrationen

Um erweiterte Funktionen und Konnektivitätsoptionen für Ihre Oracle-Datenbanken bereitzustellen, lässt sich Oracle Database@ AWS-Services mit Amazon VPC Lattice AWS integrieren. Sie können Netzwerkpfade AWS-Services direkt von Ihrem ODB-Netzwerk aus konfigurieren, ohne dass zusätzliche VPCs oder komplexe Netzwerkeinrichtungen erforderlich sind.

Oracle Database@AWS unterstützt die folgenden AWS Managed Service-Integrationen:

Amazon S3

Sie können Amazon S3 auf folgende Weise mit Oracle Database@AWS integrieren:

- Oracle verwaltete automatische Backups auf Amazon S3 — Oracle Database@ ermöglicht AWS automatisch den Netzwerkzugriff für automatische Backups. Diese Integration kann nicht deaktiviert werden. Wenn Sie Amazon S3 in der OCI-Konsole als Ihr verwaltetes Backup-Ziel festlegen, lädt OCI automatische Backups in einen S3-Bucket hoch.
- Direkter Zugriff auf Amazon S3 von Ihrem ODB-Netzwerk aus — Sie können den direkten ODB-Netzwerkzugriff auf S3 aktivieren und dann Skripts speichern, Dateien importieren und exportieren sowie zugehörige Dateien in einem S3-Bucket speichern. Sie können diesen Zugriff deaktivieren. Diese Einstellung ist unabhängig vom automatischen Netzwerkzugriff für von Oracle verwaltete automatische Backups.

Null-ETL-Integration in Amazon Redshift

Sie können die Zero-ETL-Integration Ihres ODB-Netzwerks mit Amazon Redshift aktivieren. Diese Integration ermöglicht es Ihnen, Daten aus Ihren Oracle-Datenbanken, die in Oracle Database@ laufen,AWS ohne den herkömmlichen ETL-Prozess (Extrahieren, Transformieren und Laden) nach Amazon Redshift zu replizieren. Diese Integration ermöglicht Analysen und KI-Workloads in Echtzeit, indem Ihre Oracle-Daten automatisch mit Amazon Redshift synchronisiert werden.

Neben verwalteten Integrationen für AWS Dienste können Sie VPC Lattice auch verwenden, um auf Dienste und Ressourcen zuzugreifen, die in anderen gehostet werden VPCs, oder von Ihrer VPC aus auf ODB-Netzwerkinstanzen zuzugreifen. Sie können den Zugriff und die Ressourcen mithilfe der VPC Lattice-Konsole, CLI und verwalten. APIs Weitere Informationen finden Sie in den folgenden Ressourcen:

- In Oracle Database@ sichern AWS
- Oracle Database@AWS Zero-ETL-Integration mit Amazon Redshift
- Was ist Amazon VPC Lattice? und VPC Lattice für Oracle Database@AWS

Weiterleitung von Datenverkehr von mehreren VPCs

Um mehreren Benutzern VPCs den Zugriff auf Oracle Database@AWS Ressourcen in einem ODB-Netzwerk zu ermöglichen, können Sie unser AWS Cloud-WAN verwenden AWS Transit Gateway .

AWS Transit Gateway

Ein Amazon VPC Transit Gateway ist ein Netzwerk-Transit-Hub, der für die Verbindung VPCs und lokale Netzwerke verwendet wird. Ein ODB-Netzwerk unterstützt nur one-to-one direktes Peering zwischen dem ODB-Netzwerk und einer einzelnen VPC. Sie können Ihr ODB-Netzwerk mit einer VPC verbinden und diese VPC dann mit einem Transit-Gateway verbinden. Das Gateway kann eine Verbindung zu mehreren herstellen. VPCs Mit dieser Transit-Gateway-Konfiguration können Sie den Verkehr zwischen mehreren VPC-Subnetzen an ein einzelnes ODB-Netzwerk weiterleiten.

Weitere Informationen finden Sie unter Konfiguration von Amazon VPC Transit Gateways für Oracle Database@AWS.

AWS Cloud-WAN

AWS Cloud WAN ist ein verwalteter WAN-Dienst (Wide Area Networking), mit dem Sie ein einheitliches globales Netzwerk aufbauen, verwalten und überwachen können, das Ressourcen in Ihren Cloud- und lokalen Umgebungen verbindet. Mithilfe des zentralen Dashboards können Sie lokale Niederlassungen, Rechenzentren und das VPCs gesamte globale Netzwerk miteinander verbinden. AWS

Sie können Ihr ODB-Netzwerk mit einer VPC verbinden und diese VPC dann mit dem Cloud WAN-Kernnetzwerk verbinden. Mit dieser Konfiguration können Sie Cloud WAN verwenden,

um den Verkehr zwischen mehreren VPCs oder lokalen Netzwerken und Ihrem ODB-Netzwerk weiterzuleiten. Weitere Informationen finden Sie unter Konfiguration von AWS Cloud WAN für Oracle Database@AWS.

Exadata-VM-Cluster

Ein Exadata-VM-Cluster ist ein Satz eng miteinander verbundener Exadata. VMs Jede VM verfügt über eine vollständige Oracle-Datenbankinstallation, die alle Funktionen der Oracle Enterprise Edition umfasst, einschließlich Oracle Real Application Clusters (Oracle RAC) und Oracle Grid Infrastructure. Sie können eine oder mehrere Oracle Exadata-Datenbanken auf einem VM-Cluster erstellen. Diagramme, die die Architektur von VMs und VM-Clustern zeigen, finden Sie unter Exadata Database Service on Dedicated Infrastructure Technical Architecture.

Wenn Sie einen VM-Cluster erstellen, geben Sie Informationen an, die Folgendes beinhalten:

- Ein ODB-Netzwerk
- Eine Oracle Exadata-Infrastruktur
- Die Datenbankserver, auf denen die VMs im Cluster platziert werden sollen
- Die Gesamtmenge des nutzbaren Exadata-Speichers

Sie können die CPU-Kerne, den Arbeitsspeicher und den lokalen Speicher für jede VM in einem VM-Cluster konfigurieren. Weitere Informationen finden Sie unter Schritt 3: Erstellen Sie einen Exadata-VM-Cluster oder einen Autonomous VM-Cluster in Oracle Database@AWS.

Autonome VM-Cluster

Autonome VM-Cluster sind vollständig verwaltete Datenbanken, die wichtige Verwaltungsaufgaben mithilfe von maschinellem Lernen und KI automatisieren. Im Gegensatz zu herkömmlichen Datenbanken stellen autonome Datenbanken die Datenbank automatisch bereit, sichern, aktualisieren, sichern und optimieren, ohne dass menschliches Eingreifen erforderlich ist.

Sie können die Anzahl der ECPU-Kerne pro VM, den Datenbankspeicher pro CPU, den Datenbankspeicher und die maximale Anzahl autonomer Container-Datenbanken konfigurieren. Weitere Informationen finden Sie unter Schritt 3: Erstellen Sie einen Exadata-VM-Cluster oder einen Autonomous VM-Cluster in Oracle Database@AWS.

Oracle Exadata-Datenbanken

Oracle Exadata ist ein technisch ausgereiftes System, das eine Hochleistungsplattform für den Betrieb von Oracle-Datenbanken bietet. Mit verwenden Sie die AWS Konsole Oracle Database@AWS, um die Oracle Exadata-Infrastruktur und VM-Cluster zu erstellen, die die Exadata-Datenbanken hosten. Anschließend verwenden Sie OCI, um die Oracle-Datenbanken APIs zu erstellen und zu verwalten. Weitere Informationen finden Sie unter Schritt 4: Erstellen Sie Oracle Exadata-Datenbanken in Oracle Cloud Infrastructure.

Einführung in Oracle Database@AWS

Bevor Sie mit der Nutzung beginnen können Oracle Database@AWS, stellen Sie sicher, dass Sie für die Benutzer registriert sind AWS und die erforderlichen Benutzer erstellt haben. Dann können Sie Oracle Database@ bei AWS erwerben, AWS Marketplace indem Sie ein privates Angebot von Oracle annehmen.

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS-Managementkonsoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung -Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center -Benutzerhandbuch.
2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter Benutzerzugriff mit der Standardeinstellung konfigurieren.AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center - Benutzerhandbuch.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center - Benutzerhandbuch.

Fordern Sie ein privates Angebot für Oracle Database@ an AWS

Mit der Funktion „Private Angebote für AWS Marketplace Verkäufer“ können Sie AWS Preise und EULA-Bedingungen für Oracle Database@ von Oracle anfordern und erhalten. Sie verhandeln Preise und Konditionen mit Oracle, woraufhin Oracle ein privates Angebot für AWS-Konto die von Ihnen angegebenen Angebote erstellt. Sie nehmen das private Angebot an und erhalten den ausgehandelten Preis und die Nutzungsbedingungen. Zu diesem Zeitpunkt können Sie das Oracle Database@AWS Dashboard verwenden. Wenn der private Angebotsvertrag sein Ablaufdatum erreicht, werden Sie entweder automatisch zur öffentlichen Preisgestaltung des Produkts weitergeleitet oder Sie haben Ihr Abonnement bei Oracle Database@ gekündigt.AWSWeitere Informationen zu privaten Angeboten finden Sie unter Private Angebote in. AWS Marketplace

Um ein privates Angebot anzufordern und anzunehmen für Oracle Database@AWS

1. Melden Sie sich bei der an AWS-Managementkonsole.
2. Suchen Sie nach Oracle AWS Database@ und wählen Sie es dann aus.
3. Wählen Sie Privates Angebot anfordern aus.

   > **Note**
   >
   > Das Oracle Database@AWS Dashboard ist erst verfügbar, nachdem Sie ein privates Angebot angenommen haben.

4. Geben Sie auf der Oracle Cloud Infrastructure (OCI) -Website Details wie die Region und Ihre Kontaktinformationen an.
5. Warten Sie, bis sich ein Vertreter von OCI mit Ihnen in Verbindung setzt und Ihnen ein privates Angebot unterbreitet.
6. Wählen Sie in der AWS-Managementkonsole die Option Privates Angebot anzeigen aus.

7. Wählen Sie das Angebot und dann Angebot anzeigen aus.
8. Wählen Sie „Vertrag erstellen“ und antworten Sie auf die nachfolgenden Aufforderungen, um das private Angebot anzunehmen.
9. Nachdem Sie das private Angebot angenommen haben, müssen Sie Ihr OCI-Konto aktivieren. Sie können direkt von hier aus AWS-Managementkonsole auf die Oracle-Aktivierungslinks zugreifen.
    1. Navigieren Sie in der Konsole zum Abschnitt Erste Schritte.
    2. Klicken Sie in der Konsole auf den Oracle-Aktivierungslink. Alternativ können Sie auch den Aktivierungslink verwenden, der Ihnen per E-Mail zugeschickt wurde.
    3. Wählen Sie auf der Oracle-Aktivierungsseite aus, ob Sie ein neues Oracle Cloud-Konto erstellen oder ein vorhandenes Konto erweitern möchten.
    4. Schließen Sie den Aktivierungsvorgang ab, indem Sie den Anweisungen auf dem Bildschirm folgen.
    5. Nach dem Absenden Ihrer Aktivierungsanfrage wird im der AWS-Managementkonsole der Status Aktivierung läuft angezeigt. Das Dashboard wird vorübergehend deaktiviert und es wird ein Grund angezeigt.
    6. Nach Abschluss der Aktivierung ist das Oracle Database@AWS Dashboard verfügbar, mit dem Sie Ihre Ressourcen verwalten können.
10. Wählen Sie im AWS-Managementkonsole Dashboard aus.

Abonnieren Sie Oracle Database@AWS in mehreren Regionen

Wenn Sie das Abonnement abschließen AWS Marketplace und Oracle Database@AWS das Onboarding abschließen, AWS-Konto ist Ihr Abonnement mit Ihrem OCI-Mietverhältnis verknüpft. Dieser Link wird zusammen mit den zugehörigen Ressourcen automatisch in alle AWS Regionen repliziert, in denen er verfügbar ist. Oracle Database@AWS Sie abonnieren und registrieren sich einmal, anstatt den Vorgang für jede Region zu wiederholen.

Gehen Sie wie folgt vor, um die Nutzung Oracle Database@AWS in mehreren Regionen durchzuführen:

1. Abonnieren Sie das Abonnement Oracle Database@AWS über den Onboarding-Prozess AWS Marketplace und schließen Sie ihn ab.

Wenn Sie Oracle Database@ zum ersten Mal abonnieren AWS, wird Ihr Konto in einer Heimatregion aktiviert. Sie geben die Heimatregion in Oracle Cloud Infrastructure (OCI) an.

2. Aktivieren Sie Ihre bevorzugten Regionen über die OCI-Konsole.

   Wenn Sie eine Region in OCI nicht aktivieren und dann in der Oracle Database@AWS Konsole zu dieser Region wechseln, erhalten Sie eine Fehlermeldung, dass Sie kein Abonnement abgeschlossen haben. In diesem Fall müssen Sie diese Region in OCI aktivieren, bevor Sie das Oracle Database@AWS Dashboard in dieser Region verwenden können.
3. Zugriff Oracle Database@AWS in jeder unterstützten AWS Region, ohne den Abonnementvorgang zu wiederholen.

Erste Schritte mit Oracle Database@AWS

Um mit der Verwendung zu beginnen Oracle Database@AWS, können Sie die folgenden Ressourcen mithilfe der Oracle Database@AWS Konsole, der CLI oder erstellen APIs:

1. ODB-Netzwerk
2. Oracle Exadata-Infrastruktur
3. Exadata-VM-Cluster oder Autonomer VM-Cluster
4. ODB-Peering-Verbindung

Um Oracle Exadata-Datenbanken in Ihrer Infrastruktur zu erstellen, müssen Sie die Oracle Cloud Infrastructure (OCI) -Konsole oder APIs nicht das Dashboard verwenden. Oracle Database@AWS Somit stellen Sie Ressourcen in zwei Cloud-Umgebungen bereit: Netzwerk- und Infrastrukturressourcen befinden sich in OCI AWS, während sich die Kontrollebene für die Datenbankadministration in OCI befindet. Weitere Informationen finden Sie Oracle Database@AWSin der Oracle Cloud Infrastructure-Dokumentation.

Voraussetzungen für die Einrichtung Oracle Database@AWS

Bevor Sie Ihre Oracle Exadata-Infrastruktur konfigurieren, stellen Sie sicher, dass Sie Folgendes tun:

- Führen Sie die Schritte unter Einführung in Oracle Database@AWS aus. Sie müssen ein privates Nutzungsangebot angenommen haben. Oracle Database@AWS
- Erteilen Sie Ihrem IAM-Prinzipal die unter aufgeführten Richtlinienberechtigungen. Erlauben Sie Benutzern die Bereitstellung von Oracle Database@AWS Ressourcen Diese Berechtigungen sind für die Verwendung Oracle Database@AWS erforderlich.

Unterstützte OCI-Dienste auf Oracle Database@AWS

Oracle Database@AWS unterstützt die folgenden Oracle Cloud Infrastructure (OCI) -Dienste:

- Oracle Exadata Database Service auf einer dedizierten Infrastruktur — Bietet eine vollständig verwaltete, dedizierte Exadata-Umgebung, auf die von dort aus zugegriffen werden kann. AWS Weitere Informationen finden Sie unter Oracle Cloud Exadata Database Service on Dedicated Infrastructure in der OCI-Dokumentation.

- Autonome Datenbank auf einer dedizierten Exadata-Infrastruktur — Bietet eine hochautomatisierte, vollständig verwaltete Datenbankumgebung, die in OCI ausgeführt wird, mit dedizierten Hardware- und Softwareressourcen. Weitere Informationen finden Sie in der OCI-Dokumentation unter About Autonomous Database on Dedicated Exadata Infrastructure.

Unterstützte Regionen für Oracle Database@AWS

Sie können Folgendes verwenden Oracle Database@AWS AWS-Regionen:

USA Ost (Nord-Virginia)

Sie können das AZs mit dem physischen IDs `use1-az4` und verwenden`use1-az6`.

USA West (Oregon)

Sie können das AZs mit dem physischen IDs `usw2-az3` und verwenden`usw2-az4`.

Asien-Pazifik (Tokio)

Sie können das AZs mit dem physischen IDs `apne1-az1` und verwenden`apne1-az4`.

USA Ost (Ohio)

Sie können das AZs mit dem physischen IDs `use2-az1` und verwenden`use2-az2`.

Europa (Frankfurt)

Sie können das AZs mit dem physischen IDs `euc1-az1` und verwenden`euc1-az2`.

Kanada (Zentral)

Sie können die AZ mit der physischen ID verwenden`cac1-az4`.

Asien-Pazifik (Sydney)

Sie können die AZ mit der physischen ID verwenden`apse2-az4`.

Führen Sie den folgenden Befehl aus, um die logischen AZ-Namen in Ihrem Konto zu finden IDs, die der vorherigen physischen AZ zugeordnet sind.

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

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

Planung des IP-Adressraums in Oracle Database@AWS

Planen Sie den IP-Adressraum sorgfältig ein Oracle Database@AWS. Berücksichtigen Sie den IP-Adressverbrauch anhand der Anzahl der VM-Cluster, einschließlich der Anzahl der VM-Cluster VMs pro Cluster, die Sie im ODB-Netzwerk bereitstellen können. Weitere Informationen finden Sie unter ODB Network Design in der Oracle Cloud Infrastructure-Dokumentation.

Themen

- Einschränkungen für IP-Adressen im ODB-Netzwerk
- CIDR-Anforderungen des Client-Subnetzes für das ODB-Netzwerk
- CIDR-Anforderungen für das Backup-Subnetzwerk für das ODB-Netzwerk
- IP-Nutzungsszenarien für das ODB-Netzwerk

Einschränkungen für IP-Adressen im ODB-Netzwerk

Beachten Sie die folgenden Einschränkungen in Bezug auf CIDR-Bereiche im ODB-Netzwerk:

- Sie können den CIDR-Bereich des Client- oder Backup-Subnetzes für das ODB-Netzwerk nicht ändern, nachdem Sie ihn erstellt haben.
- Sie können die VPC-CIDR-Bereiche in der Spalte Eingeschränkte Zuordnungen in der Tabelle unter Einschränkungen für IPv4 CIDR-Blockzuordnungen nicht verwenden.
- Für Exadata X9M sind die IP-Adressen 100.106.0.0/16 und 100.107.0.0/16 für die Cluster-Verbindung von OCI Automation reserviert, sodass Sie Folgendes nicht tun können:
  - Weisen Sie diese Bereiche dem Client- oder Backup-CIDR-Bereich des ODB-Netzwerks zu.
  - Verwenden Sie diese Bereiche für eine VPC-CIDR, die für die Verbindung mit dem ODB-Netzwerk verwendet wird.
- Die folgenden CIDR-Bereiche sind für Oracle Cloud Infrastructure reserviert und können nicht für das ODB-Netzwerk verwendet werden:
  - Reservierter Bereich für Oracle Cloud CIDR 169.254.0.0/16
  - Reservierte Klasse D 224.0.0.0 — 239.255.255.255
  - Reservierte Klasse E 240.0.0.0 — 255.255.255.255

- Die CIDR-Bereiche der IP-Adressen für die Client- und Backup-Subnetze dürfen sich nicht überschneiden.
- Sie dürfen die den Client- und Backup-Subnetzen zugewiesenen IP-Adress-CIDR-Bereiche nicht mit den VPC-CIDR-Bereichen überschneiden, die für die Verbindung mit dem ODB-Netzwerk verwendet werden.
- Sie können VMs in einem VM-Cluster keine Bereitstellung in verschiedenen ODB-Netzwerken durchführen. Das Netzwerk ist eine Eigenschaft des VM-Clusters, was bedeutet, dass Sie es nur VMs im VM-Cluster im selben ODB-Netzwerk bereitstellen können.

CIDR-Anforderungen des Client-Subnetzes für das ODB-Netzwerk

In der folgenden Tabelle finden Sie die Anzahl der IP-Adressen, die vom Dienst und der Infrastruktur für das Client-Subnetz CIDR verwendet werden. Die CIDR-Mindestgröße für das Client-Subnetz ist /27, und die maximale Größe ist /16.

Anzahl der IP-Adressen	Konsumiert von	Hinweise
6	Oracle Database@AWS	Diese IP-Adressen sind unabhängig davon reserviert, wie viele VM-Cluster Sie im ODB-Netzwerk bereitstellen. Oracle Database@AWS verbraucht Folgendes: • 3 IP-Adressen, die für die ODB-Netzwerkressourcen reserviert sind, in AWS • 3 IP-Adressen, die für den OCI-Netzwerkdienst reservier t sind
3	Jeder VM-Cluste r	Diese IP-Adressen sind für Single Client Access Names (SCANs) reserviert, unabhängig davon, wie viele in jedem VM-Cluster vorhanden VMs sind.
4	Jede VM	Diese IP-Adressen hängen ausschließlich von der Anzahl der IP-Adressen VMs in der Infrastruktur ab.

CIDR-Anforderungen für das Backup-Subnetzwerk für das ODB-Netzwerk

In der folgenden Tabelle finden Sie die Anzahl der IP-Adressen, die vom Dienst und der Infrastruktur für das Backup-Subnetz CIDR verwendet werden. Die CIDR-Mindestgröße für das Backup-Subnetz ist /28 und die maximale Größe ist /16.

Anzahl der IP-Adressen	Konsumiert von	Hinweise
3	Oracle Database@AWS	Diese IP-Adressen sind unabhängig davon reserviert, wie viele VM-Cluster Sie im ODB-Netzwerk bereitstellen. Oracle Database@AWS verbraucht Folgendes: • 2 IP-Adressen am Anfang des CIDR-Bereichs • 1 IP-Adresse am Ende des CIDR-Bereichs
3	Jede VM	Diese IP-Adressen hängen ausschließlich von der Anzahl der IP-Adressen VMs in der Infrastruktur ab.

IP-Nutzungsszenarien für das ODB-Netzwerk

In der folgenden Tabelle sehen Sie die IP-Adressen, die im ODB-Netzwerk für verschiedene Konfigurationen von VM-Clustern verbraucht werden. Während /28 der technische Mindest-CIDR-Bereich für das Client-Subnetz CIDR ist, um einen VM-Cluster mit 2 bereitzustellen, empfehlen wir VMs, mindestens einen /27-CIDR-Bereich zu verwenden. In diesem Fall wird der IP-Bereich von den VM-Clustern nicht vollständig genutzt und ermöglicht die Zuweisung zusätzlicher IP-Adressen.

Konfiguration	Client IPs verbraucht	IPs Mindestanzahl an Kunden	Backup IPs verbraucht	IPs Mindestsicherung
1 VM-Cluster mit 2 VMs	17 (6 Dienste + 3 Cluster + 4*2)	32 (CIDR-Bereich /27)	(93 Service + 3*2)	16 (CIDR-Reihe /28)
1 VM-Cluster mit 3 VMs	21 (6 Dienste + 3 Cluster + 4*3)	32 (CIDR-Bereich /27)	12 (3 Dienste + 3*3)	16 (CIDR-Reihe /28)

Konfiguration	Client IPs verbraucht	IPs Mindestanzahl an Kunden	Backup IPs verbraucht	IPs Mindestsicherung
1 VM-Cluster mit 4 VMs	25 (6 Dienste + 3 Cluster + 4*4)	32 (CIDR-Bereich /27)	15 (3 Dienste + 3*4)	16 (CIDR-Reihe /28)
1 VM-Cluster mit 8 VMs	41 (6 Dienste + 3 Cluster + 4*8)	64 (CIDR-Bereich /26)	27 (3 Dienste + 3*8)	32 (CIDR-Reihe /27)

Die folgende Tabelle zeigt, wie viele Instanzen jeder Konfiguration für einen bestimmten Client-CIDR-Bereich möglich sind. Beispielsweise VMs verbraucht ein VM-Cluster mit 4 24 IP-Adressen im Client-Subnetz. Wenn der CIDR-Bereich /25 ist, sind 128 IP-Adressen verfügbar. Somit können Sie 5 VM-Cluster im Subnetz bereitstellen.

Konfiguration des VM-Clusters	Zahl mit /27 (32 IPs)	Zahl mit /26 (64) IPs	Zahl mit /25 (128) IPs	Zahl mit /24 (256) IPs	Zahl bei /23 (512) IPs	Nummer wenn /22 (1024) IPs
1 VM-Cluster mit 2 VMs (16 IPs)	1	3	7	15	30	60
1 VM-Cluster mit 3 VMs (20 IPs)	1	3	6	12	24	48
1 VM-Cluster mit 4 VMs (24 IPs)	1	2	5	10	20	40
2 VM-Cluster mit VMs jeweils 2 (27 IPs)	1	2	4	9	18	36
2 VM-Cluster mit VMs jeweils 3 (35 IPs)	0	1	3	7	14	28
2 VM-Cluster mit VMs jeweils 4 (43 IPs)	0	1	2	5	11	23

Schritt 1: Erstellen Sie ein ODB-Netzwerk in Oracle Database@AWS

Ein ODB-Netzwerk ist ein privates isoliertes Netzwerk, das die OCI-Infrastruktur in einer Availability Zone (AZ) hostet. Ein ODB-Netzwerk und eine Oracle Exadata-Infrastruktur sind Voraussetzungen für die Bereitstellung von VM-Clustern und die Erstellung von Exadata-Datenbanken. Sie können das ODB-Netzwerk und die Oracle Exadata-Infrastruktur in beliebiger Reihenfolge erstellen. Weitere Informationen erhalten Sie unter ODB-Netzwerk und ODB-Peering.

Bei dieser Aufgabe wird davon ausgegangen, dass Sie gelesen haben. Planung des IP-Adressraums in Oracle Database@AWS Informationen zum Ändern oder Löschen des ODB-Netzwerks zu einem späteren Zeitpunkt finden Sie unterOracle-Datenbank verwalten@AWS.

So erstellen Sie ein ODB-Netzwerk

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Oracle Database@AWS Konsole unter https://console.aws.amazon.com/odb/.
2. Wählen Sie oben rechts Ihre AWS Region aus. Weitere Informationen finden Sie unter Unterstützte Regionen für Oracle Database@AWS.
3. Wählen Sie im linken Bereich ODB-Netzwerke aus.
4. Wählen Sie ODB-Netzwerk erstellen.
5. Geben Sie unter ODB-Netzwerkname einen Netzwerknamen ein. Der Name muss 1—255 Zeichen lang sein und mit einem alphabetischen Zeichen oder Unterstrich beginnen. Er darf keine aufeinanderfolgenden Bindestriche enthalten.
6. Wählen Sie für Availability Zone einen AZ-Namen aus. Informationen zur Unterstützung AZs finden Sie unterUnterstützte Regionen für Oracle Database@AWS.
7. Geben Sie für Client-Subnetz-CIDR einen CIDR-Bereich für die Client-Verbindungen an. Weitere Informationen finden Sie unter CIDR-Anforderungen des Client-Subnetzes für das ODB-Netzwerk.
8. Geben Sie für Backup-Subnetz-CIDR einen CIDR-Bereich für die Backup-Verbindungen an. Um den Backup-Verkehr zu isolieren und die Ausfallsicherheit zu verbessern, empfehlen wir, dass sich Backup-CIDR und Client-CIDR nicht überschneiden. Weitere Informationen finden Sie unter CIDR-Anforderungen für das Backup-Subnetzwerk für das ODB-Netzwerk.
9. Wählen Sie für die DNS-Konfiguration eine der folgenden Optionen:

Standard

Geben Sie unter Domainnamenpräfix einen Namen ein, der als Präfix für Ihre Domain verwendet werden soll. Der Domainname ist fest als oraclevcn.com festgelegt. Wenn Sie beispielsweise eingeben, lautet der vollqualifizierte Domainname **`myhost`** myhost.oraclevcn.com.

Benutzerdefinierter Domainname

Geben Sie unter Domainname einen vollständigen Domainnamen ein. Sie könnten beispielsweise myhost.myodb.com eingeben.

10. (Optional) Wählen Sie für Serviceintegrationen einen Service aus, der mithilfe von VPC Lattice in Ihr Netzwerk integriert werden soll. Oracle Database@AWS lässt sich in verschiedene Systeme integrieren AWS-Services , um erweiterte Funktionen und Verbindungsoptionen für Ihre Oracle-Datenbanken bereitzustellen. Wählen Sie eine der folgenden Integrationen aus:

    Amazon S3

    Aktivieren Sie den direkten ODB-Netzwerkzugriff auf Amazon S3. Ihre Datenbanken können für Datenimport/-export oder benutzerdefinierte Backups auf S3 zugreifen. Sie können eine JSON-Richtlinie eingeben. Weitere Informationen finden Sie unter Benutzerverwaltete Backups auf Amazon S3 in Oracle Database@AWS.

    Zero-ETL

    Ermöglichen Sie mithilfe von Amazon Redshift Echtzeitanalysen und maschinelles Lernen für Transaktionsdaten. Weitere Informationen finden Sie unter Oracle Database@AWS Zero-ETL-Integration mit Amazon Redshift.

    > **Note**
    >
    > Wenn Sie Ihr ODB-Netzwerk erstellen, konfiguriert Oracle Database@AWS automatisch den Netzwerkzugriff für von Oracle verwaltete Backups auf Amazon S3 vor. Sie können diese Integration nicht aktivieren oder deaktivieren. Weitere Informationen finden Sie unter AWS Service-Integrationen.

11. (Optional) Geben Sie für Tags bis zu 50 Tags für das Netzwerk ein. Ein Tag ist ein Schlüssel-Wert-Paar, mit dem Sie Ihre Ressourcen organisieren und verfolgen können.

12. Wählen Sie „ODB-Netzwerk erstellen“.

Nachdem Sie ein ODB-Netzwerk erstellt haben, können Sie es mit einer VPC verbinden. ODB-Peering ist eine vom Benutzer erstellte Netzwerkverbindung, mit der der Datenverkehr privat zwischen einer Amazon VPC und einem ODB-Netzwerk weitergeleitet werden kann. Nach dem Peering kann eine EC2 Amazon-Instance innerhalb der VPC mit Ressourcen im ODB-Netzwerk kommunizieren, als ob sie sich im selben Netzwerk befinden würden. Weitere Informationen finden Sie unter Konfiguration von ODB-Peering zu einer Amazon VPC in der Oracle-Datenbank@AWS.

Schritt 2: Erstellen Sie eine Oracle Exadata-Infrastruktur in Oracle Database@AWS

Die Oracle Exadata-Infrastruktur ist die zugrunde liegende Architektur von Datenbankservern, Speicherservern und Netzwerken, auf denen Oracle Exadata-Datenbanken ausgeführt werden. Wählen Sie entweder Exadata X9M oder X11M als Systemmodell. Anschließend können Sie mithilfe der Konsole VM-Cluster auf der Exadata-Infrastruktur erstellen. AWS

Sie können die Oracle Exadata-Infrastruktur und das ODB-Netzwerk in beliebiger Reihenfolge erstellen. Sie müssen bei der Erstellung der Infrastruktur keine Netzwerkinformationen angeben.

Sie können eine Oracle Exadata-Infrastruktur nicht ändern, nachdem Sie sie erstellt haben. Informationen zum Löschen einer Exadata-Infrastruktur finden Sie unter. Löschen einer Oracle Exadata-Infrastruktur in Oracle Database@AWS

So erstellen Sie eine Exadata-Infrastruktur

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Oracle Database@AWS Konsole unter. https://console.aws.amazon.com/odb/
2. Wählen Sie im linken Bereich Exadata-Infrastrukturen aus.
3. Wählen Sie Create Exadata Infrastructure.
4. Geben Sie für den Namen der Exadata-Infrastruktur einen Namen ein. Der Name muss 1—255 Zeichen lang sein und mit einem alphabetischen Zeichen oder Unterstrich beginnen. Er darf keine aufeinanderfolgenden Bindestriche enthalten.
5. Wählen Sie für Availability Zone eine der unterstützten Zonen aus. AZs Klicken Sie anschließend auf Weiter.

6. Wählen Sie für das Exadata-Systemmodell entweder Exadata.X9M oder Exadata.X11M. Wählen Sie für Exadata.X11M auch die folgenden Servertypen aus:

   - Wählen Sie unter Datenbankservertyp den Datenbankserver-Modelltyp Ihrer Exadata-Infrastruktur aus. Derzeit ist X11M die einzige Wahl.
   - Wählen Sie als Speicherservertyp den Speicherserver-Modelltyp Ihrer Exadata-Infrastruktur aus. Derzeit ist X11M-HC die einzige Wahl.

7. Behalten Sie für Datenbankserver den Standardwert 2 bei oder bewegen Sie den Schieberegler, um bis zu 32 Server auszuwählen. Um mehr als 2 anzugeben, fordern Sie bei OCI eine Erhöhung des Limits an.

   Jeder Exadata X9M-Datenbankserver unterstützt 126. OCPUs Jeder Exadata X11M-Datenbankserver unterstützt 760. ECPUs Die Gesamtzahl der Rechenleistung ändert sich, wenn Sie die Anzahl der Server ändern. Weitere Informationen zu OCPUs und ECPUs finden Sie unter Compute Models in Autonomous Database in der Oracle-Dokumentation.

8. Behalten Sie für Speicherserver den Standardwert 3 bei oder bewegen Sie den Schieberegler, um bis zu 64 Server auszuwählen. Wenn Sie mehr als 3 angeben möchten, fordern Sie bei OCI eine Erhöhung des Limits an. Jeder X9M-Speicherserver bietet 64 TB. Jeder X11m-Speicherserver bietet 80 TB. Die Gesamtspeicherkapazität in TB ändert sich, wenn Sie die Anzahl der Server ändern. Klicken Sie anschließend auf Weiter.

9. Konfigurieren Sie für das Wartungsfenster, wann das System gewartet werden kann:

   a. Wählen Sie für die Zeitplanungspräferenz eine der folgenden Optionen aus:

      - Von Oracle verwalteter Zeitplan — Oracle bestimmt den optimalen Zeitpunkt für Wartungsaktivitäten.
      - Vom Kunden verwalteter Zeitplan — Sie geben an, wann Wartungsaktivitäten durchgeführt werden können.

   b. Wählen Sie für den Patching-Modus eine der folgenden Optionen aus:

      - Rollend — Updates werden jeweils auf einen Knoten angewendet, sodass die Datenbank während des Patchens verfügbar bleibt.
      - Nicht fortlaufend — Updates werden auf alle Knoten gleichzeitig angewendet, was zu Ausfallzeiten führen kann.

   c. Wenn Sie den vom Kunden verwalteten Zeitplan ausgewählt haben, konfigurieren Sie die folgenden zusätzlichen Einstellungen:

- Wählen Sie unter Wartungsmonate die Monate aus, in denen die Wartung durchgeführt werden kann.
- Wählen Sie unter Woche des Monats aus, in welcher Woche des Monats Wartungsarbeiten durchgeführt werden können (erste, zweite, dritte, vierte oder letzte).
- Wählen Sie unter Wochentag den Tag aus, an dem die Wartung durchgeführt werden kann (Montag bis Sonntag).
- Wählen Sie unter Startzeit die Stunde aus, zu der das Wartungsfenster beginnt. Die Zeit ist in UTC angegeben.
- Wählen Sie unter Vorlaufzeit für Benachrichtigungen aus, wie viele Tage im Voraus Sie über bevorstehende Wartungsarbeiten informiert werden möchten.

> **Note**
>
> Oracle Cloud Infrastructure führt in diesem Fenster die Systemwartung durch. Während der Wartung bleibt Ihre Exadata-Infrastruktur verfügbar, es kann jedoch zu kurzen Perioden mit höherer Latenz kommen.

10. (Optional) Geben Sie für Kontakte mit OCI-Wartungsbenachrichtigungen bis zu 10 E-Mail-Adressen ein. AWS leitet diese E-Mail-Adressen an OCI weiter. Wenn Aktualisierungen vorgenommen werden, sendet OCI Benachrichtigungen an die aufgelisteten Adressen.
11. (Optional) Geben Sie für Tags bis zu 50 Tags für die Infrastruktur ein. Ein Tag ist ein Schlüssel-Wert-Paar, mit dem Sie Ihre Ressourcen organisieren und verfolgen können.
12. Wählen Sie Weiter und überprüfen Sie Ihre Infrastruktureinstellungen.
13. Wählen Sie „Exadata-Infrastruktur erstellen“.

Schritt 3: Erstellen Sie einen Exadata-VM-Cluster oder einen Autonomous VM-Cluster in Oracle Database@AWS

Ein Exadata-VM-Cluster ist eine Reihe von Clustern, VMs auf denen Sie Oracle Exadata-Datenbanken erstellen können. Sie erstellen die VM-Cluster auf der Exadata-Infrastruktur. Sie können mehrere VM-Cluster mit unterschiedlichen Oracle Exadata-Infrastrukturen im selben ODB-Netzwerk bereitstellen. Sie haben die volle administrative Kontrolle über die Datenbanken, die Sie auf Exadata-VM-Clustern erstellen.

Ein Autonomous VM-Cluster ist ein vorab zugewiesener Pool von Oracle Exadata-Rechen- und Speicherressourcen, der auf VM-Ebene virtualisiert ist und Autonomous Databases (ADB) ausführt. Im Gegensatz zu benutzerverwalteten Datenbanken, die Sie auf einem Exadata-VM-Cluster erstellen, optimiert sich eine autonome Datenbank selbst, patcht selbst und wird von Oracle und nicht von einem Datenbankadministrator verwaltet.

Beachten Sie bei der Erstellung von VM-Clustern die folgenden Einschränkungen:

- Sie können einen VM-Cluster nur in der AZ bereitstellen, in der Sie Ihr ODB-Netzwerk und Ihre Oracle Exadata-Infrastruktur erstellt haben.
- Wenn Sie einen VM-Cluster nicht für mehrere Konten gemeinsam nutzen, muss er sich in derselben Oracle AWS-Konto Exadata-Infrastruktur befinden. Wenn Sie ein ODB-Netzwerk und eine Oracle Exadata-Infrastruktur von einem AWS Konto mit einem vertrauenswürdigen Konto gemeinsam nutzen AWS RAM , kann das vertrauenswürdige Konto VM-Cluster in seinem eigenen Konto erstellen.
- Sie können in Ihrem ODB-Netzwerk nur VM-Cluster bereitstellen. Andere Ressourcen sind nicht erlaubt.
- Sie können die Speicherzuweisung nicht ändern, nachdem Sie einen VM-Cluster erstellt haben.

> **Important**
>
> Der Erstellungsvorgang kann je nach Größe des VM-Clusters über 6 Stunden dauern.

Exadata VM cluster

Um einen Exadata-VM-Cluster zu erstellen

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die Oracle Database@AWS Konsole unter. https://console.aws.amazon.com/odb/
2. Wählen Sie im linken Bereich Exadata VM Clusters aus.
3. Wählen Sie Create VM cluster.
4. Geben Sie für den Namen des VM-Clusters einen Namen ein. Der Name muss 1—255 Zeichen lang sein und mit einem alphabetischen Zeichen oder Unterstrich beginnen. Er darf keine aufeinanderfolgenden Bindestriche enthalten.

5. (Optional) Geben Sie für den Namen des Grid Infrastructure-Clusters eine Grid-Infrastrukturversion für Ihren VM-Cluster ein, die mit der von Ihnen verwendeten Oracle-Datenbankversion übereinstimmt. Der Name muss 1—11 Zeichen lang sein und darf keine Bindestriche enthalten.
6. Geben Sie für Zeitzone eine Zeitzone ein.
7. Wählen Sie für Lizenzoptionen die Option Bring Your Own License (BYOL) oder License Included und anschließend Next aus. Bei dieser Lizenz handelt es sich um die von Oracle bereitgestellte OCI-Lizenz, nicht um eine Lizenz von. AWS
8. Konfigurieren Sie die Exadata-Infrastruktureinstellungen wie folgt:

   a. Wählen Sie für Infrastruktur Folgendes aus:

      - Wählen Sie unter Exadata-Infrastrukturname die Infrastruktur aus, die für diesen VM-Cluster verwendet werden soll.
      - Wählen Sie für die Grid Infrastructure-Version die Version aus, die für diesen VM-Cluster verwendet werden soll.
      - Wählen Sie für die Exadata-Image-Version die Version aus, die für diesen VM-Cluster verwendet werden soll. Wir empfehlen Ihnen, die angezeigte Version zu wählen, bei der es sich um die höchste verfügbare Version handelt.

   b. Wählen Sie für Datenbankserver einen oder mehrere Datenbankserver aus, auf denen Ihr VM-Cluster gehostet werden soll.

   c. Gehen Sie für die Konfiguration wie folgt vor:

      - Wählen Sie die Anzahl der CPU-Kerne, den Arbeitsspeicher und den lokalen Speicher für jede VM aus, oder akzeptieren Sie die Standardwerte.
      - Wählen Sie die Gesamtmenge an Exadata-Speicher für den VM-Cluster aus, oder akzeptieren Sie den Standard.

   d. (Optional) Wählen Sie für die Speicherzuweisung eine der folgenden Optionen aus:

      - Aktivieren Sie die Speicherzuweisung für Exadata Sparse-Snapshots
      - Aktivieren Sie die Speicherzuweisung für lokale Backups

      Die nutzbare Speicherzuweisung ändert sich, wenn Sie Optionen auswählen. Sie können diese Speicherzuweisung später nicht ändern. Überprüfen Sie Ihre Auswahl und wählen Sie dann Weiter.

9. Konfigurieren Sie die Konnektivität wie folgt:

    a. Wählen Sie für das ODB-Netzwerk ein vorhandenes ODB-Netzwerk aus.

    b. Geben Sie unter Hostnamenpräfix ein Präfix für den VM-Cluster ein. Stellen Sie sicher, dass Sie den Domainnamen nicht angeben. Das Präfix bildet den ersten Teil des Hostnamens des Oracle Exadata VM-Clusters.

    > **Note**
    >
    > Der Host-Domänenname ist fest als oraclevcn.com festgelegt.

    c. Geben Sie für den SCAN-Listener-Port (TCP/IP) eine Portnummer für den TCP-Zugriff auf den Single Client Access Name (SCAN) -Listener ein. Der Standardport ist 1521. Sie können auch einen benutzerdefinierten SCAN-Port im Bereich 1024—8999 eingeben, mit Ausnahme der folgenden Portnummern: 2484, 6100, 6200, 7060, 7070, 7085 und 7879. Klicken Sie anschließend auf Weiter.

    d. Geben Sie für SSH-Schlüsselpaare den öffentlichen Schlüsselteil eines oder mehrerer Schlüsselpaare ein, die für den SSH-Zugriff auf den VM-Cluster verwendet werden. Klicken Sie anschließend auf Weiter.

10. (Optional) Wählen Sie Diagnosen und Tags wie folgt aus:

    a. Wählen Sie aus, ob die Erfassung von Diagnosen für Diagnoseereignisse, Health Monitor und Incident-Logs und Trace-Sammlungen aktiviert werden soll. Oracle kann diese Diagnoseinformationen verwenden, um Probleme zu identifizieren, nachzuverfolgen und zu lösen.

    b. Geben Sie für Tags bis zu 50 Tags für den VM-Cluster ein. Ein Tag ist ein Schlüssel-Wert-Paar, mit dem Sie Ihre Ressourcen organisieren und verfolgen können. Klicken Sie anschließend auf Weiter.

11. Überprüfen Sie die Einstellungen. Wählen Sie dann Create VM cluster.

Autonomous VM cluster

Um einen autonomen VM-Cluster zu erstellen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Oracle Database@AWS Konsole unter https://console.aws.amazon.com/odb/.
2. Wählen Sie im linken Bereich Autonomous VM Clusters aus.

3. Wählen Sie Autonomen VM-Cluster erstellen.
4. Geben Sie für den Namen des VM-Clusters einen Namen ein. Der Name muss 1—255 Zeichen lang sein und mit einem alphabetischen Zeichen oder Unterstrich beginnen. Er darf keine aufeinanderfolgenden Bindestriche enthalten.
5. Geben Sie für Zeitzone eine Zeitzone ein.
6. Wählen Sie für Lizenzoptionen die Option Bring Your Own License (BYOL) oder License Included und anschließend Next aus. Bei dieser Lizenz handelt es sich um die von Oracle bereitgestellte OCI-Lizenz, nicht um eine Lizenz von. AWS
7. Konfigurieren Sie die Exadata-Infrastruktureinstellungen wie folgt:

   a. Wählen Sie unter Exadata-Infrastrukturname die Infrastruktur aus, die für diesen autonomen VM-Cluster verwendet werden soll.

   b. Wählen Sie für Datenbankserver einen oder mehrere Datenbankserver aus, auf denen Ihr Autonomous VM-Cluster gehostet werden soll.

   c. Gehen Sie für die Konfiguration wie folgt vor:

      - Wählen Sie die Anzahl der ECPU-Kerne pro VM, den Datenbankspeicher pro CPU, den Datenbankspeicher und die maximale Anzahl autonomer Container-Datenbanken aus, oder akzeptieren Sie die Standardwerte.
      - Wählen Sie die Gesamtmenge an Exadata-Speicher für den Autonomous VM-Cluster aus, oder akzeptieren Sie den Standard.
8. Konfigurieren Sie die Konnektivität wie folgt:

   a. Wählen Sie für das ODB-Netzwerk ein vorhandenes ODB-Netzwerk aus.

   b. Geben Sie für den SCAN-Listener-Port (TCP/IP) eine Portnummer für Port (ohne TLS) ein. Der Standardport ist 1521. Sie können auch einen Port (TLS) im Bereich 1024—8999 eingeben, mit Ausnahme der folgenden Portnummern: 2484, 6100, 6200, 7060, 7070, 7085 und 7879. Klicken Sie anschließend auf Weiter.

      Wählen Sie Gegenseitige TLS-Authentifizierung (mTLS) aktivieren aus, um die gegenseitige TLS-Authentifizierung zu ermöglichen.
9. (Optional) Wählen Sie Diagnosen und Tags wie folgt aus:

   a. Wählen Sie aus, ob Sie die Änderung der Konfiguration für den von Oracle verwalteten Zeitplan oder für den vom Kunden verwalteten Zeitplan planen möchten. Wenn Sie den

vom Kunden verwalteten Zeitplan wählen, legen Sie die Wartungsmonate, die Wochen des Monats, den Wochentag und die Startzeit (UTC) fest.

b. Geben Sie für Tags bis zu 50 Tags für den Autonomous VM-Cluster ein. Ein Tag ist ein Schlüssel-Wert-Paar, mit dem Sie Ihre Ressourcen organisieren und verfolgen können. Klicken Sie anschließend auf Weiter.

10. Überprüfen Sie die Einstellungen. Wählen Sie dann Autonomen VM-Cluster erstellen.

Schritt 4: Erstellen Sie Oracle Exadata-Datenbanken in Oracle Cloud Infrastructure

Oracle Database@AWS In können Sie die folgenden Ressourcen mithilfe der AWS Konsole, CLI oder erstellen und verwalten APIs:

- ODB-Netzwerke
- Oracle Exadata-Infrastruktur
- Exadata-VM-Cluster und autonome VM-Cluster
- ODB-Peering-Verbindungen

Um Oracle Exadata-Datenbanken auf der von Ihnen erstellten Infrastruktur zu erstellen und zu verwalten, müssen Sie die Oracle Cloud Infrastructure-Konsole und nicht das Dashboard verwenden. Oracle Database@AWS Sie können eine benutzerverwaltete Exadata-Datenbank auf einem Exadata-VM-Cluster und eine Autonome Datenbank auf einem Autonomous Exadata-VM-Cluster erstellen. Informationen zum Erstellen von Oracle-Datenbanken in OCI finden Sie unter Exadata Database in der Oracle Cloud Infrastructure-Dokumentation.

Um Oracle Exadata-Datenbanken zu erstellen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Oracle Database@AWS Konsole unter. https://console.aws.amazon.com/odb/
2. Wählen Sie im linken Bereich Exadata VM Clusters oder Autonomous VM Clusters aus.
3. Wählen Sie einen VM-Cluster aus, um die Detailseite aufzurufen.
4. Wählen Sie In OCI verwalten, um zur Oracle Cloud Infrastructure-Konsole weitergeleitet zu werden.
5. Erstellen Sie Ihre benutzerverwaltete Exadata-Datenbank oder Autonome Datenbank in OCI.

Konfiguration von ODB-Peering zu einer Amazon VPC in der Oracle-Datenbank@AWS

ODB-Peering ist eine vom Benutzer erstellte Netzwerkverbindung, mit der der Datenverkehr privat zwischen einer Amazon VPC und einem ODB-Netzwerk weitergeleitet werden kann. Es besteht eine one-to-one Beziehung zwischen einer VPC und einem ODB-Netzwerk. Nachdem Sie eine Peering-Verbindung über die Konsole, CLI oder API hergestellt haben, stellen Sie sicher, dass Sie Ihre VPC-Routing-Tabellen aktualisieren und die DNS-Auflösung konfigurieren. Einen konzeptionellen Überblick über ODB-Peering finden Sie unter. ODB-Peering

Eine ODB-Peering-Verbindung in Oracle Database@ erstellen AWS

Mit ODB-Peering-Verbindungen können Sie eine private Netzwerkkonnektivität zwischen Ihrer Oracle Exadata-Infrastruktur und den in Ihrem Amazon ausgeführten Anwendungen einrichten. VPCs Jede ODB-Peering-Verbindung ist eine separate Ressource, die Sie unabhängig vom ODB-Netzwerk erstellen, anzeigen und löschen können.

Beim Erstellen einer ODB-Peering-Verbindung können Sie CIDR-Bereiche für Peer-Netzwerke angeben. Diese Technik beschränkt den Netzwerkzugriff auf die erforderlichen Subnetze, reduziert potenzielle Angriffsziele und ermöglicht eine detailliertere Netzwerksegmentierung zur Erfüllung von Compliance-Anforderungen.

Sie können die folgenden Arten von ODB-Peering-Verbindungen erstellen:

ODB-Peering für dasselbe Konto

Sie können im selben Konto eine ODB-Peering-Verbindung zwischen einem ODB-Netzwerk und einer Amazon VPC herstellen. AWS

Kontoübergreifendes ODB-Peering

Sie können eine ODB-Peering-Verbindung zwischen einem ODB-Netzwerk in einem Konto und einer Amazon VPC in einem anderen Konto herstellen, nachdem das ODB-Netzwerk gemeinsam genutzt wurde. AWS RAM VPC-Besitzerkonten können die in der Peering-Verbindung angegebenen CIDR-Bereiche verwalten, ohne auch das ODB-Netzwerk zu besitzen.

Es besteht eine 1:1 -Beziehung zwischen einer VPC und einem ODB-Netzwerk. Sie können keine ODB-Peering-Verbindung zwischen einer VPC und mehreren ODB-Netzwerken oder zwischen einem ODB-Netzwerk und mehreren herstellen. VPCs

Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Konsole unter. Oracle Database@AWS https://console.aws.amazon.com/odb/
2. Wählen Sie im Navigationsbereich ODB-Peering-Verbindungen aus.
3. Wählen Sie ODB-Peering-Verbindung erstellen aus.
4. (Optional) Geben Sie für den ODB-Peering-Namen einen eindeutigen Namen für Ihre Verbindung ein.
5. Wählen Sie für das ODB-Netzwerk das ODB-Netzwerk aus, das gepeert werden soll.
6. Wählen Sie für Peer-Netzwerk die Amazon VPC aus, die mit Ihrem ODB-Netzwerk verbunden werden soll.
7. (Optional) Geben Sie für Peer-Netzwerk CIDRs zusätzliche CIDR-Blöcke von der Peer-VPC an, die auf das ODB-Netzwerk zugreifen können. Wenn Sie nichts angeben CIDRs, wird allen CIDRs von der Peer-VPC aus Zugriff gewährt.
8. (Optional) Fügen Sie unter Tags ein Schlüssel- und Wertepaar hinzu.
9. Wählen Sie „ODB-Peering-Verbindung erstellen“.

Nachdem Sie eine ODB-Peering-Verbindung hergestellt haben, konfigurieren Sie Ihre Amazon VPC-Routing-Tabellen so, dass der Datenverkehr an das Peering-ODB-Netzwerk weitergeleitet wird. Weitere Informationen finden Sie unter Konfiguration von VPC-Routentabellen für ODB-Peering. Beachten Sie, dass Oracle Database@ die ODB-Netzwerk-Routentabellen AWS automatisch konfiguriert.

AWS CLI

Verwenden Sie den Befehl, um eine ODB-Peering-Verbindung herzustellen. `create-odb-peering-connection`

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

Verwenden Sie den Parameter, um den Zugriff auf das ODB-Netzwerk auf bestimmte CIDR-Bereiche zu beschränken. `--peer-network-cidrs-to-be-added` Wenn Sie keine CIDR-Bereiche angeben, haben alle Bereiche Zugriff.

```
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"
```

Verwenden Sie den Befehl, um Ihre ODB-Peering-Verbindungen aufzulisten. `list-odb-peering-connections`

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

Verwenden Sie den Befehl, um Details zu einer bestimmten ODB-Peering-Verbindung abzurufen. `get-odb-peering-connection`

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

Aktualisierung einer ODB-Peering-Verbindung

Sie können eine bestehende ODB-Peering-Verbindung aktualisieren, um ein Peer-Netzwerk hinzuzufügen oder zu entfernen. CIDRs Sie steuern, welche Subnetze in der Peer-VPC Zugriff auf Ihr ODB-Netzwerk haben.

Konsole

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die Oracle Database@AWS Konsole unter. https://console.aws.amazon.com/odb/
2. Wählen Sie im Navigationsbereich ODB-Peering-Verbindungen aus.
3. Wählen Sie die ODB-Peering-Verbindung aus, die Sie aktualisieren möchten.
4. Wählen Sie Aktionen und dann Peering-Verbindung aktualisieren aus.
5. Fügen Sie im CIDRs Abschnitt Peer-Netzwerk nach Bedarf CIDR-Blöcke hinzu oder entfernen Sie sie:

   - Wählen Sie zum Hinzufügen CIDRs CIDR hinzufügen und geben Sie den CIDR-Block ein.

- Um zu entfernen CIDRs, wählen Sie das X neben dem CIDR-Block, den Sie entfernen möchten.

6. Wählen Sie Peering-Verbindung aktualisieren.

AWS CLI

CIDRs Um einer ODB-Peering-Verbindung ein Peer-Netzwerk hinzuzufügen, geben Sie den Parameter `--peer-network-cidrs-to-be-added` im Befehl an. `update-odb-peering-connection`

```
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"
```

Um ein Peer-Netzwerk CIDRs aus einer ODB-Peering-Verbindung zu entfernen, geben Sie den Parameter `--peer-network-cidrs-to-be-removed` im Befehl an. `update-odb-peering-connection`

```
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"
```

Konfiguration von VPC-Routentabellen für ODB-Peering

Eine Routing-Tabelle enthält Regeln, sogenannte Routen, die festlegen, wohin der Netzwerkverkehr von Ihrem Subnetz oder Gateway gelenkt wird. Das Ziel-CIDR in einer Routing-Tabelle ist ein Bereich von IP-Adressen, in den der Datenverkehr fließen soll. Wenn Sie eine VPC für ODB-Peering zu Ihrem ODB-Netzwerk angegeben haben, aktualisieren Sie Ihre VPC-Routentabelle mit dem Ziel-IP-Bereich in Ihrem ODB-Netzwerk. Weitere Informationen zum ODB-Peering finden Sie unter. ODB-Peering

Verwenden Sie den Befehl, um eine Routentabelle zu aktualisieren. AWS CLI `ec2 create-route` In den folgenden Beispielen werden Amazon VPC-Routentabellen aktualisiert. Weitere Informationen finden Sie unter Konfiguration von VPC-Routentabellen für ODB-Peering.

```
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
```

Die ODB-Netzwerk-Routentabellen werden automatisch mit der CIDRs VPC aktualisiert. Um den Zugriff auf das ODB-Netzwerk nur für ein bestimmtes Subnetz und CIDRs nicht für alle CIDRs in der VPC zu ermöglichen, können Sie CIDRs beim Erstellen einer ODB-Peering-Verbindung ein Peer-Netzwerk angeben oder eine bestehende ODB-Peering-Verbindung aktualisieren, um gepeerte CIDR-Bereiche hinzuzufügen oder zu entfernen. Weitere Informationen erhalten Sie unter Eine ODB-Peering-Verbindung in Oracle Database@ erstellen AWS und Aktualisierung einer ODB-Peering-Verbindung.

Weitere Informationen zu VPC-Routentabellen finden Sie unter Subnetz-Routentabellen im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch und ec2 create-route in der Befehlsreferenz.AWS CLI

Konfiguration von DNS für Oracle Database@AWS

Amazon Route 53 ist ein hochverfügbarer und skalierbarer Domain Name System (DNS) - Webservice, den Sie für DNS-Routing verwenden können. Wenn Sie eine ODB-Peering-Verbindung zwischen Ihrem ODB-Netzwerk und einer VPC herstellen, benötigen Sie einen Mechanismus, um DNS-Abfragen für ODB-Netzwerkressourcen innerhalb der VPC aufzulösen. Sie können Amazon Route 53 verwenden, um die folgenden Ressourcen zu konfigurieren:

- Ein ausgehender Endpunkt

  Der Endpunkt ist erforderlich, um DNS-Abfragen an das ODB-Netzwerk zu senden.
- Eine Resolver-Regel

  Diese Regel gibt den Domänennamen der DNS-Abfragen an, die der Route 53-Resolver an das DNS für das ODB-Netzwerk weiterleitet.

Wie funktioniert DNS in Oracle Database@AWS

Oracle Database@AWS verwaltet die DNS-Konfiguration (Domain Name System) für das ODB-Netzwerk automatisch. Für den Domainnamen können Sie entweder ein benutzerdefiniertes Präfix für den Standarddomänennamen `oraclevcn.com` oder einen vollständig benutzerdefinierten Domainnamen angeben. Weitere Informationen finden Sie unter Schritt 1: Erstellen Sie ein ODB-Netzwerk in Oracle Database@AWS.

Bei Oracle Database@AWS der Bereitstellung eines ODB-Netzwerks werden die folgenden Ressourcen erstellt:

- Ein virtuelles Cloud-Netzwerk (VCN) mit Oracle Cloud Infrastructure (OCI) mit denselben CIDR-Blöcken wie das ODB-Netzwerk

  Dieses VCN befindet sich im verknüpften OCI-Tenancy des Kunden. Es besteht eine 1:1 - Zuordnung zwischen einem ODB-Netzwerk und einem OCI-VCN. Jedes ODB-Netzwerk ist mit einem OCI-VCN verknüpft.
- Ein privater DNS-Resolver innerhalb des OCI VCN

  Dieser DNS-Resolver verarbeitet DNS-Abfragen innerhalb des OCI VCN. Die OCI-Automatisierung erstellt Datensätze für den VM-Cluster. Scans verwenden den `*.oraclevcn.com` vollqualifizierten Domänennamen (FQDN).
- Ein DNS-Listening-Endpunkt innerhalb des OCI VCN für den privaten DNS-Resolver

  Sie finden den DNS-Listening-Endpunkt auf der Seite mit den ODB-Netzwerkdetails in der Konsole. Oracle Database@AWS

Konfiguration eines ausgehenden Endpunkts in einem ODB-Netzwerk in Oracle Database@AWS

Ein ausgehender Endpunkt ermöglicht das Senden von DNS-Abfragen von Ihrer VPC an ein Netzwerk oder eine IP-Adresse. Der Endpunkt gibt die IP-Adressen an, von denen Anfragen stammen. Um DNS-Abfragen von Ihrer VPC an Ihr ODB-Netzwerk weiterzuleiten, erstellen Sie mit der Route 53 53-Konsole einen ausgehenden Endpunkt. Weitere Informationen finden Sie unter Weiterleiten ausgehender DNS-Abfragen an Ihr Netzwerk.

So konfigurieren Sie einen ausgehenden Endpunkt in einem ODB-Netzwerk

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im linken Bereich die Option Outbound Endpoints aus.
3. Wählen Sie in der Navigationsleiste die Region für die VPC aus, in der Sie den ausgehenden Endpunkt erstellen möchten.
4. Klicken Sie auf Create outbound endpoint (Ausgehenden Endpunkt erstellen).
5. Füllen Sie den Abschnitt Allgemeine Einstellungen für ausgehenden Endpunkt wie folgt aus:

a. Wählen Sie eine Sicherheitsgruppe aus, die ausgehende TCP- und UDP-Konnektivität zu folgenden Verbindungen ermöglicht:

   - IP-Adressen, die die Resolver für DNS-Abfragen in Ihrem ODB-Netzwerk verwenden
   - Ports, die die Resolver für DNS-Abfragen in Ihrem ODB-Netzwerk verwenden

b. Wählen Sie für Endpoint Type (Endpunkttyp) IPv4 aus.

c. Wählen Sie für Protokolle für diesen Endpunkt Do53 aus.

6. Geben Sie im Feld IP-Adressen die folgenden Informationen ein:

   - Geben Sie entweder IP-Adressen an, oder lassen Sie den Route 53 Resolver IP-Adressen aus den verfügbaren Adressen im Subnetz für Sie auswählen. Wählen Sie mindestens 2 bis maximal 6 IP-Adressen für DNS-Abfragen. Wir empfehlen, dass Sie IP-Adressen in mindestens zwei verschiedenen Availability Zones wählen.
   - Wählen Sie für Subnetz Subnetze mit folgenden Eigenschaften aus:
     - Routentabellen, die Routen zu den IP-Adressen des DNS-Listeners im ODB-Netzwerk enthalten
     - Netzwerkzugriffskontrolllisten (ACLs), die UDP- und TCP-Verkehr zu den IP-Adressen und den Ports zulassen, die die Resolver für DNS-Abfragen im ODB-Netzwerk verwenden
     - Netzwerk ACLs , das Datenverkehr von Resolvern im Zielportbereich 1024-65535 zulässt
7. (Optional) Geben Sie für Tags Tags für den Endpunkt an.
8. Wählen Sie Absenden aus.

Konfiguration einer Resolver-Regel in Oracle Database@AWS

Eine Resolver-Regel besteht aus einer Reihe von Kriterien, die bestimmen, wie DNS-Abfragen weitergeleitet werden. Verwenden Sie entweder eine Regel erneut oder erstellen Sie eine Regel, die den Domänennamen der DNS-Abfragen angibt, die der Resolver an das DNS für das ODB-Netzwerk weiterleitet.

Verwenden einer vorhandenen Resolver-Regel

Um eine bestehende Resolver-Regel zu verwenden, hängt Ihre Aktion vom Regeltyp ab:

Eine Regel für dieselbe Domain in derselben AWS Region wie die VPC in Ihrem AWS-Konto

Ordnen Sie die Regel Ihrer VPC zu, anstatt eine neue Regel zu erstellen. Wählen Sie die Regel im Regel-Dashboard aus und ordnen Sie sie der VPCs in der AWS Region geltenden Regel zu.

Eine Regel für dieselbe Domain in derselben Region wie Ihre VPC, aber in einem anderen Konto

Verwenden Sie diese Option AWS Resource Access Manager , um die Regel aus dem Remote-Konto mit Ihrem Konto zu teilen. Wenn Sie eine Regel teilen, geben Sie auch den entsprechenden ausgehenden Endpunkt weiter. Nachdem Sie die Regel mit Ihrem Konto geteilt haben, wählen Sie die Regel im Regel-Dashboard aus und verknüpfen Sie sie mit der VPCs in Ihrem Konto. Weitere Informationen finden Sie unter Weiterleitungsregeln verwalten.

Eine neue Resolver-Regel erstellen

Wenn Sie eine bestehende Resolver-Regel nicht wiederverwenden können, erstellen Sie mit der Amazon Route 53-Konsole eine neue Regel.

Um eine neue Resolver-Regel zu erstellen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im linken Bereich Regeln aus.
3. Wählen Sie in der Navigationsleiste die Region für die VPC aus, in der sich der ausgehende Endpunkt befindet.
4. Wählen Sie Regel erstellen aus.
5. Füllen Sie die Abschnitte „Regel für ausgehenden Verkehr“ wie folgt aus:
    a. Wählen Sie als Regeltyp die Option Regel weiterleiten aus.
    b. Geben Sie für Domänenname den vollständigen Domänennamen aus dem ODB-Netzwerk an.
    c. Verwenden Sie VPCs dazu diese Regel, indem Sie sie der VPC zuordnen, von der aus DNS-Abfragen an Ihr ODB-Netzwerk weitergeleitet werden.
    d. Wählen Sie für ausgehenden Endpunkt den ausgehenden Endpunkt aus, den Sie in erstellt haben. Konfiguration eines ausgehenden Endpunkts in einem ODB-Netzwerk in Oracle Database@AWS

> **Note**
>
> Die mit dieser Regel verknüpfte VPC muss nicht dieselbe VPC sein, in der Sie den ausgehenden Endpunkt erstellt haben.

6. Füllen Sie den Abschnitt Ziel-IP-Adressen wie folgt aus:
   a. Geben Sie als IP-Adresse die IP-Adresse der DNS-Listener-IP in Ihrem ODB-Netzwerk an.
   b. Geben Sie für Port 53 an. Dies ist der Port, den der Resolver für DNS-Abfragen verwendet.

   > **Note**
   >
   > Der Route 53 Resolver leitet DNS-Abfragen, die dieser Regel entsprechen und von einer mit dieser Regel verknüpften VPC stammen, an den referenzierten ausgehenden Endpunkt weiter. Diese Abfragen werden an die Ziel-IP-Adressen weitergeleitet, die Sie in den Ziel-IP-Adressen angeben.

   c. Wählen Sie als Übertragungsprotokoll Do53 aus.
7. (Optional) Geben Sie für Tags Tags für die Regel an.
8. Wählen Sie Absenden aus.

Testen Sie Ihre DNS-Konfiguration in Oracle Database@AWS

Nachdem Sie Ihren ausgehenden Endpunkt und die Resolver-Regel erstellt haben, testen Sie, ob der DNS korrekt aufgelöst wird. Führen Sie mithilfe einer EC2 Amazon-Instance in Ihrer Anwendungs-VPC eine DNS-Auflösung wie folgt durch:

Für Linux oder macOS

Verwenden Sie einen Befehl der Form`dig` *`record-name record-type`*.

Für Windows

Verwenden Sie einen Befehl der Form`nslookup -type=`*`record-name record-type`*.

Konfiguration von Amazon VPC Transit Gateways für Oracle Database@AWS

Amazon VPC Transit Gateways ist ein Netzwerk-Transit-Hub, der virtuelle private Clouds (VPCs) und lokale Netzwerke miteinander verbindet. Jede VPC in der hub-and-spoke Architektur kann eine Verbindung zum Transit-Gateway herstellen, um Zugriff auf andere verbundene VPCs zu erhalten. AWS Transit Gateway unterstützt den Verkehr sowohl für als IPv4 auch IPv6.

In Oracle Database@AWS unterstützt ein ODB-Netzwerk eine Peering-Verbindung zu nur einer VPC. Wenn Sie ein Transit-Gateway mit einer VPC verbinden, die mit einem ODB-Netzwerk verbunden ist, können Sie mehrere Verbindungen VPCs zu diesem Gateway herstellen. Anwendungen, die in diesen verschiedenen Umgebungen ausgeführt werden, VPCs können auf einen Exadata-VM-Cluster zugreifen, der in Ihrem ODB-Netzwerk läuft.

Das folgende Diagramm zeigt ein Transit-Gateway, das mit zwei VPCs und einem lokalen Netzwerk verbunden ist.

Im obigen Diagramm wird eine VPC per Peering mit einem ODB-Netzwerk verbunden. In dieser Konfiguration kann das ODB-Netzwerk den Verkehr an alle Personen weiterleiten, die an das Transit-Gateway VPCs angeschlossen sind. Die Routentabelle für jede VPC umfasst sowohl die lokale Route als auch Routen, die den für das ODB-Netzwerk bestimmten Verkehr an das Transit-Gateway senden.

In werden Ihnen die Anzahl der Verbindungen AWS Transit Gateway, die Sie pro Stunde zum Transit-Gateway herstellen, und die Menge des durchfließenden Datenverkehrs in Rechnung gestellt. AWS Transit Gateway Informationen zu den Kosten finden Sie unter AWS Transit Gateway Preise.

Voraussetzungen

Stellen Sie sicher, dass Ihre Oracle Database@AWS Umgebung die folgenden Anforderungen erfüllt:

- Die VPC, die mit Ihrem ODB-Netzwerk verbunden ist, muss sich in demselben befinden. AWS-Konto Wenn sich die Peering-VPC in einem anderen Konto als dem ODB-Netzwerk befindet, schlagen Transit-Gateway-Anhänge unabhängig von den Freigabekonfigurationen fehl.
- Die VPC, die mit Ihrem ODB-Netzwerk verbunden ist, muss über eine Transit-Gateway-Verbindung verfügen.

> **Note**
>
> Wenn das Transit-Gateway für die gemeinsame Nutzung konfiguriert ist, kann es sich in einem beliebigen Konto befinden. Somit muss sich das Gateway selbst nicht im selben Konto wie das VPC- und ODB-Netzwerk befinden.

- Der Transit-Gateway-Anhang muss sich in derselben Availability Zone (AZ) wie das ODB-Netzwerk befinden.

Einschränkungen

Beachten Sie die folgenden Einschränkungen von Amazon VPC Transit Gateways für: Oracle Database@AWS

- Amazon VPC Transit Gateways bietet keine native Integration zur Verwendung eines ODB-Netzwerks als Anhang. Daher sind VPC-Funktionen wie die folgenden nicht verfügbar:
  - Auflösung von öffentlichen DNS-Hostnamen in private IP-Adressen
  - Ereignisbenachrichtigung bei Änderungen der ODB-Netzwerktopologie, des Routings und des Verbindungsstatus
- Multicast-Verkehr zum ODB-Netzwerk wird nicht unterstützt.

Einrichtung und Konfiguration eines Transit-Gateways

Sie erstellen und konfigurieren ein Transit-Gateway mithilfe der Amazon VPC-Konsole oder `aws ec2` Befehle. Beim folgenden Verfahren wird davon ausgegangen, dass Sie kein ODB-Netzwerk haben, das mit einer VPC in Ihrem verbunden ist. AWS-Konto Wenn in Ihrem Konto bereits ein ODB-Netzwerk und eine VPC miteinander verbunden sind, überspringen Sie die Schritte 1—3.

> **Note**
>
> Wenn Sie die Anlagen an Ihre VPC anhängen oder erneut anhängen, stellen Sie sicher, dass Sie die CIDR-Bereiche erneut in das ODB-ODB-Netzwerk eingeben.

Um ein Transit-Gateway einzurichten und zu konfigurieren für Oracle Database@AWS

1. Erstellen Sie ein ODB-Netzwerk. Weitere Informationen finden Sie unter Schritt 1: Erstellen Sie ein ODB-Netzwerk in Oracle Database@AWS.
2. Erstellen Sie eine VPC mit demselben Konto, das das ODB-Netzwerk enthält. Weitere Informationen finden Sie unter Create a VPC im Amazon VPC-Benutzerhandbuch.
3. Erstellen Sie eine ODB-Peering-Verbindung zwischen Ihrem ODB-Netzwerk und Ihrer VPC. Weitere Informationen finden Sie unter Konfiguration von ODB-Peering zu einer Amazon VPC in der Oracle-Datenbank@AWS.
4. Richten Sie ein Transit-Gateway ein, indem Sie die Schritte unter Erste Schritte mit der Verwendung von Amazon VPC Transit Gateways befolgen. Das Gateway muss sich entweder im selben Netzwerk AWS-Konto wie das ODB-Netzwerk und die VPC befinden oder von einem anderen Konto gemeinsam genutzt werden.

   > **Important**
   >
   > Erstellen Sie den Transit-Gateway-Anhang in derselben AZ wie das ODB-Netzwerk.

5. Fügen Sie Ihrem ODB-Netzwerk CIDR-Bereiche für die Netzwerke VPCs und die lokalen Netzwerke hinzu, die Sie an Ihr Kernnetzwerk anschließen möchten. Weitere Informationen finden Sie unter Aktualisierung eines ODB-Netzwerks in Oracle Database@AWS.

   Wenn Sie die CLI verwenden, führen Sie den Befehl `update-odb-network` mit `--peered-cidrs-to-be-added` und aus`--peered-cidrs-to-be-removed`. Weitere Informationen finden Sie in der AWS CLI -Befehlsreferenz.

Konfiguration von AWS Cloud WAN für Oracle Database@AWS

AWS Cloud WAN ist ein verwalteter WAN-Dienst (Wide Area Networking). Sie können AWS Cloud WAN verwenden, um ein einheitliches globales Netzwerk aufzubauen, zu verwalten und zu überwachen, das Ressourcen verbindet, die in Ihren Cloud- und lokalen Umgebungen ausgeführt werden.

In AWS Cloud WAN ist ein globales Netzwerk ein einzelnes, privates Netzwerk, das als High-Level-Container für Ihre Netzwerkobjekte fungiert. Ein Kernnetzwerk ist der Teil Ihres globalen Netzwerks, der von verwaltet wird AWS.

AWS Cloud-WAN bietet die folgenden Hauptvorteile:

- Zentralisiertes Netzwerkmanagement, das den Betrieb vereinfacht und gleichzeitig die Sicherheit in mehreren Regionen gewährleistet
- Kernnetzwerke mit integrierter Segmentierung zur Isolierung des Datenverkehrs über mehrere Routingdomänen
- Support von Richtlinien zur Automatisierung des Netzwerkmanagements und zur Definition konsistenter Konfigurationen in Ihrem globalen Netzwerk

In Oracle Database@AWS unterstützt ein ODB-Netzwerk Peering nur zu einer VPC. Wenn Sie ein AWS Cloud-WAN-Kernnetzwerk mit einer Peering-VPC verbinden, wird globales Datenverkehrs-Routing aktiviert. Anwendungen, die VPCs über mehrere Regionen verteilt sind, können auf Exadata-VM-Cluster in Ihrem ODB-Netzwerk zugreifen. Sie können den ODB-Netzwerkverkehr in einem eigenen Segment isolieren oder den Zugriff auf andere Segmente ermöglichen.

Das folgende Diagramm zeigt ein AWS Cloud-WAN-Kernnetzwerk, das mit drei VPCs und einem lokalen Netzwerk verbunden ist.

AWS Cloud WAN bietet keine native Integration zur Verwendung eines ODB-Netzwerks als Anhang. Daher sind VPC-Funktionen wie die folgenden nicht verfügbar:

- Auflösung von öffentlichen DNS-Hostnamen in private IP-Adressen
- Ereignisbenachrichtigung bei Änderungen der ODB-Netzwerktopologie, des Routings und des Verbindungsstatus

In AWS Cloud WAN wird Ihnen Folgendes stündlich in Rechnung gestellt:

- Anzahl der Regionen (zentrale Netzwerk-Edges)
- Anzahl der Kernnetzwerkanschlüsse
- Die Menge des Datenverkehrs, der über die Anlagen durch Ihr Kernnetzwerk fließt

Detaillierte Preisinformationen finden Sie unter AWS Cloud-WAN-Preise.

Um ein Kernnetzwerk zu konfigurieren für Oracle Database@AWS

1. Fügen Sie Ihrem ODB-Netzwerk CIDR-Bereiche für die VPCs und lokalen Netzwerke hinzu, die Sie an Ihr Kernnetzwerk anschließen möchten. Weitere Informationen finden Sie unter Aktualisierung eines ODB-Netzwerks in Oracle Database@AWS.

> **Note**
>
> Wenn Sie die Anlagen an Ihre VPC anhängen oder erneut anhängen, stellen Sie sicher, dass Sie die CIDR-Bereiche erneut in das ODB-ODB-Netzwerk eingeben.

2. Folgen Sie den Schritten unter Globales AWS Cloud-WAN-Netzwerk und Kernnetzwerk erstellen.

Gemeinsame Nutzung von Rechten in Oracle Database@AWS

Mit Oracle Database@AWS können Sie AWS Marketplace-Berechtigungen für Oracle Database@AWS innerhalb AWS-Konten derselben Organisation gemeinsam nutzen. AWS Auf diese Weise können andere Konten mithilfe Ihres Abonnements ihre eigene Oracle Exadata-Infrastruktur und ihre eigenen ODB-Netzwerkressourcen bereitstellen.

Freigabemethoden

Oracle Database@AWS unterstützt zwei Methoden für die gemeinsame Nutzung:

Teilen von Rechten mit AWS License Manager

- Gewähren Sie anderen Konten die Möglichkeit, ihre eigene Oracle Exadata-Infrastruktur und ihre eigenen ODB-Netzwerkressourcen bereitzustellen
- Jedes Konto arbeitet unabhängig und bietet die volle Kontrolle über den Ressourcenlebenszyklus
- Am besten geeignet, um die Self-Service-Bereitstellung für Teams oder Geschäftsbereiche zu ermöglichen

Gemeinsame Nutzung von Ressourcen mit AWS Resource Access Manager ()AWS RAM

- Teilen Sie bereits bereitgestellte Oracle Exadata-Infrastruktur- und ODB-Netzwerkressourcen
- Zentralisieren Sie das Infrastrukturmanagement und ermöglichen Sie Empfängerkonten gleichzeitig die Erstellung von VM-Clustern
- Optimieren Sie die Kosten, indem mehrere Konten dieselbe Infrastruktur verwenden

Je nach den Anforderungen Ihres Unternehmens können Sie beide Methoden zur gemeinsamen Nutzung gleichzeitig verwenden.

Einschränkungen für Oracle Database@AWS Entitlement Sharing

Beachten Sie bei der gemeinsamen Nutzung von Oracle AWS Database@-Berechtigungen die folgenden Einschränkungen:

- Sie können die Daten nur innerhalb Ihrer Organisation teilen AWS-Konten AWS
- Sie können es nicht mit einer gesamten Organisationseinheit (OU) oder der gesamten Organisation teilen
- Einem Konto können nur Rechte von einem Käuferkonto (aus einem privaten Angebot) zugeteilt werden
- Ein Käuferkonto kann keine Ansprüche mit einem anderen Käuferkonto teilen
- Empfängerkonten müssen den Oracle AWS Database@-Service initialisieren, bevor sie den gemeinsamen Anspruch nutzen können
- Operationen zur Gewährung von Ansprüchen können nur von der Region USA Ost (Nord-Virginia) aus durchgeführt werden

Oracle AWS Database@-Berechtigungen kontenübergreifend teilen

Um die Zusammenarbeit zu ermöglichen und gleichzeitig die Kosten zu optimieren, sollten Sie Oracle AWS Database@-Berechtigungen mit anderen AWS-Konten innerhalb derselben Organisation teilen. AWS In diesem Thema wird erklärt, wie Sie Berechtigungen mithilfe von AWS License Manager gemeinsam nutzen können.

Voraussetzungen für die gemeinsame Nutzung von Berechtigungen

Bevor Sie Oracle AWS Database@-Berechtigungen gemeinsam nutzen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Ein aktives Oracle AWS Database@-Abonnement (Sie müssen das Käuferkonto sein, über das das private Angebot angenommen wurde) AWS Marketplace
- Die IDs AWS Konten in Ihrer Organisation, mit denen Sie Rechte teilen möchten
- Erforderliche Berechtigungen für Lizenzgeber und Empfänger zur Nutzung von AWS License Manager-Ressourcen und -Vorgängen (weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für License Manager im AWS License Manager Manager-Benutzerhandbuch)
- Die unten aufgeführten Berechtigungen gelten für Sie (Gewährer) und den Empfänger des Anspruchs (Empfänger)

Für die gemeinsame Nutzung von Ansprüchen sind Berechtigungen erforderlich

Zusätzlich zu den AWS License Manager Manager-Berechtigungen AWS benötigt Oracle Database@ die folgenden Berechtigungen:

Erteiler-Berechtigungen

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

Berechtigungen des Erteilten

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

Oracle AWS Database@-Berechtigungen mithilfe von License Manager mit einem anderen Konto teilen AWS

Um Rechte mit einem anderen AWS Konto zu teilen, erstellen Sie mit AWS License Manager einen Zuschuss. Weitere Informationen finden Sie unter Verteilen von License Manager Manager-Berechtigungen im AWS License Manager Manager-Benutzerhandbuch.

Nachdem Sie den Zuschuss erstellt haben, muss der Empfänger (Empfänger):

- Akzeptieren und aktivieren Sie den Zuschuss. Weitere Informationen finden Sie unter Annahme und Aktivierung von Grants in License Manager im AWS License Manager Manager-Benutzerhandbuch.
- Folgen Sie den Anweisungen zur Initialisierung für Oracle AWS Database@.

Nach Abschluss der Initialisierung kann der Empfänger mithilfe der gemeinsamen Berechtigung Oracle AWS Database@-Ressourcen bereitstellen.

Gemeinsame Nutzung von Ressourcen in der Oracle-Datenbank@AWS

Mit Oracle Database@AWS können Sie die Exadata-Infrastruktur und Ihr ODB-Netzwerk für mehrere Personen in derselben Organisation gemeinsam nutzen. AWS-Konten AWS Auf diese Weise können Sie die Infrastruktur einmal bereitstellen und sie für alle vertrauenswürdigen Konten wiederverwenden. So können Sie Kosten senken und gleichzeitig die Verantwortlichkeiten trennen.

Wenn Sie Ressourcen gemeinsam nutzen:

- Das Konto, dem die Ressource gehört (Besitzerkonto), behält die Kontrolle über den Ressourcenlebenszyklus.
- Konten, die Zugriff auf gemeinsam genutzte Ressourcen (vertrauenswürdige Konten) erhalten, können diese Ressourcen auf der Grundlage der erteilten Berechtigungen einsehen und verwenden.
- Vertrauenswürdige Konten können ihre eigenen Ressourcen in einer gemeinsam genutzten Infrastruktur erstellen, die zugrunde liegenden gemeinsam genutzten Ressourcen jedoch nicht löschen.

Integration von Oracle Database@AWS mit AWS RAM

Oracle Database@AWS verwendet AWS Resource Access Manager (AWS RAM), um eine sichere, kontrollierte gemeinsame Nutzung von Ressourcen zwischen Konten zu ermöglichen. Mit AWS RAM können Sie Ihre Oracle AWS Database@-Ressourcen sicher für mehrere AWS Konten innerhalb derselben Organisation gemeinsam nutzen. AWS AWS RAM vereinfacht die gemeinsame Nutzung von Ressourcen, reduziert den betrieblichen Aufwand und bietet Sicherheit und Transparenz in gemeinsam genutzten Oracle AWS Database@-Ressourcen.

Mit können Sie Ressourcen AWS RAM, die Ihnen gehören, gemeinsam nutzen, indem Sie eine gemeinsame Nutzung erstellen. Eine Ressourcenfreigabe gibt an, welche Ressourcen gemeinsam genutzt werden sollen und AWS-Konten mit wem sie gemeinsam genutzt werden sollen.

Vorteile der gemeinsamen Nutzung von Ressourcen in Oracle Database@AWS

Die gemeinsame Nutzung von Oracle AWS Database@-Ressourcen durch mehrere Konten bietet die folgenden Vorteile:

- Kostenoptimierung — Stellen Sie die teure Exadata-Infrastruktur einmalig über ein Administratorkonto bereit und teilen Sie sie mit mehreren Konten, wodurch die Gesamtkosten gesenkt werden.
- Trennung der Zuständigkeiten — Sorgen Sie für klare Grenzen zwischen Infrastrukturadministratoren und Datenbankbenutzern und ermöglichen Sie gleichzeitig die Zusammenarbeit.
- Vereinfachtes Management — Zentralisieren Sie die Bereitstellung und Verwaltung der Infrastruktur und ermöglichen Sie gleichzeitig verteilte Datenbankoperationen.
- Konsistente Verwaltung — Wenden Sie konsistente Richtlinien und Kontrollen für gemeinsam genutzte Ressourcen an.

Ein Administrator kann beispielsweise die Oracle Exadata-Infrastruktur und das ODB-Netzwerk in seinem Konto bereitstellen AWS-Konto und es mit Entwicklerkonten teilen. Entwickler können dann VM-Cluster auf dieser gemeinsam genutzten Infrastruktur erstellen, ohne ihre eigene teure Hardware bereitstellen zu müssen. Dieser Ansatz reduziert die Kosten erheblich und gewährleistet gleichzeitig eine korrekte Trennung der Verantwortlichkeiten zwischen den Konten.

So funktioniert die gemeinsame Nutzung von Ressourcen in Oracle Database@AWS

Sie können die folgenden Oracle AWS Database@-Ressourcen gemeinsam nutzen:

- Oracle Exadata-Infrastruktur
- ODB-Netzwerk

Oracle Database@ nutzt AWS die vorherigen Ressourcen über den folgenden Prozess gemeinsam:

1. Das Käuferkonto (das Konto, das das AWS private Angebot von Oracle Database@ über AWS Marketplace annimmt) stellt Oracle AWS Database@-Ressourcen wie die Exadata-Infrastruktur und ein ODB-Netzwerk bereit.
2. Das Käuferkonto erstellt eine gemeinsame Nutzung von Ressourcen und gibt dabei die Ressourcen an AWS RAM, die gemeinsam genutzt werden sollen, und die vertrauenswürdigen Konten, mit denen sie geteilt werden sollen.
3. Die gemeinsam genutzten Ressourcen für die vertrauenswürdigen Konten innerhalb derselben Organisation werden automatisch akzeptiert.
4. Vor der Verwendung gemeinsam genutzter Ressourcen müssen vertrauenswürdige Konten den Oracle AWS Database@-Dienst in ihrem Konto initialisieren, indem sie den `aws odb initialize-service` Befehl verwenden oder in der Oracle Database@-Konsole Konto aktivieren wählen.AWS
5. Nach der Initialisierung können vertrauenswürdige Konten ihre eigenen Ressourcen in der gemeinsam genutzten Infrastruktur erstellen, z. B. VM-Cluster in der gemeinsam genutzten Exadata-Infrastruktur und im ODB-Netzwerk.

Berechtigungen für gemeinsam genutzte Ressourcen für vertrauenswürdige Konten

Wenn Sie Ressourcen gemeinsam nutzen, wählt Oracle Database@AWS automatisch bestimmte Aktionen (verwaltete Berechtigungen) für jeden Ressourcentyp aus:

Für die Exadata-Infrastruktur

Oracle Database@AWS gewährt vertrauenswürdigen Konten die folgenden Berechtigungen:

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

Für das ODB-Netzwerk

Vertrauenswürdigen Konten werden die folgenden Berechtigungen gewährt:

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

Bei der gemeinsamen Nutzung von Ressourcen wird der hierarchische Charakter der Oracle AWS Database@-Ressourcen berücksichtigt. Wenn Sie beispielsweise die Exadata-Infrastruktur gemeinsam nutzen, können vertrauenswürdige Konten VM-Cluster auf dieser Infrastruktur erstellen, aber sie können die Exadata-Infrastruktur selbst nicht ändern oder löschen.

Wenn eine Ressource nicht gemeinsam genutzt wird, verlieren vertrauenswürdige Konten die Möglichkeit, neue Ressourcen in der gemeinsam genutzten Infrastruktur zu erstellen. Alle Ressourcen, die sie bereits erstellt haben, bleiben jedoch zugänglich und funktionsfähig.

Einschränkungen für die gemeinsame Nutzung von Oracle Database@ Ressourcen AWS

Bevor Sie Ressourcen gemeinsam nutzen, sollten Sie die folgenden Einschränkungen beachten.

Einschränkungen beim Teilen von Ressourcen

Beachten Sie bei der gemeinsamen Nutzung von Oracle AWS Database@-Ressourcen die folgenden Einschränkungen:

- Sie können Ressourcen nur mit teilen. AWS-Konto IDs
- Sie können Ressourcen nur AWS-Konten innerhalb derselben AWS Organisation gemeinsam nutzen.
- Sie teilen sich Ressourcen innerhalb einer bestimmten AWS Region. Um Ressourcen regionsübergreifend gemeinsam zu nutzen, müssen Sie in jeder Region separate Ressourcenfreigaben einrichten.

- Wenn Sie eine Ressourcenfreigabe erstellen, werden die Aktionen (verwaltete Berechtigungen) für jeden Ressourcentyp automatisch ausgewählt und können nicht geändert werden.
- Sie können Oracle Database@ nicht AWS als Ressource verwenden und mit anderen teilen. AWS-Konten
- Ein vertrauenswürdiges Konto kann gemeinsam genutzte Ressourcen von nur einem Käuferkonto (aus einem privaten Angebot) verwenden. Somit können sich zwei Käuferkonten keine Ressourcen mit demselben vertrauenswürdigen Konto teilen.
- Ein Käuferkonto kann Ressourcen nicht mit einem anderen Käuferkonto teilen.
- Ressourcen, die mit einem vertrauenswürdigen Konto geteilt werden, müssen zuerst vom Käuferkonto in der Heimatregion des Käufers gemeinsam genutzt werden.
- Wenn Sie die gemeinsame Nutzung einer Ressource beenden, empfehlen wir Ihnen, etwa 15 Minuten zu warten, bevor Sie dieselbe Ressource erneut mit demselben vertrauenswürdigen Konto teilen.

Einschränkungen bei der Erstellung und Verwendung gemeinsam genutzter Ressourcen

Beachten Sie beim Erstellen oder Verwenden von Oracle AWS Database@-Ressourcen die folgenden Einschränkungen:

- Nur das Käuferkonto kann Exadata-Infrastruktur und ODB-Netzwerkressourcen erstellen. Das Käuferkonto ist das Konto, das das private Angebot von Oracle AWS Database@ akzeptiert.
- Vertrauenswürdige Konten können Ressourcen nur auf der Exadata-Infrastruktur erstellen, die vom Käuferkonto gemeinsam genutzt wird.
- Vertrauenswürdige Konten müssen den Oracle AWS Database@-Service in ihrem Konto initialisieren, bevor sie gemeinsam genutzte Ressourcen verwenden können.

Einschränkungen beim Löschen gemeinsam genutzter Ressourcen

- Sie können eine Exadata-Infrastruktur mit VM-Clustern, die von vertrauenswürdigen Konten erstellt wurden, erst löschen, wenn diese VM-Cluster entfernt wurden.
- Sie können ein ODB-Netzwerk mit einer ODB-Peering-Verbindung, die von einem vertrauenswürdigen Konto erstellt wurde, erst löschen, wenn die ODB-Peering-Verbindung entfernt wurde.

- Das Käuferkonto kann keine Oracle AWS Database@-Ressourcen löschen, die von vertrauenswürdigen Konten erstellt wurden.
- Vertrauenswürdige Konten können gemeinsam genutzte Ressourcen anzeigen, aber keine Oracle AWS Database@-Ressourcen ändern oder löschen, die dem Käuferkonto gehören.

Oracle Database@AWS Ressourcen über Konten hinweg teilen

Um die Zusammenarbeit zu ermöglichen und gleichzeitig die Kosten zu optimieren, teilen Sie Oracle AWS Database@-Ressourcen mit anderen AWS-Konten innerhalb derselben AWS Organisation. In diesem Thema wird erklärt, wie Ressourcen mithilfe von AWS Resource Access Manager ()AWS RAM gemeinsam genutzt werden.

Themen

- Voraussetzungen für die gemeinsame Nutzung von Ressourcen
- Gemeinsame Nutzung von Oracle AWS Database@-Ressourcen mit einem anderen Konto mithilfe von AWS RAM
- Ihre Ressourcenfreigaben anzeigen
- Aktualisieren oder Löschen von Ressourcenfreigaben mit AWS RAM

Voraussetzungen für die gemeinsame Nutzung von Ressourcen

Bevor Sie Oracle AWS Database@-Ressourcen gemeinsam nutzen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Ein aktives Oracle AWS Database@-Abonnement (Sie müssen das Käuferkonto sein, über das das private Angebot angenommen wurde) AWS Marketplace
- Die IDs oder die Namen der Ressourcen, die Sie gemeinsam nutzen möchten, z. B. die Exadata-Infrastruktur oder ODB-Netzwerke
- Die IDs AWS Konten in Ihrer Organisation, für die Sie Ressourcen gemeinsam nutzen möchten
- Erforderliche Berechtigungen zum Erstellen von Ressourcenfreigaben in AWS RAM
- Die Möglichkeit, Ressourcen gemeinsam zu AWS Organizations nutzen AWS RAM (weitere Informationen finden Sie unter Aktivieren der gemeinsamen Nutzung von Ressourcen AWS Organizations im AWS Resource Access Manager Benutzerhandbuch)

Gemeinsame Nutzung von Oracle AWS Database@-Ressourcen mit einem anderen Konto mithilfe von AWS RAM

Um eine Exadata-Infrastruktur oder ein ODB-Netzwerk mit einem anderen AWS Konto gemeinsam zu nutzen, erstellen Sie eine Ressourcenfreigabe mit. AWS RAM Dadurch kann das vertrauenswürdige Konto VM-Cluster auf Ihrer Exadata-Infrastruktur erstellen.

Konsole

1. Öffnen Sie die AWS RAM Konsole unter. https://console.aws.amazon.com/ram/
2. Wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus.
3. Geben Sie unter Name einen aussagekräftigen Namen für Ihre Ressourcenfreigabe ein.
4. Unter Ressourcentyp auswählen eine der folgenden Ressourcen:
   - Oracle-Datenbank@ ODB-Netzwerk AWS
   - Oracle-Datenbank@ Exadata-Infrastruktur AWS
5. Wählen Sie die Exadata-Infrastrukturressourcen aus, die Sie gemeinsam nutzen möchten. Wählen Sie Weiter, bis Sie zu Grant access to principals gelangen.
6. Wählen Sie unter Principals das AWS Konto aus AWS-Konten, mit dem Sie Inhalte teilen möchten, und geben IDs Sie es ein.
7. Wählen Sie unter Verwaltete Berechtigungen die folgenden Berechtigungen aus, damit das vertrauenswürdige Konto VM-Cluster auf der gemeinsam genutzten Exadata-Infrastruktur erstellen kann:
   - AWSRAMDefaultBerechtigungODBNetwork
   - AWSRAMDefaultBerechtigungODBCloudExadataInfrastructure
8. Wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus.

AWS CLI

Verwenden Sie den Befehl AWS CLI, um Ressourcen mithilfe von gemeinsam zu nutzen. `aws ram create-resource-share` Im folgenden Beispiel wird eine Ressourcenfreigabe mit dem Namen erstellt`ExadataInfraShare`, die die angegebene Exadata-Infrastruktur gemeinsam mit dem Konto 222222222222 verwendet, sodass dieses Konto VM-Cluster auf der gemeinsam genutzten Infrastruktur erstellen kann.

```
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
```

Ihre Ressourcenfreigaben anzeigen

So siehst du die Ressourcen, die du geteilt hast, und die Konten, mit denen du sie geteilt hast:

Konsole

1. Öffnen Sie die AWS RAM Konsole unter https://console.aws.amazon.com/ram/.
2. Wählen Sie Geteilte Ressourcen, um Ressourcen anzuzeigen, die Sie mit anderen Konten geteilt haben.
3. Wählen Sie eine Ressourcenfreigabe aus, um deren Details anzuzeigen, einschließlich der gemeinsam genutzten Ressourcen und der Prinzipale, mit denen sie geteilt wurden.

AWS CLI

Verwenden Sie den `get-resource-shares` folgenden Befehl AWS CLI, um Ihre Ressourcenfreigaben mithilfe von anzuzeigen:

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

Verwenden Sie den `list-resources` folgenden Befehl, um die Ressourcen in einer bestimmten Ressourcenfreigabe anzuzeigen:

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

Verwenden Sie den `list-principals` folgenden Befehl, um die Principals (Konten) anzuzeigen, mit denen eine Ressourcenfreigabe gemeinsam genutzt wird:

```
aws ram list-principals \
    --resource-owner SELF \
```

```
    --resource-share-arns arn:aws:ram:us-east-1:111111111111:resource-share/12345678-
abcd-1234-efgh-111111111111
```

Aktualisieren oder Löschen von Ressourcenfreigaben mit AWS RAM

Um die gemeinsame Nutzung einer Ressource mit einem vertrauenswürdigen Konto zu beenden AWS RAM, führen Sie eine der folgenden Aktionen durch:

- Entfernen Sie die Ressource aus der Ressourcenfreigabe.
- Entfernen Sie das vertrauenswürdige Konto aus der Ressourcenfreigabe.
- Löschen Sie die Ressourcenfreigabe.

Bevor Sie den Zugriff auf eine gemeinsam genutzte Ressource widerrufen oder sie löschen, sollten Sie die folgenden Auswirkungen berücksichtigen:

- Vertrauenswürdige Konten können in der nicht gemeinsam genutzten Infrastruktur keine neuen Ressourcen mehr erstellen.
- Bestehende Ressourcen, die durch vertrauenswürdige Konten in der gemeinsam genutzten Exadata-Infrastruktur erstellt wurden, funktionieren weiterhin und sind für diese weiterhin zugänglich. AWS-Konten
- Sie können eine Exadata-Infrastruktur mit VM-Clustern, die von vertrauenswürdigen Konten erstellt wurden, erst löschen, wenn diese VM-Cluster entfernt wurden.

Bevor Sie die gemeinsame Nutzung von Ressourcen beenden, empfehlen wir Ihnen, sich mit den vertrauenswürdigen Konten abzustimmen, um einen reibungslosen Übergang zu gewährleisten.

Weitere Informationen finden Sie unter Aktualisieren einer Ressourcenfreigabe in AWS RAM und Löschen einer Ressourcenfreigabe AWS RAM in im AWS Resource Access Manager Benutzerhandbuch.

Initialisierung Oracle Database@AWS in einem vertrauenswürdigen Konto

Ein vertrauenswürdiges Konto ist ein Konto AWS-Konto , das Sie als berechtigt bezeichnen, Resource Shares zu erhalten. Es muss sich um eine andere Person AWS-Konto in Ihrer AWS Organisation handeln. Bevor Sie gemeinsam genutzte Oracle AWS Database@-Ressourcen in

einem vertrauenswürdigen Konto verwenden können, müssen Sie den Dienst initialisieren. Die Initialisierung erstellt die erforderlichen Metadaten und stellt die Verbindung zwischen Ihrer AWS-Konto und der Oracle Cloud Infrastructure her.

Themen

- Was ist die Oracle AWS Database@-Initialisierung?
- Nächste Schritte

Was ist die Oracle AWS Database@-Initialisierung?

Nachdem eine Ressource mit Ihrem Konto gemeinsam genutzt wurde, müssen Sie den Oracle AWS Database@-Service initialisieren, bevor Sie auf die gemeinsam genutzte Ressource zugreifen oder sie verwenden können. Wenn Sie versuchen, Oracle Database@ zu verwenden,AWS APIs ohne zuerst den Dienst zu initialisieren, erhalten Sie eine Fehlermeldung.

Die Initialisierung ist ein einmaliger Vorgang. Es erstellt die erforderlichen Metadaten und stellt eine Verbindung zwischen Ihrer AWS-Konto und der Oracle Cloud Infrastructure her.

Sie können den Dienst entweder mit der AWS Management Console oder dem AWS CLI initialisieren.

Konsole

1. Öffnen Sie die Oracle AWS Database@-Konsole unter. https://console.aws.amazon.com/odb/
2. Wenn Sie mit diesem Konto zum ersten Mal auf die Oracle AWS Database@-Konsole zugreifen, wird eine Willkommensseite angezeigt.
3. Wählen Sie Konto aktivieren.
4. Der Initialisierungsprozess für den Dienst beginnt. Es kann einige Minuten dauern, bis dieser Vorgang abgeschlossen ist.
5. Aktualisieren Sie die Willkommensseite regelmäßig, bis aus der Schaltfläche Konto aktivieren die Schaltfläche Dashboard wird.
6. Wählen Sie Dashboard, um mit der Nutzung von Oracle Database@AWS zu beginnen.

AWS CLI

Um Oracle Database@AWS in Ihrem vertrauenswürdigen Konto mit dem zu initialisieren, verwenden Sie den AWS CLI Befehl. `initialize-service`

```
aws odb initialize-service
```

Verwenden Sie den Befehl, um den Initialisierungsstatus zu überprüfen. `get-oci-onboarding-status`

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

Wenn die Initialisierung abgeschlossen ist, zeigt die Ausgabe den Status an`ACTIVE_LIMITED`, was bedeutet, dass Ihr Konto auf gemeinsam genutzte Ressourcen zugreifen kann, aber keine neue Exadata-Infrastruktur oder ein neues ODB-Netzwerk erstellen kann.

Nächste Schritte

Nachdem Sie Oracle Database@AWS in Ihrem vertrauenswürdigen Konto initialisiert haben, können Sie Folgendes tun:

- Zeigen Sie gemeinsam genutzte Ressourcen mit den `get` Befehlen `list` und oder in der Konsole an. AWS
- Erstellen Sie VM-Cluster und autonome VM-Cluster auf einer gemeinsam genutzten Exadata-Infrastruktur und einem gemeinsamen ODB-Netzwerk.
- Erstellen Sie eine ODB-Peering-Verbindung in einem gemeinsam genutzten ODB-Netzwerk.

Weitere Hinweise zum Arbeiten mit gemeinsam genutzten Ressourcen finden Sie unter. Arbeiten mit gemeinsam genutzten Oracle Database@AWS Ressourcen in einem vertrauenswürdigen Konto

Arbeiten mit gemeinsam genutzten Oracle Database@AWS Ressourcen in einem vertrauenswürdigen Konto

Nachdem eine Ressource für Ihr vertrauenswürdiges Konto freigegeben wurde und Sie den Oracle AWS Database@-Service initialisiert haben, können Sie die gemeinsam genutzte Ressource anzeigen und verwenden. In diesem Thema wird erklärt, wie Sie mit gemeinsam genutzten Ressourcen in einem vertrauenswürdigen Konto arbeiten.

Themen

- Einschränkungen für gemeinsam genutzte Ressourcen in einem vertrauenswürdigen Konto

- Erstellen von VM-Clustern auf einer gemeinsam genutzten Exadata-Infrastruktur
- Geteilte Ressourcen in einem vertrauenswürdigen Konto anzeigen
- ODB-Peering mit gemeinsam genutzten ODB-Netzwerken einrichten

Einschränkungen für gemeinsam genutzte Ressourcen in einem vertrauenswürdigen Konto

Beachten Sie bei der Arbeit mit gemeinsam genutzten Oracle AWS Database@-Ressourcen die folgenden Einschränkungen:

- Die gemeinsame Nutzung von Ressourcen wird nur innerhalb derselben AWS Organisation unterstützt.
- Nur das Käuferkonto (das Konto, das das AWS private Angebot von Oracle Database@ akzeptiert) kann die Exadata-Infrastruktur und ODB-Netzwerkressourcen erstellen.
- Sie können Ressourcen nur auf einer gemeinsam genutzten Infrastruktur und nur dann erstellen, wenn Sie über die erforderlichen Berechtigungen verfügen.
- Die spezifischen Aktionen (verwaltete Berechtigungen) für jeden Ressourcentyp werden bei der Erstellung einer Ressourcenfreigabe automatisch ausgewählt und können nicht geändert werden.
- Sie können keine Ressourcen ändern oder löschen, die einem anderen Konto gehören.
- Ressourcen, die Sie auf einer gemeinsam genutzten Infrastruktur erstellen, gehören Ihrem Konto und werden auf Ihre OCI-Kontingente angerechnet. Das Gleiche gilt für übergeordnete Ressourcen.
- Wenn das Besitzerkonto die gemeinsame Nutzung einer Ressource aufhebt, können Sie in dieser gemeinsam genutzten Infrastruktur keine neuen Ressourcen mehr erstellen. Ihre vorhandenen Ressourcen funktionieren jedoch weiterhin.
- Die regionsübergreifende gemeinsame Nutzung von Ressourcen wird nicht unterstützt. Sie können Ressourcen nur innerhalb derselben AWS Region gemeinsam nutzen.
- Ressourcen für vertrauenswürdige Konten werden dem Käufer des Oracle AWS Database@-Abonnements in Rechnung gestellt.
- Wenn Sie eine gemeinsam genutzte Ressource verwenden, müssen Sie den Amazon-Ressourcennamen (ARN) angeben.

Erstellen von VM-Clustern auf einer gemeinsam genutzten Exadata-Infrastruktur

Wenn Ihr vertrauenswürdiges Konto Zugriff auf eine gemeinsam genutzte Exadata-Infrastruktur und ein gemeinsam genutztes ODB-Netzwerk hat, können Sie Exadata-VM-Cluster, autonome VM-Cluster oder ODB-Peerings auf dieser Infrastruktur erstellen.

> **Note**
>
> Wenn Sie eine Ressource verwenden, die für Sie gemeinsam genutzt wird, müssen Sie nicht nur die Ressourcen-ID angeben, sondern auch den Amazon-Ressourcennamen (ARN) angeben.

Konsole

1. Öffnen Sie die Oracle AWS Database@-Konsole unter. https://console.aws.amazon.com/odb/
2. Wählen Sie im Navigationsbereich Exadata VM Clusters oder Autonomous VM Clusters aus.
3. Wählen Sie VM-Cluster erstellen oder Autonomen VM-Cluster erstellen.
4. Wählen Sie für Exadata-Infrastruktur die gemeinsam genutzte Exadata-Infrastruktur aus, auf der Sie den VM-Cluster erstellen möchten.
5. Füllen Sie die verbleibenden Felder nach Bedarf für Ihre VM-Clusterkonfiguration aus.
6. Wählen Sie VM-Cluster erstellen oder Autonomen VM-Cluster erstellen.

AWS CLI

Verwenden Sie den folgenden Befehl, um einen VM-Cluster auf einer gemeinsam genutzten Exadata-Infrastruktur mithilfe von zu erstellen: AWS CLI`create-cloud-vm-cluster`

```
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..." \
```

Verwenden Sie den folgenden Befehl, um mit dem einen Autonomous VM-Cluster auf einer gemeinsam genutzten Exadata-Infrastruktur zu erstellen AWS CLI: `create-cloud-vm-cluster`

```
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
```

Der VM-Cluster wird auf der angegebenen gemeinsam genutzten Exadata-Infrastruktur erstellt und gehört Ihrem vertrauenswürdigen Konto.

Geteilte Ressourcen in einem vertrauenswürdigen Konto anzeigen

Sie können Ressourcen, die mit Ihrem Konto geteilt wurden, in der AWS Management Console oder im anzeigen AWS CLI.

Konsole

1. Öffnen Sie die Oracle AWS Database@-Konsole unter. https://console.aws.amazon.com/odb/
2. Wählen Sie im Navigationsbereich den Ressourcentyp aus, den Sie anzeigen möchten: Exadata-Infrastruktur oder ODB-Netzwerk.
3. In der Konsole werden Ressourcen angezeigt, die mit Ihnen geteilt wurden.
4. Wählen Sie eine gemeinsam genutzte Ressource aus, um deren Details anzuzeigen.

AWS CLI

Um gemeinsam genutzte Ressourcen mithilfe von anzuzeigen AWS CLI, verwenden Sie den entsprechenden `list` Befehl für den Ressourcentyp. Um beispielsweise die Exadata-Infrastruktur aufzulisten:

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

In der Antwort werden Ressourcen angezeigt, die mit Ihnen geteilt wurden.

Um detaillierte Informationen zu einer bestimmten gemeinsam genutzten Ressource zu erhalten, verwenden Sie den entsprechenden `get` Befehl mit der Ressourcen-ID:

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

ODB-Peering mit gemeinsam genutzten ODB-Netzwerken einrichten

Um die Kommunikation zwischen Ihren Anwendungen und Datenbanken in gemeinsam genutzten ODB-Netzwerken zu ermöglichen, können Sie ODB-Peering zwischen Ihrer VPC und dem gemeinsam genutzten ODB-Netzwerk einrichten. Weitere Informationen zum ODB-Peering finden Sie unter. Eine ODB-Peering-Verbindung in Oracle Database@ erstellen AWS

Konsole

1. Öffnen Sie die Oracle AWS Database@-Konsole unter. https://console.aws.amazon.com/odb/
2. Wählen Sie im Navigationsbereich ODB-Peering.
3. Wählen Sie ODB-Netzwerk-Peering erstellen.
4. Wählen Sie für ODB-Netzwerk das gemeinsam genutzte ODB-Netzwerk aus, mit dem Sie eine Peering-Verbindung herstellen möchten.
5. Wählen Sie für Peer-Netzwerk Ihre VPC aus.
6. Wählen Sie ODB-Netzwerk-Peering erstellen.

AWS CLI

Verwenden Sie den Befehl, um mithilfe des eine Netzwerk-Peering-Verbindung zwischen Ihrer VPC und einem gemeinsam genutzten ODB-Netzwerk herzustellen. AWS CLI`create-odb-peering-connection`

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

Nachdem Sie die Peering-Verbindung hergestellt haben, aktualisieren Sie Ihre Routentabellen, um den Verkehr zwischen den Peering-Netzwerken zu ermöglichen.

```
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-Datenbank verwalten@AWS

Sie können einige Oracle Database@AWS Ressourcen ändern und löschen, nachdem Sie sie erstellt haben.

Aktualisierung eines ODB-Netzwerks in Oracle Database@AWS

Sie können die folgenden ODB-Netzwerkressourcen aktualisieren:

- Der ODB-Netzwerkname
- Die Amazon VPC, die für den Aufbau einer ODB-Peering-Verbindung zum ODB-Netzwerk verwendet werden soll
- Die VPC-CIDR-Bereiche, die auf Exadata-Ressourcen im ODB-Netzwerk zugreifen können

> **Note**
>
> Durch die Angabe von CIDR-Bereichen beschränken Sie die Konnektivität auf die erforderlichen VPC-Subnetze, anstatt die gesamte VPC für das ODB-Netzwerk verfügbar zu machen.

In diesem Abschnitt wird davon ausgegangen, dass Sie bereits ein ODB-Netzwerk in erstellt haben. Schritt 1: Erstellen Sie ein ODB-Netzwerk in Oracle Database@AWS

Um ein ODB-Netzwerk zu aktualisieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Oracle Database@AWS Konsole unter https://console.aws.amazon.com/odb/.
2. Wählen Sie im linken Bereich ODB-Netzwerke aus.
3. Wählen Sie das Netzwerk aus, das Sie ändern möchten.
4. Wählen Sie Ändern aus.
5. (Optional) Geben Sie für den ODB-Netzwerknamen einen neuen Netzwerknamen ein. Der Name muss 1—255 Zeichen lang sein und mit einem alphabetischen Zeichen oder Unterstrich beginnen. Er darf keine aufeinanderfolgenden Bindestriche enthalten.

6. (Optional) Geben Sie für Peered CIDRs die CIDR-Bereiche der gepeerten VPC an, die Konnektivität zum ODB-Netzwerk benötigen. Um den Zugriff einzuschränken, empfehlen wir, die mindestens erforderlichen CIDR-Bereiche anzugeben.
7. (Optional) Aktivieren oder deaktivieren Sie für Configure Service Integrations Amazon S3 oder Zero-ETL.
8. Wählen Sie Weiter und dann Ändern.

Löschen eines ODB-Netzwerks in Oracle Database@AWS

Sie können ein ODB-Netzwerk löschen. In diesem Abschnitt wird davon ausgegangen, dass Sie bereits ein ODB-Netzwerk in erstellt haben. Schritt 1: Erstellen Sie ein ODB-Netzwerk in Oracle Database@AWS Sie können kein ODB-Netzwerk löschen, das derzeit von einem VM-Cluster verwendet wird.

Um ein ODB-Netzwerk zu löschen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Oracle Database@AWS Konsole unter https://console.aws.amazon.com/odb/.
2. Wählen Sie im linken Bereich ODB-Netzwerke aus.
3. Wählen Sie das Netzwerk aus, das Sie löschen möchten.
4. Wählen Sie Löschen aus.
5. (Optional) Wählen Sie Zugeordnete OCI-Ressourcen löschen, um die OCI-Ressourcen zu löschen, die zusammen mit dem ODB-Netzwerk erstellt wurden.
6. Geben Sie **`delete me`** in das Textfeld ein.
7. Wählen Sie Löschen aus.

Löschen eines VM-Clusters in Oracle Database@AWS

Sie können einen Exadata-VM-Cluster oder einen Autonomen VM-Cluster löschen. In diesem Abschnitt wird davon ausgegangen, dass Sie bereits einen VM-Cluster in erstellt haben. Schritt 3: Erstellen Sie einen Exadata-VM-Cluster oder einen Autonomous VM-Cluster in Oracle Database@AWS

Um einen VM-Cluster zu löschen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Oracle Database@AWS Konsole unter https://console.aws.amazon.com/odb/.
2. Wählen Sie im linken Bereich Exadata VM Clusters oder Autonomous VM Clusters aus.
3. Wählen Sie einen VM-Cluster zum Löschen aus.
4. Wählen Sie Löschen aus.
5. Wenn Sie dazu aufgefordert werden, geben Sie die Eingabe ein **`delete me`** und wählen Sie dann Löschen.

Löschen einer Oracle Exadata-Infrastruktur in Oracle Database@AWS

Sie können eine Oracle Exadata-Infrastruktur löschen. In diesem Abschnitt wird davon ausgegangen, dass Sie bereits eine Oracle Exadata-Infrastruktur in erstellt haben. Schritt 2: Erstellen Sie eine Oracle Exadata-Infrastruktur in Oracle Database@AWS Sie können keine Exadata-Infrastruktur löschen, die derzeit von einem VM-Cluster verwendet wird.

Um eine Oracle Exadata-Infrastruktur zu löschen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Oracle Database@AWS Konsole unter. https://console.aws.amazon.com/odb/
2. Wählen Sie im linken Bereich Exadata-Infrastrukturen aus.
3. Wählen Sie eine Exadata-Infrastruktur zum Löschen aus.
4. Wählen Sie Löschen aus.
5. Wenn Sie dazu aufgefordert werden, geben Sie ein **`delete me`** und wählen Sie dann Löschen.

Löschen einer ODB-Peering-Verbindung

Wenn Sie eine ODB-Peering-Verbindung nicht mehr benötigen, können Sie sie löschen. Sie müssen alle ODB-Peering-Verbindungen löschen, bevor Sie ein ODB-Netzwerk löschen können.

Konsole

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die Oracle Database@AWS Konsole unter. https://console.aws.amazon.com/odb/
2. Wählen Sie im Navigationsbereich ODB-Peering-Verbindungen aus.
3. Wählen Sie die zu löschende ODB-Peering-Verbindung aus.
4. Wählen Sie Löschen aus.
5. Um den Löschvorgang zu bestätigen, geben Sie die Taste ein **`delete me`** und wählen Sie Löschen.

AWS CLI

Verwenden Sie den Befehl, um eine ODB-Peering-Verbindung zu löschen. `delete-odb-peering-connection`

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

In Oracle Database@ sichern AWS

Oracle Database@AWS bietet mehrere Backup-Optionen zum Schutz Ihrer Oracle-Datenbanken. Sie können von Oracle verwaltete Backups verwenden, die sich nahtlos in Amazon S3 integrieren lassen, oder Ihre eigenen benutzerverwalteten Backups mit Oracle Recovery Manager (RMAN) erstellen.

Von Oracle verwaltete Backups auf Amazon S3

Wenn Sie ein ODB-Netzwerk erstellen, konfiguriert Oracle Database@AWS automatisch den Netzwerkzugriff für von Oracle verwaltete Backups auf Amazon S3. OCI konfiguriert die erforderlichen DNS-Einträge und Sicherheitslisten. Diese Konfigurationen ermöglichen den Verkehr zwischen dem OCI Virtual Cloud Network (VCN) und Amazon S3. Das ODB-Netzwerk aktiviert oder steuert keine automatischen Backups.

Von Oracle verwaltete Backups werden vollständig von OCI verwaltet. Wenn Sie Ihre Oracle Exadata-Datenbank erstellen, können Sie automatische Backups aktivieren, indem Sie in der OCI-Konsole Automatische Backups aktivieren wählen. Wählen Sie eines der folgenden Backup-Ziele:

- Amazon S3
- OCI-Objektspeicher
- Autonomer Wiederherstellungsdienst

Weitere Informationen finden Sie unter Backup Exadata Database in der OCI-Dokumentation.

Benutzerverwaltete Backups auf Amazon S3 in Oracle Database@AWS

Mit Oracle Database@AWS können Sie mithilfe des Exadata Database Service auf einer dedizierten Infrastruktur benutzerverwaltete Backups Ihrer Datenbank erstellen. Sie sichern Ihre Daten mit Oracle Recovery Manager (RMAN) und speichern sie in Ihren Amazon S3 S3-Buckets. Sie haben die volle Kontrolle über die Planung von Backups, die Aufbewahrungsrichtlinien und die Speicherkosten und behalten gleichzeitig die Vorteile des Managed Services von Oracle Database@.AWS

> **Note**
>
> Oracle Database@ unterstützt AWS keine benutzerverwalteten Backups für Autonomous Database on Dedicated Infrastructure.

Benutzerverwaltete Backups ergänzen die AWS verwalteten Backup-Lösungen von Oracle Database@.AWS Sie können manuelle Backups für Compliance-Anforderungen, regionsübergreifende Notfallwiederherstellung oder zur Integration in bestehende Backup-Management-Workflows verwenden.

Sie können die folgenden benutzerverwalteten Backup-Techniken verwenden:

Oracle Secure Backup

Streamen Sie Backups mit optimaler Leistung direkt auf Amazon S3.

Storage Gateway

Verwenden Sie Storage Gateway für dateibasierte Backups, die eine NFS-Freigabe verwenden.

S3-Einhängepunkt

Verwenden Sie einen Dateiclient, um einen Amazon S3 S3-Bucket als lokales Dateisystem zu mounten.

Voraussetzungen für benutzerverwaltete Backups auf Amazon S3 in Oracle Database@AWS

Bevor Sie Ihre Oracle Exadata-Datenbanken auf Amazon S3 sichern können, gehen Sie wie folgt vor:

1. Ermöglichen Sie den direkten Zugriff auf Amazon S3 von Ihrem ODB-Netzwerk aus.
2. Konfigurieren Sie Netzwerkkonnektivität und Routing zwischen Oracle Database@AWS und Amazon S3.

Zugriff von Ihrem ODB-Netzwerk auf Amazon S3 aktivieren

Um Ihre Datenbank manuell auf Amazon S3 zu sichern, aktivieren Sie den direkten Zugriff auf S3 von Ihrem ODB-Netzwerk aus. Diese Technik ermöglicht Ihren Datenbanken den Zugriff auf Amazon S3

für Ihre Geschäftsanforderungen, z. B. für Datenimport/-export oder benutzerverwaltete Backups. Sie haben die volle Kontrolle über das Zielziel des Backup-Speichers und können mithilfe von Richtlinien den Zugriff auf Amazon S3 mithilfe von VPC Lattice einschränken.

Der direkte Zugriff auf Amazon S3 von Ihrem ODB-Netzwerk aus ist standardmäßig nicht aktiviert. Sie können den S3-Zugriff aktivieren, wenn Sie Ihr ODB-Netzwerk erstellen oder ändern.

Konsole

Um den direkten Zugriff auf Amazon S3 von Ihrem ODB-Netzwerk aus zu ermöglichen

1. Öffnen Sie die Oracle AWS Database@-Konsole unter. https://console.aws.amazon.com/odb/
2. Wählen Sie im Navigationsbereich ODB-Netzwerke aus.
3. Wählen Sie das ODB-Netzwerk aus, für das Sie den Amazon S3 S3-Zugriff aktivieren möchten.
4. Wählen Sie Ändern aus.
5. Wählen Sie Amazon S3.
6. (Optional) Konfigurieren Sie ein Amazon S3-Richtliniendokument, um den Zugriff auf Amazon S3 zu kontrollieren. Wenn Sie keine Richtlinie angeben, gewährt die Standardrichtlinie vollen Zugriff.
7. Wählen Sie Weiter und dann Ändern.

AWS CLI

Um den direkten Amazon S3 S3-Zugriff von Ihrem ODB-Netzwerk aus zu aktivieren, verwenden Sie den `update-odb-network` Befehl mit dem `s3-access` Parameter:

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

Verwenden Sie den folgenden `--s3-policy-document` Parameter, um ein Amazon S3 S3-Richtliniendokument zu konfigurieren:

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

Wenn der Amazon S3-Zugriff aktiviert ist, können Sie über Ihr ODB-Netzwerk auf Amazon S3 zugreifen, indem Sie das regionale DNS `s3.region.amazonaws.com` verwenden. OCI konfiguriert

diesen DNS-Namen standardmäßig. Um einen benutzerdefinierten DNS-Namen zu verwenden, ändern Sie Ihren VCN-DNS, um sicherzustellen, dass der benutzerdefinierte DNS auf die IP-Adresse des Servicenetzwerkendpunkts aufgelöst wird.

Konfiguration der Netzwerkkonnektivität zwischen Oracle Database@AWS und Amazon S3

Um benutzerverwaltete Backups auf Amazon S3 zuzulassen, muss Ihre VM auf den Amazon VPC-Endpunkt S3 zugreifen können. In der OCI-Konsole können Sie die Sicherheitsregeln in einer Netzwerksicherheitsgruppe (NSG) bearbeiten, um den eingehenden und ausgehenden Verkehr zu kontrollieren. Bei benutzerverwalteten Backups fließt der Datenverkehr über das Client-Subnetz und nicht über das Backup-Subnetz. In den folgenden Schritten aktualisieren Sie das NSGs Client-Subnetz, um die Ausgangsregel für die VPC-Endpunkt-IP-Adresse hinzuzufügen.

Um VM-Zugriff auf den Amazon S3 S3-Endpunkt zu ermöglichen

1. Öffnen Sie die Oracle AWS Database@-Konsole unter. https://console.aws.amazon.com/odb/
2. Wählen Sie ODB-Netzwerke.
3. Wählen Sie den Namen des ODB-Netzwerks.
4. Wählen Sie OCI-Ressourcen.
5. Wählen Sie den Tab Serviceintegrationen.
6. Beachten Sie unter Amazon S3 die folgenden Informationen:
   - Die IPv4 Adresse des Amazon VPC S3-Endpunkts. Sie benötigen diese Informationen später. Zum Beispiel könnte die IP-Adresse sein`192.168.12.223`.
   - Der Domainname des Amazon VPC S3-Endpunkts. Sie benötigen diese Informationen später. Zum Beispiel könnte der Domainname sein`s3.us-east-1.amazonaws.com`.
7. Wählen Sie im linken Navigationsbereich Exadata VM Clusters und dann Ihren VM-Clusternamen aus.
8. Wählen Sie oben auf der Seite die Registerkarte Zusammenfassung aus.
9. Wählen Sie Virtuelle Maschinen und dann den Namen Ihrer VM.
10. Notieren Sie sich den Wert im Feld DNS-Name. Dies ist der Hostname, den Sie angeben, wenn Sie eine Verbindung zu Ihrer VM herstellen`ssh`.
11. Wählen Sie oben rechts die Option In OCI verwalten aus. Dadurch wird die OCI-Konsole geöffnet.

12. Wählen Sie auf der Listenseite für virtuelle Cloud-Netzwerke die VCN aus, die die Netzwerksicherheitsgruppe (NSG) für das ODB-Netzwerkclient-Subnetz () enthält. `exa_static_nsg` Weitere Informationen finden Sie in der OCI-Dokumentation unter Sicherheitsregeln für eine NSG verwalten.
13. Führen Sie auf der Detailseite je nach der angezeigten Option eine der folgenden Aktionen aus:
    - Gehen Sie auf der Registerkarte Sicherheit zu Netzwerksicherheitsgruppen.
    - Wählen Sie unter Ressourcen die Option Netzwerksicherheitsgruppen aus.
14. Wählen Sie das NSG für das Client-Subnetz aus ()`exa_static_nsg`.
15. Fügen Sie eine Ausgangsregel für die VPC-Endpunktadresse hinzu, die Sie zuvor notiert haben.

Um die Konnektivität zu S3 von Ihrer VM aus zu testen

1. Verwenden Sie diese Option`ssh`, `root` um eine Verbindung zu der VM herzustellen, deren DNS-Namen Sie zuvor erhalten haben. Wenn Sie eine Verbindung herstellen, geben Sie eine `.pem` Datei mit Ihren SSH-Schlüsseln an.
2. Führen Sie die folgenden Befehle aus, um sicherzustellen, dass die VM auf den Amazon S3 S3-Amazon-VPC-Endpunkt zugreifen kann. Verwenden Sie den S3-Domainnamen, den Sie sich zuvor notiert haben.

```
# 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
```

Sicherung auf Amazon S3 mit Oracle Secure Backup

Oracle Secure Backup fungiert als SBT-Schnittstelle für die Verwendung mit Recovery Manager (RMAN). Sie können RMAN mit Oracle Secure Backup verwenden, um Ihre Oracle AWS Database@-Datenbanken direkt auf Amazon S3 zu sichern. Oracle Secure Backup bietet die folgenden Vorteile:

- Oracle Secure Backup optimiert den Datentransfer zwischen RMAN und S3.
- Es ist kein Zwischenspeicher für Backups erforderlich.
- Oracle Secure Backup verwaltet den Lebenszyklus Ihrer Backup-Medien.

So sichern Sie mit Oracle Secure Backup auf Amazon S3

1. Installieren Sie das Oracle Secure Backup-Modul auf Ihrem Exadata VM-Server. Ersetzen Sie die Platzhalterwerte durch Ihren AWS Zugriffsschlüssel und Ihren geheimen Zugriffsschlüssel. Weitere Informationen finden Sie in der Oracle-Dokumentation unter Backup to Cloud with Oracle Secure Backup Cloud Module.

```
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. Connect zu RMAN her und konfigurieren Sie den Backup-Kanal und den Standardgerätetyp.

```
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. Überprüfen Sie die Konfiguration.

```
RMAN> SHOW ALL;
```

4. Sichern Sie die Datenbank.

```
RMAN> BACKUP DATABASE;
```

5. Stellen Sie sicher, dass die Sicherung erfolgreich abgeschlossen wurde.

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

Sicherung auf Amazon S3 mithilfe von AWS Storage Gateway Amazon EC2

AWS Storage Gateway ist ein Hybridservice, der Ihre lokale Umgebung mit AWS Cloud Speicherdiensten verbindet. Für Oracle AWS Database@-Backups können Sie Storage Gateway verwenden, um einen dateibasierten Backup-Workflow zu erstellen, der direkt in Amazon S3 schreibt. Im Gegensatz zur Oracle Secure Backup-Technik verwalten Sie den Lebenszyklus der Backups.

In dieser Lösung erstellen Sie eine separate EC2 Amazon-Instance für die Konfiguration von Storage Gateway. Sie fügen auch ein Amazon EBS-Volume hinzu, um die Lese- und Schreibvorgänge in Amazon S3 zwischenzuspeichern.

Diese Technik bietet die folgenden Vorteile:

- Sie benötigen keinen Medienmanager wie Oracle Secure Backup.
- Es ist kein Zwischenspeicher für Backups erforderlich.

So stellen Sie Ihr Storage Gateway bereit und erstellen eine Dateifreigabe

1. Öffnen Sie AWS-Managementkonsole at https://console.aws.amazon.com/storagegateway/home/ und wählen Sie die AWS Region aus, in der Sie Ihr Gateway erstellen möchten.
2. Stellen Sie ein Amazon S3-File-Gateway bereit und aktivieren Sie es mit einer EC2 Amazon-Instance als Hub. Folgen Sie den Anweisungen unter Bereitstellen eines benutzerdefinierten EC2 Amazon-Hosts für S3 File Gateway im Storage Gateway Gateway-Benutzerhandbuch.

   Achten Sie bei der Konfiguration Ihres File-Gateways darauf, dass Sie wie folgt vorgehen:

   - Fügen Sie mindestens ein Amazon EBS-Volume für den Cache-Speicher mit einer Größe von mindestens 150 GiB hinzu.
   - Öffnen Sie TCP/UDP Port 2049 für den NFS-Zugriff in Ihrer Sicherheitsgruppe. Auf diese Weise können Sie NFS-Dateifreigaben erstellen.
   - Öffnen Sie den TCP-Port 80 für eingehenden Datenverkehr, um einen einmaligen HTTP-Zugriff während der Gateway-Aktivierung zu ermöglichen. Nach der Aktivierung können Sie diesen Port schließen.
3. Erstellen Sie einen Amazon VPC-Endpunkt für private Konnektivität zwischen Ihrem ODB-Netzwerk und dem Storage Gateway. Weitere Informationen finden Sie unter Zugreifen auf einen AWS Dienst über einen Schnittstellen-VPC-Endpunkt.
4. Erstellen Sie über die Storage Gateway Gateway-Konsole eine Dateifreigabe für Ihren Amazon S3 S3-Bucket. Weitere Informationen finden Sie unter Dateifreigabe erstellen.

Um Ihre Datenbank mit Storage Gateway auf Amazon S3 zu sichern

1. Verwenden Sie in einem Terminal, `ssh` um eine Verbindung zum DNS-Namen der Exadata-VM herzustellen. Informationen zum Ermitteln des DNS-Namens finden Sie unter. Voraussetzungen für benutzerverwaltete Backups auf Amazon S3 in Oracle Database@AWS

2. Erstellen Sie auf dem Exadata VM-Cluster-Server ein Verzeichnis für den NFS-Mount. Im folgenden Beispiel wird das Verzeichnis `/home/oracle/sgw_mount/` erstellt.

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

3. Mounten Sie die NFS-Freigabe in dem Verzeichnis, das Sie gerade erstellt haben. Im folgenden Beispiel wird die Freigabe für das Verzeichnis `/home/oracle/sgw_mount/` erstellt. *SG-IP-address*Ersetzen Sie es durch Ihre Storage Gateway Gateway-IP-Adresse und *your-bucket-name* durch den Namen Ihres S3-Buckets.

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

4. Connect zu RMAN her und sichern Sie die Datenbank im bereitgestellten Verzeichnis. Im folgenden Beispiel wird der Kanal erstellt `rman_local_bkp` und der Pfad zum Einhängepunkt verwendet, um die Sicherungsdateien zu formatieren.

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

5. Stellen Sie sicher, dass die Sicherungsdateien im Mount-Verzeichnis erstellt wurden. Das folgende Beispiel zeigt zwei Backup-Teile.

```
$ 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
```

Sicherung auf Amazon S3 mithilfe eines S3-Mountpoints

Sie können den Amazon S3-Mountpoint verwenden, um zuerst lokale Backups zu erstellen und sie dann auf Amazon S3 zu kopieren. Diese Technik erstellt Backups auf lokalem Speicher und überträgt sie dann über die Mount-Point-Schnittstelle an Amazon S3. Die Backup-Zeit ist länger als bei anderen Techniken, da Sie Daten zweimal sichern müssen.

> **Note**
>
> Direktes Backup auf Amazon S3 über den Mount Point ohne Staging wird nicht unterstützt. RMAN benötigt spezielle Dateisystemberechtigungen, die nicht mit der Amazon S3 S3-Mount-Point-Schnittstelle kompatibel sind.

Für diese Technik müssen Sie keinen Media Manager wie Oracle Secure Backup lizenzieren. Sie verwalten den Lebenszyklus Ihrer Backups.

Um mithilfe eines S3-Bereitstellungspunkts eine Sicherungskopie auf Amazon S3 zu erstellen

1. Verwenden Sie in einem Terminal, `ssh` um eine Verbindung zum DNS-Namen der Exadata-VM herzustellen. Informationen zum Ermitteln des DNS-Namens finden Sie unter. Voraussetzungen für benutzerverwaltete Backups auf Amazon S3 in Oracle Database@AWS
2. Installieren Sie den Amazon S3 S3-Mountpoint auf dem Exadata VM-Cluster-Server. Weitere Informationen zur Installation und Konfiguration finden Sie unter Mountpoint for Amazon S3 im Amazon S3 S3-Benutzerhandbuch.

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

3. Überprüfen Sie die Installation, indem Sie den `mount-s3` Befehl ausführen.

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

4. Erstellen Sie ein Zwischen-Backup-Verzeichnis auf dem lokalen Speicher des Exadata-VM-Clusterservers. Sie werden Ihre Datenbank in diesem lokalen Verzeichnis sichern und dann das Backup in Ihren S3-Bucket kopieren. Das folgende Beispiel erstellt ein Verzeichnis`/u02/rman_bkp_local`.

   ```
   mkdir /u02/rman_bkp_local
   ```

5. Erstellen Sie ein Verzeichnis für den Amazon S3 S3-Bereitstellungspunkt. Das folgende Beispiel erstellt ein Verzeichnis`/home/oracle/s3mount`.

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

6. Mounten Sie Ihren Amazon S3 S3-Bucket mithilfe des Bereitstellungspunkts. Im folgenden Beispiel wird ein S3-Bucket im Verzeichnis `/home/oracle/s3mount` bereitgestellt. *`your-s3-bucket-name`*Ersetzen Sie es durch Ihren tatsächlichen Amazon S3 S3-Bucket-Namen.

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

7. Stellen Sie sicher, dass Sie auf den Inhalt des Amazon S3 S3-Buckets zugreifen können.

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

8. Connect RMAN mit Ihrer Zieldatenbank und sichern Sie es in Ihrem lokalen Staging-Verzeichnis. Im folgenden Beispiel wird der Kanal erstellt `rman_local_bkp` und der Pfad verwendet, um die `/u02/rman_bkp_local/` Backup-Teile zu formatieren.

```
$ rman TARGET /

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

9. Stellen Sie sicher, dass die Backups im lokalen Verzeichnis erstellt wurden:

```
$ 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. Kopieren Sie die Sicherungsdateien aus dem lokalen Staging-Verzeichnis auf den Amazon S3 S3-Bereitstellungspunkt.

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

11. Stellen Sie sicher, dass Sie die Dateien erfolgreich auf Amazon S3 kopiert haben.

```
$ 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
```

Direkten Zugriff auf Amazon S3 deaktivieren

Wenn Sie von Ihrem ODB-Netzwerk aus keinen direkten Zugriff mehr auf Amazon S3 benötigen, können Sie ihn deaktivieren. Die Aktivierung oder Deaktivierung des direkten Netzwerkzugriffs auf S3 hat keinen Einfluss auf den Netzwerkzugriff auf von Oracle verwaltete Backups auf Amazon S3.

Konsole

Um den direkten Zugriff auf Amazon S3 zu deaktivieren

1. Öffnen Sie die Oracle AWS Database@-Konsole unter. https://console.aws.amazon.com/odb/
2. Wählen Sie im Navigationsbereich ODB-Netzwerke aus.
3. Wählen Sie das ODB-Netzwerk aus, für das Sie den Amazon S3 S3-Zugriff deaktivieren möchten.
4. Wählen Sie Ändern aus.
5. Deaktivieren Sie das Kontrollkästchen S3-Zugriff aktivieren.
6. Wählen Sie ODB-Netzwerk modifizieren.

AWS CLI

Verwenden Sie den Befehl `update-odb-network` mit dem Parameter `s3-access`.

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

Fehlerbehebung bei der Amazon S3 S3-Integration

Wenn Sie Probleme mit von Oracle verwalteten Backups auf Amazon S3 oder direktem Zugriff auf Amazon S3 haben, sollten Sie die folgenden Schritte zur Fehlerbehebung in Betracht ziehen:

Sie können von Ihrer Datenbank aus nicht auf Amazon S3 zugreifen

Überprüfen Sie, ob Folgendes der Fall ist:

- Stellen Sie sicher, dass der Amazon S3 S3-Zugriff für Ihr ODB-Netzwerk aktiviert ist. Verwenden Sie die `GetOdbNetwork` Aktion, um zu überprüfen, ob der `s3Access` Status lautet`Enabled`.
- Stellen Sie sicher, dass Sie den richtigen regionalen DNS-Namen verwenden:`s3.region.amazonaws.com`.
- Vergewissern Sie sich, dass Ihre Oracle-Datenbank über die erforderlichen Berechtigungen für den Zugriff auf Amazon S3 verfügt.

Von Oracle verwaltete Backups schlagen fehl

Überprüfen Sie, ob Folgendes der Fall ist:

- Von Oracle verwaltete Backups auf Amazon S3 sind standardmäßig aktiviert und können nicht deaktiviert werden. Wenn Backups fehlschlagen, überprüfen Sie die Oracle-Datenbankprotokolle auf spezifische Fehlermeldungen.
- Vergewissern Sie sich, dass die Amazon VPC Lattice-Ressourcen ordnungsgemäß konfiguriert sind, indem Sie sich die Service-Integrationsressourcen ansehen.
- Wenden Sie sich an den Oracle-Support, wenn Sie Hilfe bei Problemen mit Oracle Managed Automatic Backup benötigen. Weitere Informationen finden Sie unter Unterstützung für Oracle Database@ erhalten AWS.

Oracle Database@AWS Zero-ETL-Integration mit Amazon Redshift

Die Zero-ETL-Integration ist eine vollständig verwaltete Lösung, die Transaktions- und Betriebsdaten aus mehreren Quellen in Amazon Redshift verfügbar macht. Mit dieser Lösung können Sie Daten aus Ihren Oracle-Datenbanken, die auf Oracle Exadata oder Autonomous Database on Dedicated Exadata Infrastructure laufen, nach Amazon Redshift replizieren. Durch die automatische Synchronisation wird der herkömmliche ETL-Prozess (Extrahieren, Transformieren und Laden) vermieden. Sie ermöglicht auch Analysen und KI-Workloads in Echtzeit. Weitere Informationen finden Sie unter Null-ETL-Integrationen im Managementleitfaden zu Amazon Redshift.

Die Zero-ETL-Integration bietet die folgenden Vorteile:

- Datenreplikation in Echtzeit — Kontinuierliche Datensynchronisierung von Oracle-Datenbanken zu Amazon Redshift mit minimaler Latenz
- Eliminierung komplexer ETL-Pipelines — Es müssen keine kundenspezifischen Datenintegrationslösungen erstellt und verwaltet werden
- Geringerer Betriebsaufwand — Automatisierte Einrichtung und Verwaltung durch AWS APIs
- Vereinfachte Datenintegrationsarchitektur — Nahtlose Integration zwischen Oracle Database@AWS und Analysediensten AWS
- Verbesserte Sicherheit — Integrierte Verschlüsselung und AWS IAM-Zugriffskontrollen

Amazon Redshift erhebt keine zusätzlichen Gebühren für die Zero-ETL-Integration mit Oracle Database@.AWS Sie zahlen für die vorhandenen Amazon Redshift Redshift-Ressourcen, die zur Erstellung und Verarbeitung der im Rahmen einer Zero-ETL-Integration erstellten Änderungsdaten verwendet werden. Weitere Informationen finden Sie unter Amazon Redshift – Preise.

Unterstützte Datenbankversionen für die Zero-ETL-Integration in Oracle Database@AWS

Die Zero-ETL-Integration unterstützt die folgenden Oracle-Datenbankversionen:

- Oracle Exadata — Oracle-Datenbank 19c
- Autonome Datenbank auf einer dedizierten Infrastruktur — Oracle Database 19c und 23ai

So funktioniert die Zero-ETL-Integration in Oracle Database@AWS

Die Zero-ETL-Integration ermöglicht es Oracle Database@, Daten AWS auf Amazon Redshift zu replizieren. Die Integration nutzt Amazon VPC Lattice, um eine sichere Netzwerkkonnektivität zu schaffen. Die CDC-Technologie (Change Data Capture) gewährleistet die Datensynchronisierung in Echtzeit. Sie verwalten die Integration durch AWS Glue APIs.

Die Zero-ETL-Integrationsarchitektur umfasst Folgendes:

- Sichere Konnektivität — Verwendet SSL/TLS Verschlüsselung über TLS-Port 2484 für die Datenübertragung
- AWS Secrets Manager — Speichert Datenbankanmeldeinformationen und Zertifikate sicher mithilfe des AWS Key Management Service
- AWS Glue-Integration — Bietet eine einheitliche Verwaltungsoberfläche für Zero-ETL-Integrationen

Die Replikation erfolgt in den folgenden Schritten:

1. Herstellen einer sicheren Verbindung zur Oracle-Datenbank mithilfe von SSL auf Port 2484
2. Durchführen eines ersten vollständigen Dumps der ausgewählten Datenbanken, Schemas und Tabellen
3. Einrichtung von Change Data Capture (CDC) für die laufende Replikation in Echtzeit
4. Schreiben der replizierten Daten in den Amazon Redshift Redshift-Zielcluster

> **Important**
>
> Die Zero-ETL-Integration ist standardmäßig nicht aktiviert. Sie müssen es mit konfigurieren. AWS Glue APIs Sie können die Zero-ETL-Integration nicht direkt mit Oracle Database@ einrichten.AWS APIs

Voraussetzungen für die Zero-ETL-Integration in Oracle Database@AWS

Stellen Sie vor der Einrichtung der Zero-ETL-Integration sicher, dass Sie die folgenden Voraussetzungen erfüllen.

Allgemeine Voraussetzungen

- Oracle Database@AWS Setup — Stellen Sie sicher, dass mindestens ein VM-Cluster bereitgestellt wurde und ausgeführt wird.
- Integration mit aktiviertem Zero-ETL — Stellen Sie sicher, dass Ihr VM-Cluster oder Autonomous VM-Cluster mit einem ODB-Netzwerk verknüpft ist, für das Zero-ETL aktiviert ist.
- Unterstützte Oracle-Datenbankversionen — Sie müssen Oracle Database 19c (Oracle Exadata) oder Oracle Database 19c/23ai (Autonomous Database on Dedicated Infrastructure) verwenden.
- Gleiche AWS Region — Die Oracle-Quelldatenbank und der Amazon Redshift Redshift-Zielcluster müssen sich in derselben AWS Region befinden.

Voraussetzungen für die Oracle-Datenbank

Sie müssen Ihre Oracle-Datenbank mit den folgenden Einstellungen konfigurieren.

Einrichtung des Replikationsbenutzers

Erstellen Sie in jeder Pluggable Database (PDB), die Sie replizieren möchten, einen dedizierten Replikationsbenutzer:

- Für Oracle Exadata — Erstellen Sie einen Benutzer mit einem sicheren Passwort. `ODBZEROETLADMIN`
- Für Autonome Datenbanken auf einer dedizierten Infrastruktur — Verwenden Sie den vorhandenen `GGADMIN` Benutzer.

Erteilen Sie dem Replikationsbenutzer die folgenden Berechtigungen.

```
-- 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";
```

Zusätzliche Protokollierung

Aktivieren Sie die zusätzliche Protokollierung in Ihrer Oracle-Datenbank, um Änderungsdaten zu erfassen.

```
-- 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;
```

Um eine Zero-ETL-Integration zwischen Oracle Database@AWS und Amazon Redshift einzurichten, müssen Sie SSL konfigurieren.

Für Oracle Exadata-Datenbanken

Sie müssen SSL auf Port 2484 manuell konfigurieren. Diese Aufgabe umfasst Folgendes:

- Konfiguration `(PROTOCOL=tcps)(PORT=2484)` in `listener.ora`
- Einrichtung der Brieftasche mit `sqlnet.ora`
- Generierung und Konfiguration von SSL-Zertifikaten (siehe How To Configure SSL/TCPS For Exadata Cloud Database (exacc/EXACS) (Doc ID 2947301.1) in der My Oracle Support-Dokumentation)

Für autonome Datenbanken

SSL auf Port 2484 ist standardmäßig aktiviert. Es ist keine zusätzliche Konfiguration erforderlich.

> **Important**
>
> Der SSL-Port ist auf 2484 festgelegt.

AWS Voraussetzungen für den Service

Bevor Sie die Zero-ETL-Integration einrichten, richten Sie AWS Secrets Manager ein und konfigurieren Sie die IAM-Berechtigungen.

AWS Secrets Manager einrichten

Speichern Sie Ihre Anmeldeinformationen für die Oracle-Datenbank wie folgt in AWS Secrets Manager:

1. Erstellen Sie einen vom Kunden verwalteten Schlüssel (CMK) im AWS Key Management Service.
2. Speichern Sie Datenbankanmeldedaten mithilfe des CMK in AWS Secrets Manager.
3. Konfigurieren Sie Ressourcenrichtlinien, um den Zugriff auf Oracle Database@AWS zu ermöglichen.

Verwenden Sie die unter Unterstützte Verschlüsselungsmethoden für die Verwendung von Oracle als Quelle für den AWS Database Migration Service beschriebene Technik, um Ihre TDE-Schlüssel-ID und Ihr Kennwort abzurufen. Der folgende Befehl generiert das Base64-Wallet.

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

Das folgende Beispiel zeigt ein Geheimnis für Oracle Exadata. For *asm_service_name* *111.11.11.11* steht für die virtuelle IP für den VM-Knoten. Sie können den ASM-Listener auch bei SCAN registrieren.

```
{
  "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"
  }
}
```

Das folgende Beispiel zeigt ein Geheimnis für Autonomous Database on Dedicated Infrastructure.

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

Konfigurieren Sie die IAM-Berechtigungen.

Erstellen Sie IAM-Richtlinien, die Zero-ETL-Integrationsvorgänge ermöglichen. Die folgende Beispielrichtlinie ermöglicht die Beschreibung, Erstellung, Aktualisierung und Löschung von Vorgängen für einen Exadata-VM-Cluster. Verwenden Sie für einen autonomen VM-Cluster den Wert `cloud-autonomous-vm-cluster` anstelle von `cloud-vm-cluster` für den Ressourcen-ARN.

Überlegungen zur Zero-ETL-Integration in Oracle Database@AWS

Beachten Sie bei der Einrichtung der Zero-ETL-Integration zwischen Amazon Redshift Oracle Database@AWS und Amazon Redshift die folgenden Richtlinien:

Anfängliche Ladezeit der Daten

Die anfängliche Vollladezeit hängt von der Größe Ihrer Datenbank ab. Bei großen Datenbanken kann es mehrere Stunden oder Tage dauern, bis die erste Synchronisation abgeschlossen ist.

Leistung der Oracle-Datenbank

Die Erfassung von Änderungsdaten kann sich auf die Leistung der Oracle-Datenbank auswirken, insbesondere bei hohen Transaktionsvolumen. Überwachen Sie nach der Aktivierung der Zero-ETL-Integration die Leistung Ihrer Datenbank.

Schemaänderungen

Bei Änderungen der Data Definition Language (DDL) in der Oracle-Quelldatenbank müssen Sie möglicherweise manuell eingreifen, um die Integration neu zu erstellen. Planen Sie Schemaänderungen sorgfältig.

Allgemeine Überlegungen finden Sie unter Überlegungen zur Verwendung von Zero-ETL-Integrationen mit Amazon Redshift.

Einschränkungen für die Zero-ETL-Integration in Oracle Database@AWS

Beachten Sie die folgenden allgemeinen Einschränkungen:

Eine PDB pro Integration

Jede Zero-ETL-Integration kann nur Daten aus einer Pluggable Database (PDB) replizieren. Datenfilter wie werden nicht unterstützt. `include: pdb1.*.*, include: pdb2.*.*`

Eine einzige Integration pro autonomer Datenbank oder Exadata-Infrastruktur

Jede Zero-ETL-Integration kann nur Daten aus einer autonomen Datenbank auf einer dedizierten Infrastruktur replizieren.

Fester SSL-Port

SSL-Verbindungen müssen Port 2484 verwenden.

Gleiche Regionsanforderung

Der Quell-Cluster Oracle Database@AWS VM und der Amazon Amazon Redshift Redshift-Zielcluster müssen sich in derselben Region befinden. AWS Die regionsübergreifende Replikation wird nicht unterstützt.

Keine mTLS-Unterstützung

Mutual TLS (mTLS) wird nicht unterstützt. Wenn in Ihrer OCI-Datenbank mTLS aktiviert ist, müssen Sie es deaktivieren, um die Zero-ETL-Integration verwenden zu können.

Unveränderliche Integrationseinstellungen

Nachdem Sie den geheimen ARN- oder KMS-Schlüssel erstellt haben, der einer Integration zugeordnet ist, können Sie ihn nicht mehr ändern. Sie müssen die Integration löschen und neu erstellen, um diese Einstellungen zu ändern.

TDE-Verschlüsselung auf Spaltenebene

Transparente Datenverschlüsselung (TDE) auf Spaltenebene wird für Oracle Exadata-Datenbanken nicht unterstützt. Nur TDE auf Tablespace-Ebene wird unterstützt.

Datentypunterstützung

Einige Oracle-spezifische Datentypen werden möglicherweise nicht vollständig unterstützt oder müssen möglicherweise während der Replikation transformiert werden. Testen Sie Ihre spezifischen Datentypen gründlich, bevor Sie Ihre Datenbank für die Produktion einsetzen.

Einrichtung von Oracle AWS Database@-Integrationen mit Amazon Redshift

Gehen Sie wie folgt vor, um die Zero-ETL-Integration zwischen Ihrer Oracle-Datenbank und Amazon Redshift einzurichten:

1. Aktivieren Sie Zero-ETL in Ihrem ODB-Netzwerk.
2. Konfigurieren Sie die Voraussetzungen für die Oracle-Datenbank.
3. Richten Sie AWS Secrets Manager und AWS Key Management Service ein.
4. Konfigurieren Sie IAM-Berechtigungen.
5. Richten Sie Amazon Redshift Redshift-Ressourcenrichtlinien ein.
6. Erstellen Sie die Zero-ETL-Integration.
7. Erstellen Sie die Zieldatenbank in Amazon Redshift.

Schritt 1: Aktivieren Sie Zero-ETL für Ihr ODB-Netzwerk

Sie können die Zero-ETL-Integration für das ODB-Netzwerk aktivieren, das Ihrem Quell-VM-Cluster zugeordnet ist. Diese Integration ist standardmäßig deaktiviert.

Konsole

Um die Zero-ETL-Integration zu aktivieren

1. Öffnen Sie die Oracle AWS Database@-Konsole unter. https://console.aws.amazon.com/odb/
2. Wählen Sie im Navigationsbereich ODB-Netzwerke aus.
3. Wählen Sie das ODB-Netzwerk aus, für das Sie die Zero-ETL-Integration aktivieren möchten.
4. Wählen Sie Ändern aus.
5. Wählen Sie Zero-ETL aus.
6. Wählen Sie Weiter und dann Ändern.

AWS CLI

Um die Zero-ETL-Integration zu aktivieren, verwenden Sie den `update-odb-network` Befehl mit dem `--zero-etl-access` folgenden Parameter:

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

Verwenden Sie den Befehl, um die Zero-ETL-Integration für das ODB-Netzwerk zu aktivieren, das Ihrem Quell-VM-Cluster zugeordnet ist. `update-odb-network` Dieser Befehl konfiguriert die Netzwerkinfrastruktur, die für die Zero-ETL-Integration erforderlich ist.

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

Schritt 2: Konfigurieren Sie Ihre Oracle-Datenbank

Vervollständigen Sie die Oracle-Datenbankkonfiguration wie in den Voraussetzungen beschrieben:

- Erstellen Sie Replikationsbenutzer und gewähren Sie die erforderlichen Berechtigungen.

- Aktivieren Sie archivierte Redo-Logs.
- SSL konfigurieren (nur Oracle Exadata).
- Richten Sie gegebenenfalls ASM-Benutzer ein (nur Oracle Exadata).

Schritt 3: AWS Secrets Manager und AWS Key Management Service einrichten

Erstellen Sie einen vom Kunden verwalteten Schlüssel (CMK) und speichern Sie Ihre Datenbankanmeldeinformationen.

1. Erstellen Sie mit dem Befehl einen CMK im AWS Key Management Service. `create-key`

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

2. Speichern Sie Ihre Datenbankanmeldedaten in AWS Secrets Manager.

```
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. Fügen Sie dem Secret eine Ressourcenrichtlinie hinzu, um Oracle Database@AWS Zugriff zu gewähren.

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

`secret-resource-policy.json`Enthält im vorherigen Befehl den folgenden JSON-Code.

JSON

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

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

4. Hängen Sie eine Ressourcenrichtlinie an den CMK an. Die CMK-Ressourcenrichtlinie muss Berechtigungen sowohl für den Oracle Database@AWS Service Principal als auch für den Amazon Redshift Service Principal enthalten, um die verschlüsselte Zero-ETL-Integration zu unterstützen.

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

Die `cmk-resource-policy.json` Datei sollte die folgenden Richtlinienerklärungen enthalten. Die erste Anweisung ermöglicht den Zugriff auf den Oracle Database@AWS Service, und die zweite Anweisung ermöglicht Amazon Redshift, Grants für den KMS-Schlüssel für verschlüsselte Datenoperationen zu erstellen.

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"
          ]
        }
      }
    }
  ]
}
```

Schritt 4: IAM-Berechtigungen konfigurieren

Erstellen und fügen Sie IAM-Richtlinien hinzu, die Zero-ETL-Integrationsvorgänge ermöglichen.

```
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
```

Die folgende Richtlinie gewährt die erforderlichen Berechtigungen.

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": "*"
    }
  ]
}
```

Schritt 5: Amazon Redshift Redshift-Ressourcenrichtlinien konfigurieren

Richten Sie Ressourcenrichtlinien in Ihrem Amazon Redshift Redshift-Cluster ein, um eingehende Integrationen zu autorisieren.

```
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**
>
> Alternativ können Sie die Option Fix it for me in der Konsole verwenden. AWS Diese Option konfiguriert automatisch die erforderlichen Amazon Redshift Redshift-Richtlinien, ohne dass Sie dies manuell tun müssen.

Schritt 6: Erstellen Sie die Zero-ETL-Integration mit AWS Glue

Erstellen Sie die Zero-ETL-Integration mit dem Befehl. AWS Glue `create-integration` In diesem Befehl geben Sie den Quell-VM-Cluster und den Amazon Redshift Redshift-Ziel-Namespace an.

Das folgende Beispiel erstellt eine Integration mit einer PDB namens `pdb1` running in einem Exadata-VM-Cluster. Sie können auch einen autonomen VM-Cluster erstellen, indem Sie `cloud-vm-cluster` ihn `cloud-autonomous-vm-cluster` im Quell-ARN ersetzen. Die Angabe eines KMS-Schlüssels ist optional. Wenn Sie einen Schlüssel angeben, kann er sich von dem unterscheiden, in dem Sie ihn erstellt habenSchritt 3: AWS Secrets Manager und AWS Key Management Service einrichten.

```
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"
```

Der Befehl gibt einen Integrations-ARN zurück und setzt den Status auf`creating`. Sie können den Integrationsstatus mit dem `describe-integrations` Befehl überwachen.

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

> **Important**
>
> Pro Integration wird nur eine PDB unterstützt. Der Datenfilter muss beispielsweise eine einzelne PDB angeben. `include: pdb1.*.*` Die Quelle muss sich in derselben AWS Region und demselben Konto befinden, in der die Integration erstellt wird.

Schritt 7: Erstellen Sie eine Zieldatenbank in Amazon Redshift

Nachdem die Integration aktiv ist, erstellen Sie eine Zieldatenbank in Ihrem Amazon Redshift Redshift-Cluster.

```
-- 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";
```

Nachdem Sie die Zieldatenbank erstellt haben, können Sie die replizierten Daten abfragen.

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

```
-- Connect to the new database
\c target_database_name

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

Überprüfen Sie die Zero-ETL-Integration

Stellen Sie sicher, dass die Integration funktioniert, indem Sie den Integrationsstatus in abfragen AWS Glue und sicherstellen, dass Ihre Oracle-Änderungen auf Amazon Redshift repliziert werden.

Um zu überprüfen, ob Ihre Zero-ETL-Integration ordnungsgemäß funktioniert

1. Überprüfen Sie den Integrationsstatus.

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

   Der Status sollte `ACTIVE` oder sein`REPLICATING`.
2. Überprüfen Sie die Datenreplikation, indem Sie Änderungen an Ihrer Oracle-Datenbank vornehmen und überprüfen, ob sie in Amazon Redshift erscheinen.
3. Überwachen Sie die Replikationsmetriken in Amazon CloudWatch (falls verfügbar).

Datenfilterung für Zero-ETL-Integrationen in Oracle Database@AWS

Oracle Database@AWS Zero-ETL-Integrationen unterstützen die Datenfilterung. Sie können damit steuern, welche Daten Ihre Oracle Exadata-Quelldatenbank in Ihr Ziel-Data Warehouse repliziert. Anstatt die gesamte Datenbank zu replizieren, können Sie einen oder mehrere Filter anwenden, um bestimmte Tabellen ein- oder auszuschließen. Auf diese Weise können Sie die Speicher- und Abfrageleistung optimieren, da nur relevante Daten übertragen werden. Die Filterung ist auf Datenbank- und Tabellenebene beschränkt. Das Filtern auf Spalten- und Zeilenebene wird nicht unterstützt.

Oracle Database und Amazon Redshift behandeln die Groß-/Kleinschreibung von Objektnamen unterschiedlich, was sich sowohl auf die Datenfilterkonfiguration als auch auf Zielabfragen auswirkt. Beachten Sie Folgendes:

- Oracle Database speichert Datenbank-, Schema- und Objektnamen in Großbuchstaben, sofern sie nicht ausdrücklich in der `CREATE`-Anweisung zitiert werden. Wenn Sie beispielsweise `mytable` (ohne Anführungszeichen) erstellen, speichert das Oracle-Datenwörterbuch den Tabellennamen als `MYTABLE`. Wenn Sie den Objektnamen in Ihrer Erstellungsanweisung in Anführungszeichen setzen, behält das Oracle-Datenwörterbuch die Groß- und Kleinschreibung bei.
- Null-ETL-Datenfilter unterscheiden zwischen Groß- und Kleinschreibung und müssen genau der Groß- und Kleinschreibung von Objektnamen entsprechen, wie sie im Oracle-Datenwörterbuch vorkommen. Wenn das Oracle-Wörterbuch beispielsweise Schema und Tabellenname speichert`REINVENT.MYTABLE`, erstellen Sie einen Filter mit`include: ORCL.REINVENT.MYTABLE`.
- Amazon-Redshift-Abfragen verwenden standardmäßig Objektnamen in Kleinbuchstaben, sofern sie nicht ausdrücklich in Anführungszeichen gesetzt werden. Die Abfrage von `MYTABLE` (ohne Anführungszeichen) sucht beispielsweise nach `mytable`.

Beachten Sie die Unterschiede bei der Groß- und Kleinschreibung, wenn Sie den Amazon-Redshift-Filter erstellen und die Daten abfragen. Die Überlegungen zum Filtern Oracle Database@AWS sind dieselben wie für Amazon RDS for Oracle. Beispiele dafür, wie sich Case auf Datenfilter in einer Oracle-Datenbank auswirken kann, finden Sie unter RDS for Oracle-Beispiele im Amazon Relational Database Service User Guide.

Überwachung der Zero-ETL-Integration

Die regelmäßige Überwachung Ihrer Zero-ETL-Integration gewährleistet eine optimale Leistung und hilft, Probleme frühzeitig zu erkennen.

Überwachung des Integrationsstatus

Überwachen Sie den Status Ihrer Zero-ETL-Integrationen mit Glue. AWS APIs

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

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

Zu den Integrationsstatus gehören:

- erstellen — Die Integration wird eingerichtet
- aktiv — Die Integration läuft und repliziert Daten
- ändern — Die Integrationskonfiguration wird aktualisiert
- needs_attention — Die Integration erfordert manuelles Eingreifen
- fehlgeschlagen — Bei der Integration ist ein Fehler aufgetreten
- löschen — Die Integration wird entfernt

Überwachung der Leistung

Überwachen Sie die folgenden Aspekte Ihrer Zero-ETL-Integrationsleistung:

- Replikationsverzögerung — Der Zeitunterschied zwischen dem Zeitpunkt, an dem eine Änderung in Oracle erfolgt, und dem Zeitpunkt, an dem sie in Amazon Redshift erscheint
- Datendurchsatz — Das Datenvolumen, das pro Zeiteinheit repliziert wird
- Fehlerraten — Die Häufigkeit von Replikationsfehlern oder -ausfällen
- Ressourcenauslastung — CPU-, Arbeitsspeicher- und Netzwerkauslastung auf Quell- und Zielsystemen

Verwenden Sie Amazon CloudWatch , um diese Kennzahlen zu überwachen und Alarme für kritische Schwellenwerte einzurichten.

Verwaltung von Zero-ETL-Integrationen in Oracle Database@AWS

Nachdem Sie eine Zero-ETL-Integration erstellt haben, können Sie verschiedene Verwaltungsvorgänge ausführen, darunter das Ändern und Löschen von Integrationen. In diesem Abschnitt wird die laufende Verwaltung Ihrer Zero-ETL-Integrationen behandelt.

Ändern von Null-ETL-Integrationen

Sie können nur den Namen, die Beschreibung und die Datenfilteroptionen für eine Null-ETL-Integration in einem unterstützten Data Warehouse ändern. Sie können den AWS Key Management Service-Schlüssel, der zur Verschlüsselung der Integration verwendet wird, oder die Quell- oder Zieldatenbanken nicht ändern.

Voraussetzungen für das Ändern von Integrationen

Bevor Sie eine Zero-ETL-Integration ändern, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Erforderliche Berechtigungen — Ihr IAM-Benutzer oder Ihre IAM-Rolle muss zusätzlich zu den `odb:UpdateOutboundIntegration` Standardberechtigungen über die entsprechende Berechtigung verfügen. AWS Glue
- Integration im aktiven Status — Die Integration muss sich in einem `ACTIVE` Status befinden, nicht in`CREATING`, `MODIFYINGDELETING`, oder`FAILED`.
- Gültige Datenfiltersyntax — Neue Datenfilter müssen der unterstützten include/exclude Mustersyntax folgen.

Datenfilter ändern

Sie können ändern, welche Tabellen oder Schemas repliziert werden, indem Sie den Datenfilter ändern. Auf diese Weise können Sie Datenbankobjekte zur Replikation hinzufügen oder aus der Replikation entfernen, ohne die gesamte Integration neu erstellen zu müssen.

Verwenden Sie den `modify-integration` Befehl, um den Datenfilter für eine Integration zu ändern.

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

Sie können den Namen und die Beschreibung der Integration auch gleichzeitig ändern. Im folgenden Beispiel ändern Sie den Integrationsnamen, die Beschreibungen und die Filter für zwei Schemas in`pdb1`.

```
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**
>
> Wenn Sie den Datenfilter ändern, wechselt die Integration in einen `modifying` Status und führt eine Neusynchronisierung der Daten durch. Die Integration stoppt die Replikation,

wendet die neuen Filtereinstellungen an und setzt die Replikation mit einem Vorgang zum erneuten Laden des Ziels fort. Überwachen Sie den Integrationsstatus, um sicherzustellen, dass die Änderung erfolgreich abgeschlossen wird.

Überlegungen zu Datenfilteränderungen an Zero-ETL-Integrationen

Beachten Sie beim Ändern von Datenfiltern Folgendes:

- Beschränkung auf eine einzelne PDB — Sie können nur eine Pluggable Database (PDB) pro Integration angeben. Datenfilter wie werden nicht unterstützt `include: pdb1.*.*, include: pdb2.*.*`
- Unterbrechung der Replikation — Die Datenreplikation wird während des Änderungsvorgangs gestoppt und nach der Anwendung des neuen Filters wieder aufgenommen.
- Daten neu laden — Die Integration führt ein vollständiges Neuladen von Daten durch, die den neuen Filterkriterien entsprechen.
- Auswirkungen auf die Leistung — Große Datenfilteränderungen können viel Zeit in Anspruch nehmen und die Leistung der Quelldatenbank während des Neuladens beeinträchtigen.

Einschränkungen für Änderungen an den Zero-ETL-Integrationseinstellungen

Sie können die folgenden Einstellungen nicht ändern, nachdem Sie eine Zero-ETL-Integration erstellt haben:

- Secret ARN — Das AWS Secrets Manager-Geheimnis, das Datenbankanmeldedaten enthält
- KMS-Schlüssel — Der vom Kunden verwaltete Schlüssel, der für die Verschlüsselung verwendet wird
- Quell-ARN — Der Oracle Database@AWS VM-Cluster
- Ziel-ARN — Der Amazon Redshift Redshift-Cluster oder -Namespace

Um diese Einstellungen zu ändern, löschen Sie die bestehende Zero-ETL-Integration und erstellen Sie eine neue.

Löschen von Null-ETL-Integrationen

Wenn Sie eine Zero-ETL-Integration nicht mehr benötigen, können Sie sie löschen, um die Replikation zu beenden und die zugehörigen Ressourcen zu bereinigen.

Löschen mit AWS Glue

Löschen Sie eine Zero-ETL-Integration mithilfe der AWS Glue-API.

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

Sie können Integrationen in den folgenden Zuständen löschen:

- aktiv
- benötigt Aufmerksamkeit
- failed
- Synchronisieren

Auswirkungen des Löschens

Wenn Sie eine Zero-ETL-Integration löschen, sollten Sie die folgenden Auswirkungen berücksichtigen:

Die Replikation wird gestoppt.

Oracle Database@ repliziert AWS keine neuen Änderungen von Amazon Redshift.

Bestehende Daten werden beibehalten.

Daten, die bereits auf Amazon Redshift repliziert wurden, bleiben verfügbar.

Die Zieldatenbank bleibt bestehen.

Die aus der Integration erstellte Amazon Redshift Redshift-Datenbank wird nicht automatisch gelöscht.

> **Important**
>
> Das Löschen ist irreversibel. Wenn Sie die Replikation nach dem Löschen fortsetzen müssen, erstellen Sie eine neue Integration, die den vollen anfänglichen Ladevorgang durchführt.

Bewährte Methoden für ein Zero-ETL-Management

Folgen Sie diesen Best Practices, um eine optimale Leistung, Sicherheit und Wirtschaftlichkeit Ihrer Zero-ETL-Integrationen zu gewährleisten.

Bewährte betriebliche Verfahren

Diese betrieblichen Praktiken tragen dazu bei, zuverlässige und effiziente Zero-ETL-Integrationen aufrechtzuerhalten.

Regelmäßige Überwachung

: Richten Sie CloudWatch Alarme ein, um die Integrations- und Leistungskennzahlen zu überwachen.

Rotation der Anmeldeinformationen

: Wechseln Sie regelmäßig Datenbankkennwörter und aktualisieren Sie sie in AWS Secrets Manager.

Backup-Überprüfung

: Stellen Sie regelmäßig sicher, dass Ihre Oracle-Datenbank-Backups die für die Notfallwiederherstellung erforderlichen Komponenten enthalten.

Leistungstests

: Testen Sie die Auswirkungen der Zero-ETL-Integration auf die Leistung Ihrer Oracle-Datenbank, insbesondere in Spitzenzeiten.

Planung von Schemaänderungen

: Planen und testen Sie Schemaänderungen in einer Entwicklungsumgebung, bevor Sie sie in der Produktion anwenden.

Bewährte Methoden für die Gewährleistung der Sicherheit

Implementieren Sie diese Sicherheitsmaßnahmen, um Ihre Zero-ETL-Integration und Ihre Daten zu schützen.

Zugriff mit geringster Berechtigung

: Gewähren Sie Replikationsbenutzern und AWS IAM-Rollen nur die erforderlichen Mindestberechtigungen.

Netzwerksicherheit

Verwenden Sie Sicherheitsgruppen und NACLs beschränken Sie den Netzwerkzugriff nur auf die erforderlichen Ports und Quellen.

Verschlüsselung im Ruhezustand

Stellen Sie sicher, dass sowohl Oracle-Datenbanken als auch Amazon Redshift Redshift-Cluster Verschlüsselung im Ruhezustand verwenden.

Audit-Protokollierung

Aktivieren Sie die Audit-Protokollierung sowohl auf Oracle als auch auf Amazon Redshift, um Datenzugriffe und Änderungen nachzuverfolgen.

Geheime Verwaltung

Verwenden Sie nach Möglichkeit die automatischen Rotationsfunktionen von AWS Secrets Manager.

Kostenoptimierung

Wenden Sie diese Strategien an, um die Kosten zu optimieren und gleichzeitig eine effektive Zero-ETL-Integrationsleistung aufrechtzuerhalten.

Filterung von Daten

Verwenden Sie präzise Datenfilter, um nur die Daten zu replizieren, die Sie benötigen, und reduzieren Sie so die Speicher- und Rechenkosten.

Amazon Redshift Redshift-Optimierung

Verwenden Sie geeignete Amazon Redshift Redshift-Knotentypen und implementieren Sie Datenkomprimierung, um die Kosten zu optimieren.

Überwachung der Nutzung

Überprüfen Sie regelmäßig die Nutzung und die Kosten Ihrer Zero-ETL-Integration mit AWS Cost Explorer.

Bereinigen Sie ungenutzte Integrationen

Löschen Sie Integrationen, die nicht mehr benötigt werden, um laufende Gebühren zu vermeiden.

Fehlerbehebung bei der Zero-ETL-Integration

Dieser Abschnitt enthält Anleitungen zur Lösung häufiger Probleme bei der Zero-ETL-Integration.

Fehler bei der Einrichtung der Zero-ETL-Integration

Authentication failures (Authentifizierungsfehler)

- Stellen Sie sicher, dass der Replikationsbenutzer existiert und das richtige Passwort in AWS Secrets Manager hat.
- Stellen Sie sicher, dass dem Replikationsbenutzer alle erforderlichen Berechtigungen erteilt wurden.
- Stellen Sie sicher, dass der geheime ARN korrekt ist und dass Oracle AWS Database@ darauf zugreifen kann.
- Stellen Sie sicher, dass die CMK-Ressourcenrichtlinie den Zugriff durch den Oracle AWS Database@ Service Principal zulässt.

Probleme mit der Netzwerkkonnektivität

- Stellen Sie sicher, dass in Ihrem ODB-Netzwerk die Zero-ETL-Integration aktiviert ist.
- Stellen Sie sicher, dass SSL auf Port 2484 richtig konfiguriert ist (nur Exadata).
- Stellen Sie sicher, dass der Oracle-Datenbank-Listener läuft und Verbindungen akzeptiert.
- Stellen Sie sicher, dass Netzwerksicherheitsgruppen bestehen und NACLs Datenverkehr auf Port 2484 zugelassen ist.
- Stellen Sie sicher, dass der Dienstname in Ihrem Secret mit dem tatsächlichen Oracle-Dienstnamen übereinstimmt.

Berechtigungsfehler

- Vergewissern Sie sich, dass Ihr IAM-Benutzer oder Ihre IAM-Rolle über die erforderlichen Berechtigungen für AWS Glue Integrationsvorgänge verfügt.
- Stellen Sie sicher, dass die Amazon Redshift Redshift-Ressourcenrichtlinie eingehende Integrationen aus Ihrem VM-Cluster zulässt.
- Stellen Sie sicher, dass Oracle Database@ Zugriff auf Ihre Geheimnisse und AWS Ihren Key Management Service-Schlüssel erhalten AWS hat.

Probleme bei der Replikation

Fehler beim ersten Laden

- Stellen Sie sicher, dass die Oracle-Datenbank über ausreichende Ressourcen verfügt, um den Vollladevorgang zu unterstützen.
- Stellen Sie sicher, dass die zusätzliche Protokollierung in der Quelldatenbank aktiviert ist.
- Suchen Sie nach Sperren oder Einschränkungen auf Tabellenebene, die die Datenextraktion verhindern könnten.

Probleme bei der Erfassung von Änderungsdaten

- Stellen Sie sicher, dass die Oracle-Datenbank über ausreichend Speicherplatz und Aufbewahrung für Redo-Logs verfügt.
- Stellen Sie sicher, dass der Replikationsbenutzer Zugriff auf archivierte Redo-Logs hat.
- Stellen Sie bei ASM-fähigen Systemen sicher, dass der ASM-Benutzer richtig konfiguriert ist.
- Überwachen Sie die Leistung der Oracle-Datenbank, um sicherzustellen, dass CDC keine Ressourcenkonflikte verursacht.

Hohe Verzögerung bei der Replikation

- Überwachen Sie die Metriken zur Replikationsverzögerung in CloudWatch.
- Suchen Sie in der Quelldatenbank nach hohen Transaktionsvolumen oder großen Transaktionen.
- Stellen Sie sicher, dass der Amazon Redshift Redshift-Cluster über ausreichende Kapazität für die Verarbeitung eingehender Daten verfügt.

Probleme mit der Datenkonsistenz

Fehlende oder unvollständige Daten

- Stellen Sie sicher, dass der Datenfilter alle erforderlichen Schemas und Tabellen enthält.
- Suchen Sie nach nicht unterstützten Datentypen, die zu Replikationsfehlern führen können.
- Stellen Sie sicher, dass der Replikationsbenutzer über SELECT-Berechtigungen für alle erforderlichen Tabellen verfügt.

Fehler bei der Konvertierung des Datentyps

- Sehen Sie sich die unterstützten Datentypzuordnungen zwischen Oracle und Redshift an.
- Suchen Sie nach Oracle-spezifischen Datentypen, die möglicherweise eine benutzerdefinierte Behandlung erfordern.

- Erwägen Sie, Ihr Oracle-Schema zu ändern, um kompatiblere Datentypen zu verwenden.

Überwachung und Debugging

Verwenden Sie die folgenden Ansätze, um Probleme mit der Zero-ETL-Integration zu überwachen und zu debuggen:

- Überwachung des Integrationsstatus — Überprüfen Sie regelmäßig den Integrationsstatus mithilfe von. `aws glue describe-integrations`
- CloudWatch Metriken — Überwachen Sie die verfügbaren CloudWatch Metriken auf Replikationsleistung und Fehler.
- Oracle-Datenbanküberwachung — Überwachen Sie die Leistung und Ressourcennutzung der Oracle-Datenbank.
- Redshift-Überwachung — Überwachen Sie die Leistung und Speichernutzung des Amazon Redshift Redshift-Clusters.

Bei komplexen Problemen, die mit diesem Leitfaden zur Fehlerbehebung nicht gelöst werden können, wenden Sie sich AWS Support mit den folgenden Informationen an:

- Integrations-ARN und aktueller Status.
- Fehlermeldungen aus der Integration beschreiben Operationen.
- Oracle-Datenbank- und Amazon Redshift Redshift-Clusterkonfigurationen.
- Zeitleiste, wann das Problem auftrat.

Sicherheit in Oracle Database@AWS

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von OCI AWS und Ihnen. Das Modell der gemeinsamen Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS-Services in der läuft AWS Cloud. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, darunter die Sensibilität Ihrer Daten, die Anforderungen Ihres Unternehmens und die geltenden Gesetze und Vorschriften.

Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Ihnen bei der Überwachung und Sicherung Ihrer Oracle Database@AWS Ressourcen helfen.

Sie können den Zugriff auf Ihre Oracle Database@AWS Ressourcen verwalten. Die Methode, mit der Sie den Zugriff verwalten, hängt davon ab, welche Art von Aufgabe Sie ausführen müssen Oracle Database@AWS:

- Verwenden Sie AWS Identity and Access Management (IAM-) Richtlinien, um Berechtigungen zuzuweisen, die festlegen, wer Oracle Database@AWS Ressourcen verwalten darf. Sie können IAM beispielsweise verwenden, um zu bestimmen, wer Exadata-Infrastrukturen, VM-Cluster oder Tag-Ressourcen erstellen, beschreiben, ändern und löschen darf.
- Verwenden Sie die Sicherheitsfunktionen Ihrer Oracle-Datenbank-Engine, um zu kontrollieren, wer sich bei den Datenbanken einer DB-Instance anmelden kann. Diese Funktionen arbeiten genauso, als würden sich die Datenbanken in Ihrem lokalen Netzwerk befinden.
- Verwenden Sie Secure Socket Layers (SSL) - oder Transport Layer Security (TLS) -Verbindungen mit Exadata-Datenbanken. Weitere Informationen finden Sie unter Vorbereitung auf Walletless-Verbindungen mit TLS.
- Oracle Database@AWS ist nicht sofort über das Internet zugänglich und wird nur in privaten Subnetzen bereitgestellt. AWS

- Oracle Database@AWS verwendet viele standardmäßige TCP-Ports (Transmission Control Protocol) für verschiedene Operationen. Die vollständige Liste der Ports finden Sie unter Standardportzuweisungen.
- Zum Speichern und Verwalten von Schlüsseln mithilfe von Transparent Data Encryption (TDE), die standardmäßig aktiviert ist, werden OCI-Tresore oder Oracle Key Vault Oracle Database@AWS verwendet. Oracle Database@AWS unterstützt nicht. AWS Key Management Service
- Standardmäßig wird die Datenbank mithilfe von von Oracle verwalteten Verschlüsselungsschlüsseln konfiguriert. Die Datenbank unterstützt auch vom Kunden verwaltete Schlüssel.
- Verwenden Sie Oracle Data Safe mit Oracle Database@AWS, um den Datenschutz zu verbessern.

In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen Oracle Database@AWS , um Ihre Sicherheits- und Compliance-Ziele zu erreichen.

Topics

- Datenschutz in Oracle Database@AWS
- Identitäts- und Zugriffsmanagement für Oracle Database@AWS
- Konformitätsvalidierung für Oracle Database@AWS
- Resilienz in Oracle Database@AWS
- Verwenden von serviceverknüpften Rollen für Oracle Database@AWS
- Oracle Database@AWS Aktualisierungen der AWS verwalteten Richtlinien

Datenschutz in Oracle Database@AWS

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.

- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Oracle Database@AWS oder anderen Geräten arbeiten und dabei die Konsole, die API oder AWS-Services verwenden. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung

Exadata-Datenbanken verwenden Oracle Transparent Data Encryption (TDE), um Ihre Daten zu verschlüsseln. Ihre Daten sind auch in temporären Tablespaces, Undo-Segmenten, Redo-Logs und bei internen Datenbankoperationen wie JOIN und SORT geschützt. Weitere Informationen finden Sie unter Datensicherheit.

Verschlüsselung während der Übertragung

Exadata-Datenbanken verwenden native Verschlüsselungs- und Integritätsfunktionen von Oracle Net Services, um Verbindungen zur Datenbank zu sichern. Weitere Informationen finden Sie unter Sicherheit von Daten bei der Übertragung.

Schlüsselverwaltung

Die transparente Datenverschlüsselung umfasst einen Keystore zum sicheren Speichern von Master-Verschlüsselungsschlüsseln und ein Management-Framework zur sicheren und effizienten Verwaltung des Keystores und zur Durchführung wichtiger Wartungsvorgänge. Weitere Informationen finden Sie unter So verwalten Sie Vault-Verschlüsselungsschlüssel.

Identitäts- und Zugriffsmanagement für Oracle Database@AWS

AWS Identity and Access Management (IAM) ist ein AWS Dienst, der einem Administrator hilft, den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Oracle Database@-Ressourcen zu verwenden.AWS IAM ist ein AWS Service, den Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- Wie Oracle Database@AWS funktioniert mit IAM
- Identitätsbasierte Richtlinien für Oracle Database@AWS
- AWS verwaltete Richtlinien für Oracle Database@AWS
- Oracle Database@AWS Authentifizierung und Autorisierung in OCI
- Fehlerbehebung bei Oracle Database@AWS Identität und Zugriff

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Fehlerbehebung bei Oracle Database@AWS Identität und Zugriff).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe Wie Oracle Database@AWS funktioniert mit IAM).

- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Identitätsbasierte Richtlinien für Oracle Database@AWS).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für Verbundbenutzerzugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, dienstübergreifenden Zugriff und Anwendungen, die auf Amazon ausgeführt werden. EC2 Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an Identitäten oder Ressourcen anhängen. AWS Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können.

IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität (Benutzer, Gruppe oder Rolle) anfügen können. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mit mehreren Identitäten verbunden sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Richtlinien zur Dienstkontrolle (SCPs) — Geben Sie die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in an AWS Organizations. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.

- Richtlinien zur Ressourcenkontrolle (RCPs) — Legen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten fest. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Richtlinien zur Ressourcenkontrolle (RCPs).
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die daraus resultierenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

Wie Oracle Database@AWS funktioniert mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Oracle Database@ zu verwalten, sollten Sie sich darüber informieren AWS, welche IAM-Funktionen für die Verwendung mit Oracle Database@ verfügbar sind.AWS

IAM-Feature	Oracle Database@AWS Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja

IAM-Feature	Oracle Database@AWS Unterstützung
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Oracle Database@AWS und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für Oracle Database@AWS

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Oracle Database@AWS

Beispiele für AWS identitätsbasierte Richtlinien von Oracle Database@ finden Sie unter. Identitätsbasierte Richtlinien für Oracle Database@AWS

Ressourcenbasierte Richtlinien innerhalb Oracle Database@AWS

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und

Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für Oracle Database@AWS

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Eine Liste der Oracle Database@AWS Aktionen finden Sie unter Von Oracle Database@ definierte Aktionen AWS in der Service Authorization Reference.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix Oracle Database@AWS verwendet:

```
odb
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Beispiele für AWS identitätsbasierte Richtlinien von Oracle Database@ finden Sie unter. Identitätsbasierte Richtlinien für Oracle Database@AWS

Richtlinienressourcen für Oracle Database@AWS

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der Oracle Database@AWS Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Von Oracle Database@ definierte Ressourcen AWS in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von Oracle AWS Database@ definierte Aktionen.

Beispiele für AWS identitätsbasierte Richtlinien von Oracle Database@ finden Sie unter. Identitätsbasierte Richtlinien für Oracle Database@AWS

Schlüssel für Policy-Bedingungen für Oracle Database@AWS

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der Oracle Database@AWS Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Oracle Database@AWS in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Oracle Database@ definierte Aktionen.AWS

Beispiele für AWS identitätsbasierte Richtlinien von Oracle Database@ finden Sie unter. Identitätsbasierte Richtlinien für Oracle Database@AWS

ACLs in Oracle Database@AWS

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Oracle Database@AWS

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen, auch als Tags bezeichnet, definiert werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit Oracle Database@AWS

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie einen Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Serviceübergreifende Prinzipalberechtigungen für Oracle Database@AWS

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Prinzipals, der einen AWS Dienst aufruft, in Kombination mit dem anfordernden AWS Dienst, um Anfragen an nachgelagerte Dienste zu stellen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für Oracle Database@AWS

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen für einen AWS Dienst.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann zu Funktionseinschränkungen führen. Oracle Database@AWS Bearbeiten Sie Servicerollen nur, Oracle Database@AWS wenn Sie dazu eine Anleitung erhalten.

Dienstbezogene Rollen für Oracle Database@AWS

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einem AWS Dienst verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von Oracle Database@AWS dienstbezogenen Rollen finden Sie unter. Verwenden von serviceverknüpften Rollen für Oracle Database@AWS

Identitätsbasierte Richtlinien für Oracle Database@AWS

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Oracle AWS Database@-Ressourcen zu erstellen oder zu ändern. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von Oracle Database@ definierten Aktionen und Ressourcentypen AWS, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Oracle Database@AWS in der Service Authorization Reference.

Themen

- Best Practices für Richtlinien
- Verwenden der Oracle Database@AWS -Konsole
- Erlauben Sie Benutzern die Bereitstellung von Oracle Database@AWS Ressourcen
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Best Practices für Richtlinien

Identitätsbasierte Richtlinien bestimmen, ob jemand Oracle Database@-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann.AWS Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen

finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten AWS Dienst verwendet werden, z. CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Oracle Database@AWS -Konsole

Um auf die Oracle AWS Database@-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Oracle

AWS Database@-Ressourcen in Ihrem aufzulisten und anzuzeigen. AWS-Konto Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. AWS Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Erlauben Sie Benutzern die Bereitstellung von Oracle Database@AWS Ressourcen

Diese Richtlinie gewährt Benutzern vollen Zugriff auf die Bereitstellung von Oracle Database@AWS Ressourcen. Um die DNS-Auflösung von Ihrer VPC aus einzurichten, erstellen Sie einen ausgehenden Route 53-Resolver und fügen Sie Regeln hinzu, um DNS-Verkehr mit dem OCI-Domänennamen an die OCI-DNS-Listener-IP weiterzuleiten.

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": "*"
        }
    ]
}
```

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der OR-API. AWS CLI AWS

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

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

AWS verwaltete Richtlinien für Oracle Database@AWS

Um Berechtigungen zu Berechtigungssätzen und Rollen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS-Services verwalten und aktualisieren Sie AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Dienste fügen einer AWS verwalteten Richtlinie gelegentlich zusätzliche Berechtigungen hinzu, um neue Funktionen zu unterstützen. Diese Art von Update betrifft alle Identitäten (Berechtigungssätze und Rollen), denen die Richtlinie angehängt ist. Es ist sehr wahrscheinlich, dass Dienste eine AWS verwaltete Richtlinie aktualisieren, wenn eine neue Funktion eingeführt wird oder wenn neue Operationen verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die `ReadOnlyAccess` AWS verwaltete Richtlinie bietet beispielsweise nur Lesezugriff auf alle Ressourcen AWS-Services . Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

Themen

- AWS verwaltete Richtlinie: Amazon ODBService RolePolicy

AWS verwaltete Richtlinie: Amazon ODBService RolePolicy

Sie können die `AmazonODBServiceRolePolicy`-Richtlinie Ihren IAM-Entitäten nicht anfügen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es Oracle Database@AWS ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Oracle Database@AWS.

Weitere Informationen zur Richtlinie, einschließlich der neuesten Version des JSON-Richtliniendokuments, finden Sie unter Amazon ODBService RolePolicy im AWS Managed Policy Reference Guide.

Oracle Database@AWS Authentifizierung und Autorisierung in OCI

Wenn Sie Ressourcen für erstellen Oracle Database@AWS, befinden AWS APIs sich diese Ressourcen logischerweise in Ihrer verknüpften Oracle Cloud Infrastructure (OCI) -Tenancy. AWS Kommuniziert in Ihrem Namen mit OCI, um diese Ressourcen bereitzustellen. APIs Um das Problem mit dem verwirrten Stellvertreter zu lösen, autorisieren Sie Ihre Absicht, OCI in Ihrem verknüpften AWS STS Mandantenverhältnis zu Oracle Database@AWS verwenden und Zugriffssitzungen weiterzuleiten, um Ihre Absicht zu autorisieren, OCI APIs in Ihrem verknüpften Mietverhältnis zu verwenden. Folglich werden Ereignisse für die `sts:getCallerIdentity` API aus dem OCI-IP-Bereich in Ihren Trails und Ihrem Eventverlauf aufgezeichnet. AWS CloudTrail Erwarten Sie diese Ereignisse, wenn Sie sie verwenden Oracle Database@AWS APIs.

Fehlerbehebung bei Oracle Database@AWS Identität und Zugriff

Verwenden Sie die folgenden Informationen, um allgemeine Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Oracle Database@AWS und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in Oracle Database@AWS
- Ich bin nicht berechtigt, iam durchzuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Oracle Database@AWS Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion durchzuführen in Oracle Database@AWS

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `odb:`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `odb:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam durchzuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht autorisiert sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Oracle AWS Database@ übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Oracle Database@ auszuführen.AWS Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren Administrator. AWS Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Oracle Database@AWS Ressourcen ermöglichen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Oracle Database@ diese Funktionen AWS unterstützt, finden Sie unter. Wie Oracle Database@AWS funktioniert mit IAM
- Informationen darüber, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Zugriff auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Konformitätsvalidierung für Oracle Database@AWS

Ihre Verantwortung für die Einhaltung von Vorschriften bei der Verwendung von Oracle Database@AWS hängt von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. Die Dokumentation von Oracle zur Einhaltung von Vorschriften in der Cloud ist auf der Oracle-Website verfügbar

Resilienz in Oracle Database@AWS

Die AWS globale Infrastruktur basiert auf AWS-Regionen Availability Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz,

hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur AWS bietet Oracle Database@ mehrere Funktionen zur Unterstützung Ihrer Datenausfallsicherheit und Ihrer Backup-Anforderungen.

Verwenden von serviceverknüpften Rollen für Oracle Database@AWS

Oracle Database@AWS verwendet AWS Identity and Access Management (IAM) dienstbezogene Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. Oracle Database@AWS Mit Diensten verknüpfte Rollen sind vordefiniert Oracle Database@AWS und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS-Services in Ihrem Namen anzurufen.

Eine dienstbezogene Rolle Oracle Database@AWS erleichtert die Verwendung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Oracle Database@AWS definiert die Berechtigungen ihrer dienstbezogenen Rollen und Oracle Database@AWS kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können die Rollen nur nach dem Löschen der zugehörigen Ressourcen löschen. Dadurch werden Ihre Oracle Database@AWS Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Mit dem Dienst verknüpfte Rollenberechtigungen für Oracle Database@AWS

Oracle Database@AWS verwendet die dienstgebundene Rolle namens AWSService RoleFor ODB, um Anrufe im Namen Ihrer Ressourcen Oracle Database@AWS AWS-Services zu ermöglichen.

Die dienstgebundene AWSService RoleFor ODB-Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

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

Dieser dienstgebundenen Rolle ist eine Berechtigungsrichtlinie namens `AmazonODBServiceRolePolicy` zugeordnet, die ihr Berechtigungen für den Betrieb in Ihrem Konto erteilt. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: Amazon ODBService RolePolicy.

Note

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Wenn Sie die folgende Fehlermeldung erhalten:
Unable to create the resource. Stellen Sie sicher, dass Sie berechtigt sind, eine dienstverknüpfte Rolle zu erstellen. Andernfalls warten Sie und versuchen Sie es später noch einmal.
Stellen Sie sicher, dass Sie die folgenden Berechtigungen für Sie aktiviert sind:

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

Weitere Informationen finden Sie unter Berechtigungen für dienstverknüpfte Rollen im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Oracle Database@AWS

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine Exadata-Datenbank erstellen, Oracle Database@AWS wird die dienstbezogene Rolle für Sie erstellt.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie eine Exadata-Datenbank erstellen, Oracle Database@AWS wird die serviceverknüpfte Rolle erneut für Sie erstellt.

Bearbeitung einer serviceverknüpften Rolle für Oracle Database@AWS

Oracle Database@AWS erlaubt es Ihnen nicht, die dienstverknüpfte AWSService RoleFor ODB-Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können die Beschreibung der Rolle jedoch mithilfe von IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Oracle Database@AWS

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch alle Ihre Ressourcen löschen, bevor Sie die dienstverknüpfte Rolle löschen können.

Bereinigen einer dienstbezogenen Rolle für Oracle Database@AWS

Bevor Sie mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie sich zunächst vergewissern, dass die Rolle über keine aktiven Sitzungen verfügt, und alle Ressourcen entfernen, die von der Rolle verwendet werden.

So überprüfen Sie in der IAM-Konsole, ob die serviceverknüpfte Rolle über eine aktive Sitzung verfügt

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter. https://console.aws.amazon.com/iam/
2. Wählen Sie im Navigationsbereich der IAM Console Roles (Rollen) aus. Wählen Sie dann den Namen (nicht das Kontrollkästchen) der AWSService RoleFor ODB-Rolle aus.
3. Wählen Sie auf der Seite Summary (Zusammenfassung) für die ausgewählte Rolle die Registerkarte Access Advisor (Advisor aufrufen) aus.

4. Überprüfen Sie auf der Registerkarte Access Advisor die jüngsten Aktivitäten für die serviceverknüpfte Rolle.

> **Note**
>
> Wenn Sie sich nicht sicher sind, ob die AWSService RoleFor ODB-Rolle verwendet Oracle Database@AWS wird, können Sie versuchen, die Rolle zu löschen. Wenn der Dienst die Rolle verwendet, schlägt das Löschen fehl und Sie können sehen AWS-Regionen , wo die Rolle verwendet wird. Wenn die Rolle verwendet wird, müssen Sie warten, bis die Sitzung beendet wird, bevor Sie die Rolle löschen können. Die Sitzung für eine serviceverknüpfte Rolle können Sie nicht widerrufen.

Wenn Sie die AWSService RoleFor ODB-Rolle entfernen möchten, müssen Sie zuerst alle Ihre Oracle Database@AWS Ressourcen löschen.

Unterstützte Regionen für Oracle Database@AWS serviceverknüpfte Rollen

Oracle Database@AWS unterstützt die Verwendung von dienstbezogenen Rollen überall dort, AWS-Regionen wo der Dienst verfügbar ist. Weitere Informationen finden Sie unter AWS-Regionen und Endpunkte.

Oracle Database@AWS Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen der AWS verwalteten Richtlinien, die Oracle Database@AWS seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS-Feed auf der Seite Oracle Database@AWS Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderungen	Beschreibung	Date
Mit dem Dienst verknüpfte Rollenberechtigungen für Oracle Database@AWS	Oracle Database@AWS hat der Rolle, die mit dem `AmazonODBServiceRolePolicy` `AWSServiceRoleForODB` Dienst verknüpft	30. Juni 2025

Änderungen	Beschreibung	Date
– Aktualisierung auf eine bestehende Richtlinie	ist, neue Berechtigungen hinzugefügt. Mit diesen Berechtigungen können Oracle Database@AWS Sie Folgendes tun: • Beschreiben Sie Amazon VPC Transit Gateways-Anhänge • Beschreiben Sie EC2 Amazon-Anhänge • Aktivieren Sie eine EventBridge Amazon-Quelle Weitere Informationen finden Sie unter Mit dem Dienst verknüpfte Rollenberechtigungen für Oracle Database@AWS.	
Mit dem Dienst verknüpfte Rollenberechtigungen für Oracle Database@AWS – Aktualisierung auf eine bestehende Richtlinie	Oracle Database@AWS hat der Rolle, die mit dem `AmazonODBServiceRolePolicy` `AWSServiceRoleForODB` Service verknüpft ist, neue Berechtigungen hinzugefügt. Mit diesen Berechtigungen können Oracle Database@AWS Sie Folgendes tun: • Beschreiben Sie eine EventBridge Amazon-Quelle • Beschreiben und erstellen Sie einen Event-Bus Weitere Informationen finden Sie unter Mit dem Dienst verknüpfte Rollenberechtigungen für Oracle Database@AWS.	26. Juni 2025
AWS verwaltete Richtlinie: Amazon ODBService RolePolicy— Neue Richtlinie für dienstbezogene Rollen	Oracle Database@AWS `AmazonODBServiceRolePolicy` für die `AWSServiceRoleForODB` dienstbezogene Rolle wurde die hinzugefügt. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: Amazon ODBService RolePolicy.	2. Dezember 2024

Änderungen	Beschreibung	Date
Oracle Database@AWS hat begonnen, Änderungen zu verfolgen	Oracle Database@AWS hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	2. Dezember 2024

Überwachung der Oracle-Datenbank@AWS

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer Oracle Database@AWS anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, mit denen Sie beobachten Oracle Database@AWS, melden können, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen ergreifen können:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Sie können beispielsweise die CPU-Auslastung oder andere Kennzahlen Ihrer EC2 Amazon-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- Mit Amazon CloudWatch Logs können Sie Ihre Protokolldateien von EC2 Amazon-Instances und anderen Quellen überwachen CloudTrail, speichern und darauf zugreifen. CloudWatch Logs kann Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.
- Amazon EventBridge kann verwendet werden, um Ihre AWS Services zu automatisieren und automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu reagieren. Ereignisse aus AWS Services werden nahezu EventBridge in Echtzeit zugestellt. Sie können einfache Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen ausgeführt werden sollen, wenn ein Ereignis mit einer Regel übereinstimmt. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Überwachung Oracle Database@AWS mit Amazon CloudWatch

Sie können die Oracle Database@AWS Nutzung überwachen CloudWatch, wobei Rohdaten gesammelt und zu lesbaren Kennzahlen verarbeitet werden, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

CloudWatch Amazon-Metriken für Oracle Database@AWS

Der Oracle Database@AWS Service meldet Metriken an Amazon CloudWatch im `AWS/ODB` Namespace für VM-Cluster, Container-Datenbanken und austauschbare Datenbanken.

Themen

- Metriken für Cloud-VM-Cluster
- Metriken für Container-Datenbanken
- Metriken für austauschbare Datenbanken

Metriken für Cloud-VM-Cluster

Der Oracle Database@AWS Dienst meldet die folgenden Metriken im `AWS/ODB` Namespace für Cloud-VM-Cluster.

Metrik	Description	Einheiten
`ASMDiskgroupUtilization`	Der Prozentsatz des nutzbaren Speicherplatzes, der in einer Festplattengruppe verwendet wird. Nutzbarer Speicherplatz ist der Speicherplatz, der für Wachstum zur Verfügung steht. Die Datenträgergruppe DATA speichert unsere Oracle-Datenbankdateien.	Prozentsatz

Metrik	Description	Einheiten
	Die RECO-Festplattengruppe enthält Datenbankdateien für die Wiederherstellung wie Archive und Flashback-Logs.	
`CpuUtilization`	Die prozentuale CPU-Auslastung.	Prozentsatz
`FilesystemUtilization`	Die prozentuale Auslastung des bereitgestellten Dateisystems.	Prozentsatz
`LoadAverage`	Die durchschnittliche Systemlast beträgt mehr als 5 Minuten.	Ganzzahl
`MemoryUtilization`	Der Prozentsatz des verfügbaren Speichers für den Start neuer Anwendungen ohne Auslagerung. Der verfügbare Speicher kann mit dem folgenden Befehl abgerufen werden: `cat /proc/meminfo`	Prozentsatz
`NodeStatus`	Zeigt an, ob der Host erreichbar ist.	Ganzzahl
`OcpusAllocated`	Die Anzahl der OCPUs zugewiesenen.	Ganzzahl
`SwapUtilization`	Die prozentuale Nutzung des gesamten Swap-Speichers.	Prozentsatz

Metriken für Container-Datenbanken

Der Oracle Database@AWS Service meldet die folgenden Metriken im `AWS/ODB` Namespace für Container-Datenbanken.

Metrik	Description	Einheiten
`BlockChanges`	Die durchschnittliche Anzahl der Blöcke hat sich pro Sekunde geändert.	Änderungen pro Sekunde
`CpuUtilization`	Die als Prozentsatz ausgedrückte CPU-Auslastung, aggregiert für alle Nutzergruppen. Der Prozentsatz der Auslastung wird in Bezug auf die Anzahl der Datenbanken angegeben, CPUs die verwendet werden dürfen. Diese Zahl entspricht dem Zweifachen der Anzahl von OCPUs.	Prozentsatz
`CurrentLogons`	Die Anzahl erfolgreicher Anmeldungen während des ausgewählten Intervalls.	Anzahl
`ExecuteCount`	Die Anzahl der Benutzer- und rekursiven Aufrufe, die während des ausgewählten Intervalls SQL-Anweisungen ausgeführt haben.	Anzahl
`ParseCount`	Die Anzahl der Hard- und Soft-Parses während des ausgewählten Intervalls.	Anzahl

Metrik	Description	Einheiten
`StorageAllocated`	Gesamtmenge des Speicherplatzes, der der Datenbank zum Zeitpunkt der Erfassung zugewiesen wurde.	GB
`StorageAllocatedByTablespace`	Gesamtmenge des Speicherplatzes, der dem Tablespace zum Zeitpunkt der Erfassung zugewiesen wurde. Im Fall einer Container-Datenbank stellt diese Metrik Root-Container-Tablespaces bereit.	GB
`StorageUsed`	Gesamtmenge des Speicherplatzes, der von der Datenbank zum Zeitpunkt der Erfassung verwendet wurde.	GB
`StorageUsedByTablespace`	Gesamtmenge des Speicherplatzes, der von Tablespace zum Zeitpunkt der Erfassung genutzt wurde. Im Fall einer Container-Datenbank stellt diese Metrik Root-Container-Tablespaces bereit.	GB
`StorageUtilization`	Der Prozentsatz der bereitgestellten Speicherkapazität, der derzeit genutzt wird. Stellt den gesamten zugewiesenen Speicherplatz für alle Tablespaces dar.	Prozentsatz

Metrik	Description	Einheiten
`StorageUtilizationByTablespace`	Dies gibt den Prozentsatz des Speicherplatzes an, der vom Tablespace zum Zeitpunkt der Erfassung genutzt wurde. Im Fall einer Container-Datenbank stellt diese Metrik Root-Container-Tablespaces bereit.	Prozentsatz
`TransactionCount`	Die kombinierte Anzahl von Benutzer-Commits und Benutzer-Rollbacks während des ausgewählten Intervalls.	Anzahl
`UserCalls`	Die kombinierte Anzahl von Anmeldungen, Analysen und Ausführungsaufrufen während des ausgewählten Intervalls.	Anzahl

Metriken für austauschbare Datenbanken

Der Oracle Database@AWS Service meldet die folgenden Metriken im `AWS/ODB` Namespace für austauschbare Datenbanken.

Metrik	Description	Einheiten
`AllocatedStorageUtilizationByTablespace`	Der Prozentsatz des vom Tablespace belegten Speicherplatzes im Verhältnis zum gesamten zugewiesenen Speicherplatz. Für Container-Datenbanken stellt diese Metrik Daten für Root-Container-Tablespaces bereit.	Prozent

Metrik	Description	Einheiten
	(Statistik: Mittelwert, Intervall: 30 Minuten)	
`AvgGCCRBlockReceiveTime`	Die durchschnittliche Empfangszeit für CR-Blocks (Consistent-Read) im globalen Cache. Nur für RAC/Cluster-Datenbanken. (Statistik: Mittelwert, Intervall: 5 Minuten)	Millisekunden
`AvgGCCurrentBlockReceiveTime`	Die durchschnittliche Empfangszeit aktueller Blöcke im globalen Cache. In der Statistik wird der Mittelwert angegeben. Nur für Real Application Cluster (RAC)-Datenbanken. (Statistik: Mittelwert, Intervall: 5 Minuten)	Millisekunden
`BlockChanges`	Die durchschnittliche Anzahl von Blöcken, die sich pro Sekunde geändert haben. (Statistik: Mittelwert, Intervall: 1 Minute)	Änderungen pro Sekunde
`BlockingSessions`	Aktuelle blockierende Sitzungen. Gilt nicht für Container-Datenbanken. (Statistik: Max., Intervall: 15 Minuten)	Anzahl

Metrik	Description	Einheiten
`CPUTimeSeconds`	Die durchschnittliche Akkumulationsrate von CPU-Zeit durch Vordergrundsitzungen in der Datenbankinstanz über das Zeitintervall. Die CPU-Zeitkomponente von Average Active Sessions. (Statistik: Mittelwert, Intervall: 1 Minute)	Sekunden pro Sekunde
`CpuCount`	Die Anzahl der CPUs während des ausgewählten Intervalls.	Anzahl
`CpuUtilization`	Die CPU-Auslastung, ausgedrückt als Prozentsatz, aggregiert für alle Nutzergruppen. Der Prozentsatz der Auslastung wird in Bezug auf die Anzahl der Datenbanken angegeben, CPUs die verwendet werden dürfen. Diese Zahl entspricht dem Zweifachen der Anzahl von OCPUs. (Statistik: Mittelwert, Intervall: 1 Minute)	Prozent
`CurrentLogons`	Die Anzahl erfolgreicher Anmeldungen während des ausgewählten Intervalls. (Statistik: Summe, Intervall: 1 Minute)	Anzahl

Metrik	Description	Einheiten
DBTimeSeconds	Die durchschnittliche Akkumulationsrate von Datenbankzeit (CPU + Wait) durch Vordergrundsitzungen in der Datenbankinstanz über das Zeitintervall. Wird auch als durchschnittliche Anzahl aktiver Sitzungen bezeichnet. (Statistik: Mittelwert, Intervall: 1 Minute)	Sekunden pro Sekunde
DbmgmtJobExecutionsCount	Die Anzahl der SQL-Auftragsausführungen in einer einzelnen verwalteten Datenbank oder einer Datenbankgruppe sowie deren Status. Statusdimensionen können die folgenden Werte sein: „Erfolgreich“, „Fehlgeschlagen“, ""“InProgress. (Statistik: Summe, Intervall: 1 Minute)	Anzahl
ExecuteCount	Die Anzahl der Benutzer- und rekursiven Aufrufe, die während des ausgewählten Intervalls SQL-Anweisungen ausgeführt haben. (Statistik: Summe, Intervall: 1 Minute)	Anzahl
FRASpaceLimit	Die Speicherplatzbeschränkung für den Flash Recovery-Bereich. Gilt nicht für austauschbare Datenbanken. (Statistik: Max., Intervall: 15 Minuten)	GB

Metrik	Description	Einheiten
FRAUtilization	Die Nutzung des Flash Recovery-Bereichs. Gilt nicht für austauschbare Datenbanken. (Statistik: Mittelwert, Intervall: 15 Minuten)	Prozent
GCCRBlocksReceived	Die pro Sekunde empfangenen CR-Blöcke (Consistent-Read) im globalen Cache. Nur für RAC/Cluster-Datenbanken. (Statistik: Mittelwert, Intervall: 5 Minuten)	Blöcke pro Sekunde
GCCurrentBlocksReceived	Stellt die aktuell pro Sekunde empfangenen Blöcke im globalen Cache dar. Die Statistik gibt den Mittelwert an. Nur für Real Application Cluster (RAC) -Datenbanken. (Statistik: Mittelwert, Intervall: 5 Minuten)	Blöcke pro Sekunde
IOPS	Die durchschnittliche Anzahl von Eingabe-Ausgabe-Vorgängen pro Sekunde. (Statistik: Mittelwert, Intervall: 1 Minute)	Operationen pro Sekunde
IOThroughputMB	Der durchschnittliche Durchsatz in MB pro Sekunde. (Statistik: Mittelwert, Intervall: 1 Minute)	MB pro Sekunde

Metrik	Description	Einheiten
`InterconnectTraffic MB`	Die durchschnittliche Datenübertragungsrate zwischen den Knoten. Nur für RAC/Cluster-Datenbanken. (Statistik: Mittelwert, Intervall: 5 Minuten)	MB pro Sekunde
`InvalidObjects`	Ungültige Anzahl von Datenbankobjekten. Gilt nicht für Container-Datenbanken. (Statistik: Max., Intervall: 24 Stunden)	Anzahl
`LogicalBlocksRead`	Die durchschnittliche Anzahl von Blöcken, aus denen pro Sekunde gelesen wird SGA/ Memory (Puffer-Cache). (Statistik: Mittelwert, Intervall: 1 Minute)	Lesevorgänge pro Sekunde
`MaxTablespaceSize`	Die maximal mögliche Tablespace-Größe. Für Container-Datenbanken stellt diese Metrik Daten für Root-Container-Tablespaces bereit. (Statistik: Max., Intervall: 30 Minuten)	GB
`MemoryUsage`	Gesamtgröße des Speicherp ools in MB. (Statistik: Mittelwer t, Intervall: 15 Minuten)	MB

Metrik	Description	Einheiten
`MonitoringStatus`	Der Überwachungsstatus der Ressource. Wenn eine Metrikerfassung fehlschlägt, werden Fehlerinformationen in dieser Metrik erfasst. (Statistik: Mittelwert, Intervall: 5 Minuten)	Nicht zutreffend
`NonReclaimableFRA`	Der Bereich für schnelle Wiederherstellung, der nicht zurückgewonnen werden kann. Gilt nicht für austausch bare Datenbanken. (Statisti k: Mittelwert, Intervall: 15 Minuten)	Prozent
`OcpusAllocated`	Die tatsächliche Anzahl der vom Dienst während des ausgewählten Zeitintervalls OCPUs zugewiesenen. (Statistik: Anzahl, Intervall: 1 Minute)	Ganzzahl
`ParseCount`	Die Anzahl der harten und weichen Analysen während des ausgewählten Intervalls. (Statistik: Summe, Intervall: 1 Minute)	Anzahl
`ParsesByType`	Die Anzahl der harten oder weichen Analysen pro Sekunde. (Statistik: Mittelwert, Intervall: 1 Minute)	Parse-Vorgänge pro Sekunde

Metrik	Description	Einheiten
`ProblematicScheduledDBMSJobs`	Die problematischen geplanten Datenbankjobs werden gezählt. Gilt nicht für Container-Datenbanken. (Statistik: Max., Intervall: 15 Minuten)	Anzahl
`ProcessLimitUtilization`	Der Prozess begrenzt die Auslastung. Gilt nicht für austauschbare Datenbanken. (Statistik: Mittelwert, Intervall: 1 Minute)	Prozent
`Processes`	Die Datenbankprozesse zählen. Gilt nicht für austauschbare Datenbanken. (Statistik: Max., Intervall: 1 Minute)	Anzahl
`ReclaimableFRA`	Der Bereich für schnelle Wiederherstellung, der zurückgewonnen werden kann. Gilt nicht für austauschbare Datenbanken. (Statistik: Mittelwert, Intervall: 15 Minuten)	Prozent
`ReclaimableFRASpace`	Der zurückgewinnbare Speicherplatz im Flash Recovery-Bereich. Gilt nicht für austauschbare Datenbanken. (Statistik: Mittelwert, Intervall: 15 Minuten)	GB

Metrik	Description	Einheiten
RedoSizeMB	Die durchschnittliche Menge an generierten Wiederholungen in MB pro Sekunde. (Statistik: Mittelwert, Intervall: 1 Minute)	MB pro Sekunde
SessionLimitUtilization	Das Sitzungslimit für die Nutzung. Gilt nicht für austauschbare Datenbanken. (Statistik: Mittelwert, Intervall: 1 Minute)	Prozent
Sessions	Die Anzahl der Sitzungen in der Datenbank. (Statistik: Mittelwert, Intervall: 1 Minute)	Anzahl
StorageAllocated	Der maximale Speicherplatz, der dem Tablespace während des Intervalls zugewiesen wurde. Für Container-Datenbanken stellt diese Metrik Daten für Root-Container-Tablespaces bereit. (Statistik: Max., Intervall: 30 Minuten)	GB
StorageAllocatedByTablespace	Die maximale Menge an Speicherplatz, die dem Tablespace während des Intervalls zugewiesen wurde. Für Container-Datenbanken stellt diese Metrik Daten für Root-Container-Tablespaces bereit. (Statistik: Max., Intervall: 30 Minuten)	GB

Metrik	Description	Einheiten
`StorageUsed`	Die maximale Menge an Speicherplatz, die während des Intervalls genutzt wurde. (Statistik: Max., Intervall: 30 Minuten)	GB
`StorageUsedByTablespace`	Die maximale Menge an Speicherplatz, die Tablespace während des Intervalls belegt hat. Für Container-Datenbanken stellt diese Metrik Daten für Root-Container-Tablespaces bereit. (Statistik: Max., Intervall: 30 Minuten)	GB
`StorageUtilization`	Der Prozentsatz der bereitgestellten Speicherkapazität, der derzeit genutzt wird. Stellt den gesamten zugewiesenen Speicherplatz für alle Tablespaces dar. (Statistik: Mittelwert, Intervall: 30 Minuten)	Prozent
`StorageUtilizationByTablespace`	Der Prozentsatz des belegten Speicherplatzes, aufgeschlüsselt nach Tablespace. Für Container-Datenbanken stellt diese Metrik Daten für Root-Container-Tablespaces bereit. (Statistik: Mittelwert, Intervall: 30 Minuten)	Prozent

Metrik	Description	Einheiten
`TransactionCount`	Die kombinierte Anzahl von Benutzer-Commits und Benutzer-Rollbacks während des ausgewählten Intervalls. (Statistik: Summe, Intervall: 1 Minute)	Anzahl
`TransactionsByStatus`	Die Anzahl der festgesch riebenen oder zurückgerollten Transaktionen pro Sekunde. (Statistik: Mittelwert, Intervall: 1 Minute)	Transaktionen pro Sekunde
`UnusableIndexes`	Im Datenbankschema werden unbrauchbare Indizes gezählt. Gilt nicht für Container-Datenbanken. (Statistik: Max., Intervall: 24 Stunden)	Anzahl
`UsableFRA`	Der nutzbare Bereich für schnelle Wiederherstellung. Gilt nicht für austausch bare Datenbanken. (Statisti k: Mittelwert, Intervall: 15 Minuten)	Prozent
`UsedFRASpace`	Der Speicherverbrauch im Flash Recovery-Bereich. Gilt nicht für austauschbare Datenbanken. (Statistik: Max., Intervall: 15 Minuten)	GB

Metrik	Description	Einheiten
`UserCalls`	Die kombinierte Anzahl von Anmeldungen, Analysen und Ausführungsaufrufen während des ausgewählten Intervalls. (Statistik: Summe, Intervall: 1 Minute)	Anzahl
`WaitTimeSeconds`	Die durchschnittliche Akkumulationsrate von Wartezeiten ohne Leerlauf durch Vordergrundsitzungen in der Datenbankinstanz über das Zeitintervall. Die Wartezeit komponente von Average Active Sessions. (Statistik: Mittelwert, Intervall: 5 Minuten)	Sekunden pro Sekunde

CloudWatch Amazon-Abmessungen für Oracle Database@AWS

Sie können Oracle Database@AWS Metrikdaten filtern, indem Sie eine beliebige Dimension in der folgenden Tabelle verwenden.

Dimension	Filtert die angeforderten Daten für . . .
`cloudVmClusterId`	Der Bezeichner eines VM-Clusters.
`cloudExadataInfrastructureId`	Die Kennung der Exadata-Infrastruktur.
`collectionName`	Ein Name einer Sammlung.
`deploymentType`	Die Art der Infrastruktur.
`diskgroupName`	Ein Name einer Festplattengruppe

Dimension	Filtert die angeforderten Daten für . . .
errorCode	Ein Fehlercode.
errorSeverity	Der Schweregrad eines Fehlers.
filesystemName	Der Name eines Dateisystems.
hostName	Der Name des Host-Computers.
instanceName	Der Name einer Datenbankinstanz.
instanceNumber	Die Instanznummer einer Datenbankinstanz.
ioType	Eine Art von I/O Operation.
jobId	Eine eindeutige Kennung für einen Job.
managedDatabaseGroupId	Der Bezeichner einesManaged Database Group.
managedDatabaseId	Der Bezeichner von Managed Database a.
memoryPool	Eine Art von Speicherpool.
memoryType	Eine Art von Speicher.
ociCloudVmClusterId	Die OCI-ID eines VM-Clusters.
ociCloudExadataInfrastructureId	Die OCI-Kennung der Exadata-Infrastruktur.
parseType	Eine Art von Parse.
resourceId	Der Bezeichner einer Ressource.
resourceId_Database	Der Bezeichner einer Datenbank.
resourceId_DbNode	Der Bezeichner eines Datenbankknotens.
resourceName	Der Name einer -Ressource.

Dimension	Filtert die angeforderten Daten für . . .
`resourceName_Database`	Der Name einer Datenbank.
`resourceName_DbNode`	Der Name eines Datenbankknotens.
`resourceType`	Ein Datenbanktyp.
`schemaName`	Der Name eines Schemas.
`status`	Der Status einer Datenbank.
`tablespaceContents`	Der Inhalt eines Tablespaces.
`tablespaceName`	Der Name eines Tablespaces.
`tablespaceType`	Eine Art von Tablespace.
`transactionStatus`	Der Status einer Transaktion.
`waitClass`	Ein Ereignis der Klasse Wait.

Oracle Database@AWS Ereignisse in Amazon überwachen EventBridge

Sie können Oracle Database@AWS Ereignisse überwachen EventBridge, wodurch ein Stream von Echtzeitdaten aus Anwendungen und AWS Diensten bereitgestellt wird. EventBridge leitet diese Daten an Ziele wie AWS Lambda Amazon Simple Notification Service weiter.

> **Note**
>
> EventBridge hieß früher Amazon CloudWatch Events. Weitere Informationen finden Sie unter EventBridge Die Entwicklung von Amazon CloudWatch Events im EventBridge Amazon-Benutzerhandbuch.

Überblick über Oracle Database@AWS Ereignisse

Oracle Database@AWS Ereignisse sind strukturierte Meldungen, die auf Änderungen in den Lebenszyklen von Ressourcen hinweisen. Ein Event-Bus ist ein Router, der Ereignisse empfängt und sie an null oder mehr Ziele oder Ziele weiterleitet. Oracle Database@AWS Ereignisse können aus den folgenden Quellen generiert werden:

Ereignisse von AWS

Diese Ereignisse werden von Oracle Database@AWS APIs der AWS Seite generiert und an den Standard-Event-Bus in Ihrem übertragen AWS-Konto.

Ereignisse von OCI

Diese Ereignisse werden direkt aus OCI generiert, z. B. Ereignisse im Zusammenhang mit der Oracle Exadata-Infrastruktur oder VM-Clustern. Wenn Sie sich anmelden Oracle Database@AWS, `aws.partner/odb/` wird in Ihrem System ein Event-Bus mit Präfix erstellt, um Ereignisse von AWS-Konto OCI zu empfangen.

Oracle Database@AWS Ereignisse von AWS

Oracle Database@AWS Zu den Ereignissen von AWS gehören Lebenszyklusänderungen im Zusammenhang mit dem ODB-Netzwerk während der Erstellung und Löschung. Diese Ereignisse werden an den Standardereignisbus in Ihrem AWS-Kontoübertragen. Die Versandart ist „Best Effort“.

ODB-Netzwerkereignisse

Veranstaltung	Ereignis-ID	Fehlermeldung
Erstellung	ODB-EVENT-0001	Das ODB-Netzwerk ODBNet_ID wurde erfolgrei ch erstellt
Fehler beim Erstellen	ODB-EVENT-0011	ODB-Netzwerk ODBNet_ID konnte nicht erstellt werden
Löschung	ODB-EVENT-0002	Das ODB-Netzwerk ODBNet_ID wurde erfolgrei ch gelöscht
Fehler beim Löschen	ODB-EVENT-0012	ODB-Netzwerk ODBNet_ID konnte nicht gelöscht werden

Beispiel: Ereignis zur Erstellung eines ODB-Netzwerks

Das folgende Beispiel zeigt ein Ereignis für eine erfolgreiche ODB-Netzwerkerstellung.

```
{
  "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"
  }
}
```

Oracle Database@AWS Ereignisse von OCI

Die meisten Ereignisse werden direkt aus OCI generiert. Oracle Database@AWS erstellt einen Event-Bus mit Präfix `aws.partner/odb/` in Ihrem AWS-Konto , um Ereignisse von OCI zu empfangen. Wir empfehlen, diesen Event-Bus nicht zu löschen.

OCI bietet umfassende Ereignistypen, darunter die folgenden:

- Oracle Exadata-Infrastruktur
- VM-Cluster-Ereignisse
- CDB-Ereignisse
- PDB-Ereignisse

Weitere Informationen zu den spezifischen Ereignistypen und Einzelheiten, die OCI unterstützt, finden Sie unter Oracle Exadata Database Service on Dedicated Infrastructure Events und Events for Autonomous Database on Dedicated Exadata Infrastructure.

Ereignisse filtern Oracle Database@AWS

Die EventBridge empfohlenen Best Practices zur Einrichtung von Eventbussen finden Sie unter Event Buses in Amazon EventBridge. Je nach Ihren Anwendungsfällen können Sie EventBridge Regeln einrichten, um Ereignisse und Ziele so zu filtern, dass sie Ereignisse empfangen und verwenden.

Filtern von ODB-Netzwerkereignissen aus AWS

Nach ODB-Netzwerkereignissen von AWS können Sie nach dem folgenden Ereignismuster filtern:

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

Sie können dieses Muster mithilfe der EventBridge `put-rule` API mit dem Standardereignisbus anwenden. Weitere Informationen finden Sie PutRulein der Amazon EventBridge API-Referenz.

Oracle Database@AWS Ereignisse aus OCI filtern

Für Oracle Database@AWS Ereignisse von OCI können Sie eine Regel mit einem Befehl einrichten, der dem Beispiel PutRulein der Amazon EventBridge API-Referenz ähnelt. Beachten Sie die folgenden Richtlinien:

- Verwenden Sie je nach den Ereignistypen, die Sie filtern möchten, ein benutzerdefiniertes Ereignismuster.
- Geben Sie EventBusNameden Namen des Buses ein, der Oracle Database@AWS erstellt wurde.

Weitere Informationen zum Filtern von Ereignissen und zum Einrichten von EventBridge Zielen für mehrere Konten finden Sie unter Senden und Empfangen von Ereignissen zwischen AWS-Konten in Amazon EventBridge.

Fehlerbehebung bei Oracle Database@AWS Ereignissen

Gehen Sie wie folgt vor, wenn Sie ein Problem mit der Veranstaltungszustellung oder dem Veranstaltungsinhalt haben:

- Für ODB-Netzwerkereignisse wenden Sie sich an AWS Support.

- Für andere Oracle Database@AWS Ereignisse als ODB-Netzwerkereignisse wenden Sie sich an den Oracle Cloud Support.

Weitere Informationen finden Sie unter Unterstützung für Oracle Database@ erhalten AWS.

Oracle Database@AWS API-Aufrufe protokollieren mit AWS CloudTrail

Oracle Database@AWS ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem ausgeführten Aktionen bereitstellt AWS-Service. CloudTrail erfasst alle API-Aufrufe Oracle Database@AWS als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Oracle Database@AWS Konsole und Codeaufrufen für die Oracle Database@AWS API-Operationen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, an die die Anfrage gestellt wurde Oracle Database@AWS, die IP-Adresse, von der aus die Anfrage gestellt wurde, den Zeitpunkt der Anfrage und weitere Details ermitteln.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anforderung mit Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.
- Die Anforderung wurde im Namen eines IAM-Identity-Center-Benutzers erstellt.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

> **Note**
>
> Oracle Database@AWS zeichnet `GetCallerIdentity` API-Aufrufe von AWS Security Token Service (STS) in Ihren CloudTrail Protokollen auf. Diese STS-API-Aufrufe verifizieren die Identität von Personen Oracle Database@AWS , die in Ihrem Namen mit OCI interagieren. Sie sind ein normaler und sicherer Teil des AWS Betriebs und geben keine vertraulichen Informationen preis.

CloudTrail ist in Ihrem aktiv AWS-Konto , wenn Sie das Konto erstellen, und Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf. Der CloudTrail Ereignisverlauf bietet eine einsehbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der aufgezeichneten Verwaltungsereignisse der letzten 90 Tage in einem. AWS-Region Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf. Für die Anzeige des Eventverlaufs CloudTrail fallen keine Gebühren an.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrailLake-Event-Datenspeicher.

CloudTrail Pfade

Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Alle mit dem erstellten Pfade AWS-Managementkonsole sind regionsübergreifend. Sie können mithilfe von AWS CLI einen Einzel-Region- oder einen Multi-Region-Trail erstellen. Es wird empfohlen, einen Trail mit mehreren Regionen zu erstellen, da Sie alle Aktivitäten AWS-Regionen in Ihrem Konto erfassen. Wenn Sie einen Einzel-Region-Trail erstellen, können Sie nur die Ereignisse anzeigen, die im AWS-Region des Trails protokolliert wurden. Weitere Informationen zu Trails finden Sie unter Erstellen eines Trails für Ihr AWS-Konto und Erstellen eines Trails für eine Organisation im AWS CloudTrail -Benutzerhandbuch.

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren Amazon S3 S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3 – Preise.

CloudTrail Datenspeicher für Ereignisse in Lake

CloudTrail Mit Lake können Sie SQL-basierte Abfragen für Ihre Ereignisse ausführen. CloudTrail Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON-Format in das Apache ORC-Format. ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen. Die Selektoren, die Sie auf einen Ereignisdatenspeicher anwenden, steuern, welche Ereignisse bestehen bleiben und für Sie zur Abfrage verfügbar sind. Weitere Informationen zu CloudTrail Lake finden Sie unter Arbeiten mit AWS CloudTrail Lake im AWS CloudTrail Benutzerhandbuch.

CloudTrail Für das Speichern und Abfragen von Ereignisdaten in Lake fallen Kosten an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den

Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise.

Oracle Database@AWS Management-Ereignisse in CloudTrail

Verwaltungsereignisse bieten Informationen über Verwaltungsvorgänge, die an Ressourcen in Ihrem ausgeführt werden AWS-Konto. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. CloudTrail Protokolliert standardmäßig Verwaltungsereignisse.

Oracle Database@AWS protokolliert alle Operationen auf der Oracle Database@AWS Steuerungsebene als Verwaltungsereignisse.

Oracle Database@AWS Beispiele für Ereignisse

Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über den angeforderten API-Vorgang, Datum und Uhrzeit des Vorgangs, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass Ereignisse nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt ein CloudTrail Ereignis, das den `CreateOdbNetwork` Vorgang demonstriert.


```
{
    "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"
    }
}
```


Informationen zu CloudTrail Datensatzinhalten finden Sie im AWS CloudTrail Benutzerhandbuch unter CloudTrailDatensatzinhalt.

Problembehandlung bei Oracle Database@AWS

Verwenden Sie die folgenden Abschnitte, um Netzwerkprobleme zu beheben, auf die Sie möglicherweise stoßen. Oracle Database@AWS

Themen

- Die Erstellung des ODB-Netzwerks schlägt fehl
- Verbindungsprobleme zwischen Ihrem VPC- und ODB-Netzwerk oder VM-Clustern
- Unauflösbare Hostnamen oder Scannamen von VM-Clustern aus VPC
- Unterstützung für Oracle Database@ erhalten AWS

Die Erstellung des ODB-Netzwerks schlägt fehl

Wenn Sie kein ODB-Netzwerk erstellen können, gibt es die folgenden häufigen Ursachen:

Eingeschränkte CIDR-Bereiche

Das ODB-Netzwerk verwendet spezifische CIDR-Bereiche für die Client- und Backup-Subnetze. Stellen Sie sicher, dass sich die CIDR-Bereiche, die Sie für diese Subnetze ausgewählt haben, nicht mit eingeschränkten oder reservierten IP-Adressbereichen überschneiden.

Die folgenden CIDR-Bereiche sind reserviert und können nicht für das ODB-Netzwerk verwendet werden:

- Reservierter Bereich für Oracle Cloud: 169.254.0.0/16
- Reservierte Klasse D: 224.0.0.0 — 239.255.255.255
- Reservierte Klasse E: 240.0.0.0 — 255.255.255.255
- Künftige Verwendung von OCI: 100.105.0.0/16

Folgen Sie den EC2 Regeln für CIDR-Bereiche, wie sie in der VPC-Dokumentation beschrieben sind. Weitere Informationen finden Sie unter Einschränkungen der CIDR-Blockzuweisung.

Vermeiden Sie außerdem Überschneidungen zwischen den angegebenen CIDR-Bereichen und denen, die für die VPC-Konnektivität zum ODB-Netzwerk verwendet werden.

Überlappende VPC CIDR

Der CIDR-Bereich, den Sie für das ODB-Netzwerk angegeben haben, sollte sich nicht mit den CIDR-Bereichen überschneiden, die von Ihren vorhandenen verwendet werden. VPCs

Überlappende CIDR-Bereiche können zu Routingkonflikten führen und die erfolgreiche Erstellung des ODB-Netzwerks verhindern. Überprüfen Sie die CIDR-Bereiche des ODB-Peerings VPCs und stellen Sie sicher, dass das CIDR des ODB-Netzwerks eindeutig ist und sich nicht überschneidet.

Eigentum von VPCs

Das ODB-Netzwerk und die VPC, mit der Sie eine Verbindung herstellen, müssen demselben AWS Konto gehören. Wenn Sie versuchen, das ODB-Netzwerk mit einer VPC zu verbinden, die einem anderen Konto gehört, schlägt die Erstellung fehl. Stellen Sie sicher, dass das ODB-Netzwerk und die VPC beide demselben AWS Konto gehören.

Fehlen eines Transit-Gateways

Wenn Sie der CIDR-Liste über ODB-Netzwerk-Peering einen CIDR-Bereich hinzufügen, ohne der VPC ein Transit-Gateway zuzuweisen, schlägt der Erstellungs- oder Aktualisierungsvorgang fehl. Es gibt keine Anforderung bezüglich der CIDR-Bereiche, für die der Anhang verwendet wird.

Verbindungsprobleme zwischen Ihrem VPC- und ODB-Netzwerk oder VM-Clustern

Wenn Sie von Ihrer VPC aus keine Verbindung zum ODB-Netzwerk oder den darin enthaltenen VM-Clustern herstellen können, gibt es die folgenden häufigen Ursachen:

- VPC-Konfiguration überprüfen — Suchen Sie in der Oracle Database@AWS Konsole die VPC, die mit dem ODB-Netzwerk über Peering verbunden ist. Stellen Sie sicher, dass die VPC-ID mit der in den ODB-Netzwerkdetails angezeigten übereinstimmt.
- Routentabellen überprüfen — Suchen Sie in der Amazon VPC-Konsole nach der Routing-Tabelle, die an das Subnetz angehängt ist, in dem Ihre Anwendung ausgeführt wird. Suchen Sie nach einer Route mit einer Ziel-CIDR, die mit der Client-Subnetz-CIDR des ODB-Netzwerks übereinstimmt. Vergewissern Sie sich, dass diese Route auf den richtigen ODB-Netzwerk-ARN verweist. Wenn die Route fehlt, fügen Sie dem Client-Subnetz CIDR des ODB-Netzwerks eine neue hinzu.
- Peered validieren CIDRs — Lesen Sie den `Peered CIDRs` Abschnitt in den ODB-Netzwerkdetails. Vergewissern Sie sich, dass alle relevanten CIDR-Blöcke aus Ihrer VPC aufgelistet sind. Wenn ein erforderlicher CIDR fehlt, aktualisieren Sie den Peered-Computer. CIDRs
- Sicherheitsgruppenregeln überprüfen — Suchen Sie in der EC2 Amazon-Konsole nach den Sicherheitsgruppen für Ressourcen in Ihrer VPC. Überprüfen Sie die Regeln für eingehenden und ausgehenden Datenverkehr und aktualisieren Sie sie nach Bedarf, um den erforderlichen Datenverkehr zuzulassen.

- Availability Zones bestätigen — Identifizieren Sie in der Amazon VPC-Konsole die Availability Zone (AZ) Ihres Subnetzes. Stellen Sie sicher, dass das ODB-Netzwerk auch in derselben AZ wie Ihr Subnetz bereitgestellt wird.
- Vermeidung mehrerer ODB-Netzwerk-Peering-Verbindungen — Überprüfen Sie Ihre VPC-Peering-Verbindungen in der Konsole. Oracle Database@AWS Stellen Sie sicher, dass Sie nur eine aktive Verbindung zu einem ODB-Netzwerk haben. Wenn Sie mehr als ein ODB-Netzwerk-Peering sehen, entfernen Sie die zusätzlichen.

Unauflösbare Hostnamen oder Scannamen von VM-Clustern aus VPC

Wenn die Hostnamen oder Scannamen der VM-Cluster nicht von Ihrer VPC aus aufgelöst werden können, konfigurieren Sie die DNS-Weiterleitung auf der VPC und die folgenden Ressourcen, um DNS-Einträge aufzulösen, die im ODB-Netzwerk gehostet werden:

- Ein ausgehender Endpunkt zum Senden von DNS-Abfragen an das ODB-Netzwerk. Weitere Informationen finden Sie unter Konfiguration eines ausgehenden Endpunkts in einem ODB-Netzwerk in Oracle Database@AWS.
- Eine Resolver-Regel zur Angabe des Domainnamens der DNS-Abfragen, die der Resolver an das DNS for ODB-Netzwerk weiterleitet. Weitere Informationen finden Sie unter Konfiguration einer Resolver-Regel in Oracle Database@AWS.

Unterstützung für Oracle Database@ erhalten AWS

Erfahren Sie, wie Sie Informationen und Support für Oracle Database@AWS erhalten.

Umfang und Kontaktinformationen des Oracle-Supports

Oracle Cloud Support ist die erste Anlaufstelle für alle Fragen zu Oracle Database@AWS . Um den Support zu kontaktieren, melden Sie sich bei der Oracle Cloud Infrastructure (OCI) Console an und wählen Sie dann das Rettungsfloßsymbol aus. Wenn Sie kein My Oracle Cloud Support-Konto haben, finden Sie weitere Informationen unterMeine Oracle Cloud Support-Konten und mein Zugriff.

Zu den Problemen, bei denen Ihnen der Oracle Support weiterhelfen kann, gehören beispielsweise die folgenden:

- Probleme mit der Datenbankverbindung (Oracle TNS)

- Leistungsprobleme mit der Oracle-Datenbank
- Behebung von Oracle-Datenbankfehlern
- Netzwerkprobleme im Zusammenhang mit der Kommunikation mit dem OCI-Tenancy, der dem Service zugeordnet ist
- Das Kontingent (die Grenzwerte) wird erhöht, um mehr Kapazität zu erhalten (weitere Informationen finden Sie unter Eine Erhöhung des Limits für Datenbankressourcen beantragen)
- Skalierung, um Ihrer Oracle-Datenbankinfrastruktur mehr Rechen- und Speicherkapazität hinzuzufügen
- Hardware-Upgrades der neuen Generation
- Probleme mit der Abrechnung im Zusammenhang mit Ihren AWS Marketplace Gebühren

Wenn Sie den Oracle Support außerhalb der OCI Console kontaktieren müssen, teilen Sie Ihrem Oracle Support-Mitarbeiter mit, dass Ihr Problem mit Oracle AWS Database@ zusammenhängt. Dies liegt daran, dass Anfragen für diesen Service von einem OCI-Supportteam bearbeitet werden, das auf diese Bereitstellungen spezialisiert ist.

Telefonische Kontaktaufnahme mit dem Oracle-Support

1. Rufen Sie 1-800-223-1711 an. Wenn Sie sich außerhalb der Vereinigte Staaten befinden, besuchen Sie das Oracle Support Contacts Global Directory, um Kontaktinformationen für Ihr Land oder Ihre Region zu finden.
2. Wählen Sie Option „2", um eine neue Serviceanfrage (SR) zu öffnen.
3. Wählen Sie Option „4" für „unsicher“.
4. Teilen Sie dem Kundendienstmitarbeiter mit, dass Sie ein Problem mit Ihrem Multicloud-System haben, und teilen Sie ihm den Namen des Produkts mit. In Ihrem Namen wird eine interne Serviceanfrage gestellt und ein OCI-Supporttechniker wird sich direkt mit Ihnen in Verbindung setzen.

Sie können auch eine Frage an das Multicloud-Forum in der Cloud Customer Connect-Community von Oracle stellen. Diese Option ist für alle Kunden verfügbar.

Meine Oracle Cloud Support-Konten und mein Zugriff

Um My Oracle Cloud Support-Serviceanforderungstickets zu erstellen, muss der Administrator des Oracle AWS Database@-Dienstes Ihrer Organisation Ihre Anfrage genehmigen. Wenn Sie der Oracle

AWS Database@-Administrator sind, folgen Sie den Onboarding-Anweisungen für My Oracle Cloud Support, die in der E-Mail zur Aktivierung des Oracle AWS Database@-Dienstes enthalten sind.

Anweisungen für das Onboarding mit My Oracle Cloud Support finden Sie in den folgenden Themen:

- Konfiguration Ihres Oracle Support-Kontos
- Eine Support-Anfrage erstellen

Anweisungen zur Genehmigung von Benutzern zum Öffnen von My Oracle Cloud Support-Supportanfragen finden Sie unter Administratoraufgaben für Support.

AWS Support Umfang und Kontaktinformationen

AWS Support ist Ihre erste Anlaufstelle für alle damit AWS verbundenen Probleme und Fragen. Erstellen Sie einen AWS Support Fall für Ihr Problem, wie Sie es bei anderen AWS Diensten tun. Das AWS Support Team arbeitet bei Bedarf mit dem OCI-Support zusammen.

Beispiele für AWS Probleme mit Oracle Database@, die Ihnen helfen AWS Support können, sind unter anderem die folgenden:

- Probleme mit virtuellen Netzwerken, einschließlich Problemen mit Network Address Translation (NAT), Firewalls, DNS und Verkehrsmanagement sowie Subnetzen AWS
- Probleme mit Bastion und virtuellen Maschinen (VM), einschließlich Datenbank-Host-Verbindung, Softwareinstallation, Latenz und Host-Leistung
- Berichterstattung über Exadata-VM-Cluster-Metriken innerhalb von Amazon CloudWatch
- Probleme mit der Abrechnung im Zusammenhang mit Dienstleistungen AWS

Informationen zu AWS Support finden Sie unter Erste Schritte mit AWS Support.

Service Level Agreements von Oracle

Wenn Sie Fragen zu Oracle Database@AWS Service Level Agreements (SLAs) haben oder Servicegutschriften für SLA-Verstöße beantragen möchten, wenden Sie sich an Ihren Oracle Account Manager. Weitere Informationen finden Sie unter Service Level Agreements.

Kontingente für Oracle-Datenbank@AWS

Oracle Database@AWS ist ein Multicloud-Angebot. AWS legt keine Kontingente für Oracle Database@AWS Ressourcen fest oder erzwingt sie auch nicht. Kontingente werden von Oracle Cloud Infrastructure (OCI) durchgesetzt. Weitere Informationen zu OCI-Kontingenten finden Sie unter Kontingente und Service Limits in der Oracle Cloud Infrastructure-Dokumentation.

Dokumentenverlauf für das Oracle Database@AWS Benutzerhandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für beschrieben Oracle Database@AWS.

Änderung	Beschreibung	Datum
Oracle Database@AWS unterstützt die Regionen Asien-Pazifik (Sydney) und Kanada (Zentral)	Sie können Ihre Oracle Database@AWS Ressourcen in diesen Regionen erstellen. Weitere Informationen finden Sie unter Unterstützte Regionen für Oracle Database@AWS.	2. Februar 2026
Oracle Database@AWS unterstützt die Regionen Asien-Pazifik (Tokio), USA Ost (Ohio) und Europa (Frankfurt)	In diesen Regionen können Sie Ihre Oracle Database@AWS Ressourcen erstellen. Weitere Informationen finden Sie unter Unterstützte Regionen für Oracle Database@AWS.	22. Dezember 2025
Oracle Database@AWS unterstützt die gemeinsame Nutzung von Ansprüchen auf AWS-Konten	Mit License Manager können Sie jetzt AWS Marketplace-Berechtigungen für Oracle AWS Database@ innerhalb AWS-Konten derselben AWS Organisation gemeinsam nutzen AWS . Weitere Informationen finden Sie unter Entitlement Sharing in Oracle Database@.AWS	19. Dezember 2025

Oracle Database@AWS unterstützt die Änderung von Datenfiltern für die Zero-ETL-Integration	Oracle Database@AWS unterstützt das Ändern von Datenfiltern für bestehende Zero-ETL-Integrationen mit Amazon Redshift. Sie können Datenfiltermuster aktualisieren, um bestimmte Schemas und Tabellen von der Datenreplikation ein- oder auszuschließen. Weitere Informationen finden Sie unter Verwaltung von Zero-ETL-Integrationen.	15. Oktober 2025
Oracle Database@AWS unterstützt das CIDR-Management von Peer-Netzwerken für Peering-Verbindungen	Sie können ein Peer-Netzwerk angeben CIDRs , wenn Sie ODB-Peering-Verbindungen erstellen oder aktualisieren. Sie steuern, welche Subnetze in der Peer-VPC Zugriff auf Ihr ODB-Netzwerk haben. Ein VPC-Konto kann die CIDR-Bereiche aktualisieren, ohne auch das ODB-Netzwerk zu besitzen. Weitere Informationen finden Sie unter Konfiguration von ODB-Peering für eine Amazon VPC in. Oracle Database@AWS	10. Oktober 2025

Oracle Database@AWS unterstützt die Zero-ETL-Integration mit Amazon Redshift	Oracle Database@AWS lässt sich jetzt in VPC Lattice integrieren, um eine Zero-ETL-Integration mit Amazon Redshift zu ermöglichen. Weitere Informationen finden Sie unter Service-Integrationen für Oracle Database@AWS.	2. Juli 2025
Aktualisieren auf Berechtigungen für serviceverknüpfte IAM-Rollen	Die `AmazonODBServiceRolePolicy` Richtlinie gewährt nun zusätzliche Berechtigungen zur Beschreibung von VPC-Transit-Gateway-Anhängen, zur Beschreibung von EC2 Amazon-Subnetzen und zur Aktivierung einer EventBridge Amazon-Quelle. Weitere Informationen finden Sie unter Oracle Database@AWS Aktualisierungen der AWS verwalteten Richtlinien.	30. Juni 2025
Aktualisieren auf Berechtigungen für serviceverknüpfte IAM-Rollen	Die `AmazonODBServiceRolePolicy` Richtlinie gewährt jetzt zusätzliche Berechtigungen, um Ereignisse in Amazon EventBridge Scheduler zu beschreiben und einen Event-Bus zu erstellen oder zu beschreiben. Weitere Informationen finden Sie unter Oracle Database@AWS Aktualisierungen der AWS verwalteten Richtlinien.	26. Juni 2025

Oracle Database@AWS unterstützt die Region USA West (Oregon)	Sie können Ihre Oracle Database@AWS Ressourcen in der Region USA West (Oregon) erstellen. Die unterstützten physischen AZ IDs sind `usw2-az3` und `usw2-az4`. Weitere Informationen finden Sie unter Unterstützte Regionen für Oracle Database@AWS.	26. Juni 2025
Oracle Database@AWS unterstützt die gemeinsame Nutzung von Ressourcen zwischen AWS-Konten	Mit AWS Resource Access Manager (AWS RAM) können Sie jetzt die Exadata-Infrastruktur und VM-Cluster mit anderen AWS-Konten innerhalb Ihrer Organisation gemeinsam nutzen. Sie können die Infrastruktur einmal bereitstellen und sie dann für mehrere Konten gemeinsam nutzen, wodurch die Kosten gesenkt und gleichzeitig die Zuständigkeitstrennung gewahrt bleibt. Weitere Informationen finden Sie unter Resource Sharing in Oracle Database@AWS.	26. Juni 2025

Oracle Database@AWS unterstützt Veranstaltungen in Amazon EventBridge	Oracle Database@AWS übermittelt Ereignisse an Amazon EventBridge , um Änderungen im Ressource nlebenszyklus zu überwache n. Ereignisse werden AWS sowohl aus OCI-Quellen als auch aus OCI-Quell en generiert, sodass Sie Änderungen am ODB-Netzw erk, an der Exadata-Infrastruk tur, an VM-Clustern und Datenbanken verfolgen können. Weitere Informati onen finden Sie unter Oracle Database@AWS Ereignisse in Amazon überwachen EventBridge.	26. Juni 2025
Oracle Database@AWS unterstützt regionsübergreifen des Abonnement	Oracle Database@AWS unterstützt regionsübergreifen des Abonnement, sodass Sie den Dienst einmal abonnieren und den Dienst dann in vollem Umfang nutzen können. AWS-Regionen Weitere Informati onen finden Sie unter Oracle Database@AWS in mehreren Regionen abonnieren.	26. Juni 2025

Oracle Database@AWS unterstützt ODB-Peering-Verbindungen als separate Ressource	ODB-Peering-Verbindungen sind jetzt eine separate Ressource, die speziell APIs für das Erstellen, Anzeigen und Löschen von Peering-Verbindungen vorgesehen ist. Sie können Peering-V erbindungen zwischen einem ODB-Netzwerk und einer Amazon VPC im selben Konto oder in verschiedenen Konten herstellen. Weitere Informati onen finden Sie unter Arbeiten mit ODB-Peering-Verbin dungen.	26. Juni 2025
Oracle Database@AWS integriert das ODB-Netzwerk mit Amazon S3	Oracle Database@AWS lässt sich jetzt in VPC Lattice integrieren, um von Oracle verwaltete Backups auf Amazon S3 und direkten ODB-Netzwerkzugriff auf Amazon S3 zu ermöglichen. Weitere Informationen finden Sie unter Serviceintegrationen für Oracle Database@.AWS	26. Juni 2025

Oracle Database@AWS unterstützt autonome VM-Cluster	Sie können jetzt autonome VM-Cluster auf Ihrer Exadata-Infrastruktur erstellen. Autonome VM-Cluster sind vollständig verwaltete Datenbanken, die wichtige Verwaltungsaufgaben mithilfe von maschinellem Lernen und KI automatisieren. Weitere Informationen finden Sie unter Schritt 3: Erstellen eines Exadata-VM-Clusters oder eines Autonomen VM-Clusters in. Oracle Database@AWS	28. Mai 2025
Oracle Database@AWS unterstützt anpassbare Wartungsfenster	Sie können jetzt Wartungsfenster für Ihre Exadata-Infrastruktur mit Optionen für von Oracle oder vom Kunden verwaltete Zeitpläne konfigurieren. Sie können auch die Patch-Modi (fortlaufend oder nicht fortlaufend) auswählen und die Einstellungen für den Wartungszeitpunkt festlegen. Weitere Informationen finden Sie unter Erstellen einer Oracle Exadata-Infrastruktur in. Oracle Database@AWS	01. Mai 2025
Oracle Database@AWS unterstützt eine neue Availability Zone (AZ)	Sie können jetzt ein ODB-Netzwerk in einer AZ mit der physischen ID `use1-az4` oder `use1-az6` erstellen. Weitere Informationen finden Sie unter Oracle Exadata Infrastructure.	26. März 2025

Oracle Database@AWS unterstützt Amazon VPC Transit Gateways	Wenn Sie ein Transit-Gateway mit einer VPC verbinden, die mit einem ODB-Netzwerk verbunden ist, können Sie mehrere Verbindungen VPCs zu diesem Gateway herstellen. Anwendungen, die in diesen ausgeführt werden, VPCs können auf einen Exadata-VM-Cluster zugreifen, der in Ihrem ODB-Netzwerk läuft. Weitere Informationen finden Sie unter Konfiguration von Amazon VPC Transit Gateways für. Oracle Database@AWS	26. März 2025
Oracle Database@AWS unterstützt Datenbank- und Speicherservertypen für Exadata X11M	Sie können den Datenbankservertyp und den Speicherservertyp angeben, wenn Sie eine Infrastruktur mit Exadata X11M erstellen. Weitere Informationen finden Sie unter Erstellen einer Oracle Exadata-Infrastruktur unter. Oracle Database@AWS	4. Februar 2025

Neue Richtlinie für dienstbezogene Rollen	Oracle Database@AWS hat eine neue Richtlinie `AmazonODBServiceRolePolicy` für die `AWSServiceRoleForODB` dienstbezogene Rolle hinzugefügt. Weitere Informationen finden Sie unter Oracle Database@AWS -Aktualisierungen von AWS -verwalteten Richtlinien.	2. Dezember 2024
Erstversion	Erste Veröffentlichung des Oracle Database@AWS Benutzerhandbuchs	2. Dezember 2024

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.