Oracle Database@AWS Panduan Pengguna

Oracle Database@AWS

Oracle Database@AWS: Oracle Database@AWS Panduan Pengguna

Table of Contents

Apa itu Oracle Database@AWS?

Oracle Database@AWS adalah penawaran yang memungkinkan Anda mengakses infrastruktur Oracle Exadata yang dikelola oleh Oracle Cloud Infrastructure (OCI) di dalam pusat data. AWS Anda dapat memigrasikan beban kerja Oracle Exadata, membangun konektivitas latensi rendah dengan aplikasi yang berjalan, dan berintegrasi dengan layanan. AWS AWS Anda mendapatkan satu faktur melalui AWS Marketplace, yang diperhitungkan terhadap AWS komitmen dan hadiah Oracle Support.

Diagram berikut menunjukkan gambaran tingkat tinggi dari wilayah OCI yang terkait dengan pusat AWS data yang menampung infrastruktur Oracle Exadata. Dalam AWS Availability Zone (AZ), Anda dapat mengintip VPC Amazon ke jaringan pribadi yang terikat ke pusat data. Dengan mengintip jaringan ini, server aplikasi di VPC dapat mengakses database Oracle yang berjalan pada infrastruktur Oracle Exadata.

Fitur Oracle Database@AWS

Dengan Oracle Database@AWS, Anda mendapat manfaat dari fitur-fitur berikut:

Migrasi beban kerja database Oracle Exadata ke AWS

Dengan Oracle Database@AWS, Anda dapat dengan mudah memigrasikan beban kerja Oracle Exadata Anda ke Oracle Exadata Database Service on Dedicated Infrastructure atau Oracle Autonomous Database pada Infrastruktur Exadata Khusus di dalamnya. AWS Migrasi ini menawarkan perubahan minimal, ketersediaan fitur lengkap, kompatibilitas arsitektur, dan kinerja yang sama seperti penerapan Exadata lokal. Anda dapat menggunakan alat migrasi database Oracle standar seperti Recovery Manager (RMAN), Oracle Data Guard, tablespace yang dapat diangkut, Oracle Data Pump, Oracle, Database GoldenGate Migration AWS Service, dan Oracle Zero Downtime Migration.

Mengurangi latensi aplikasi

Anda dapat membuat konektivitas latensi rendah antara Oracle Exadata dan aplikasi yang berjalan. AWS Kedekatan dengan aplikasi yang dihosting AWS memastikan penundaan jaringan minimal dan peningkatan kinerja.

Inovasi melalui penyatuan data

Anda dapat menghasilkan wawasan yang lebih dalam dan mengembangkan inovasi baru dengan menggunakan integrasi nol-ETL untuk menyatukan data Anda di seluruh Oracle dan AWS untuk

analitik, pembelajaran mesin, dan AI generatif. Dengan integrasi nol-ETL menggunakan Amazon Redshift, Anda dapat mengaktifkan analisis real-time dan pembelajaran mesin (ML) dekat waktu nyata pada data transaksional yang disimpan di dalamnya. Oracle Database@AWS

Manajemen dan operasi yang disederhanakan

Anda bisa mendapatkan keuntungan dari pengalaman terpadu antara Oracle dan AWS dengan dukungan kolaboratif, pembelian, manajemen, dan operasi. Penggunaan layanan Oracle Database Anda memenuhi syarat untuk AWS komitmen yang ada dan manfaat lisensi Oracle, seperti Oracle Support Rewards. Anda dapat menggunakan AWS alat dan antarmuka yang sudah dikenal untuk membeli, menyediakan, dan mengelola Oracle Database@AWS sumber daya Anda. Anda dapat menyediakan dan mengelola sumber daya Anda menggunakan AWS APIs, CLI, atau. SDKs AWS APIs Panggilan OCI terkait yang APIs diperlukan untuk menyediakan dan mengelola sumber daya.

Integrasi yang mulus dengan layanan AWS

Anda dapat berintegrasi dengan AWS layanan dan aplikasi lain yang berjalan di lingkungan yang sama. Misalnya, Oracle Database@AWS terintegrasi dengan Amazon EC2, Amazon VPC, dan IAM. Anda juga dapat berintegrasi Oracle Database@AWS dengan AWS layanan seperti Amazon CloudWatch untuk pemantauan dan Amazon EventBridge untuk manajemen acara. Untuk pencadangan basis data, Anda dapat menggunakan Amazon S3, yang dirancang untuk melebihi daya tahan 11 9 detik.

Terkait Layanan AWS

Oracle Database@AWS bekerja dengan layanan berikut untuk meningkatkan ketersediaan dan skalabilitas aplikasi database Oracle Anda:

- Amazon EC2 — Menyediakan server virtual yang berfungsi sebagai server aplikasi Oracle. Anda dapat mengonfigurasi penyeimbang beban untuk merutekan lalu lintas ke server EC2 aplikasi Anda. Untuk informasi selengkapnya, lihat Panduan EC2 Pengguna Amazon.
- Amazon Virtual Private Cloud (VPC) - Memungkinkan Anda meluncurkan AWS sumber daya dalam jaringan virtual yang terisolasi secara logis yang telah Anda tentukan. Infrastruktur Oracle Exadata berada di jaringan khusus yang disebut jaringan ODB yang dapat Anda peer ke VPC. Anda kemudian dapat menjalankan server aplikasi di VPC Anda dan mengakses database Exadata Anda. Untuk informasi selengkapnya, silakan lihat ACL Jaringan di Panduan Pengguna Amazon VPC.

- Amazon VPC Lattice - Menyediakan akses asli ke AWS layanan seperti Amazon S3 dan cadangan terkelola Oracle dari jaringan ODB. Untuk informasi lebih lanjut, lihat Apa itu Amazon VPC Lattice? .
- Amazon CloudWatch — Menyediakan layanan pemantauan untuk Oracle Database@AWS. OCI mengumpulkan data metrik tentang sistem Oracle Exadata Anda dan mengirimkannya ke. CloudWatch Untuk informasi selengkapnya, lihat Pemantauan Oracle Database@AWS dengan Amazon CloudWatch.
- AWS Identity and Access Management (IAM) - Membantu Anda mengontrol akses ke Oracle Database@AWS sumber daya untuk pengguna Anda dengan aman. Gunakan IAM untuk mengontrol siapa yang dapat menggunakan AWS sumber daya Anda (otentikasi) dan sumber daya apa yang dapat digunakan pengguna dengan cara apa (otorisasi). Untuk informasi selengkapnya, lihat Manajemen identitas dan akses untuk Oracle Database@AWS.
- AWS layanan analitik — Menyediakan serangkaian layanan analitik yang luas dan hemat biaya untuk membantu Anda mendapatkan wawasan lebih cepat dari database Exadata Anda. Setiap layanan dibuat khusus untuk berbagai kasus penggunaan analitik seperti analisis interaktif, pemrosesan data besar, pergudangan data, analitik real-time, analitik operasional, dasbor, dan visualisasi. Untuk informasi selengkapnya, lihat Analytics on AWS.

Mengakses Oracle Database@AWS

Anda dapat membuat, mengakses, dan mengelola Oracle Database@AWS menggunakan Konsol Manajemen AWS. Ini menyediakan antarmuka web yang dapat Anda gunakan untuk mengakses Oracle Database@AWS.

Harga untuk Oracle Database@AWS

Anda dapat membeli Oracle Database@AWS penawaran dari. AWS Marketplace Anda pertama kali menghubungi perwakilan penjualan Oracle. Oracle kemudian membuat penawaran tersedia untuk Anda AWS Marketplace berdasarkan perjanjian harga pribadi. AWS Tagihan Anda menunjukkan biaya berdasarkan penggunaan Anda.

Tidak ada biaya transfer data ketika aplikasi Oracle dan database Oracle Anda di-host di Availability Zone (AZ) yang sama. Biaya transfer data standar berlaku untuk komunikasi antara AZs.

Saat menggunakan integrasi Oracle Database@AWS terkelola seperti Zero-ETL, backup terkelola Oracle, dan Amazon S3, biaya pemrosesan data standar untuk berbagi dan mengakses sumber

daya melalui VPC Lattice berlaku. Tidak ada biaya per jam untuk integrasi Oracle Database@AWS terkelola. Untuk informasi selengkapnya, lihat harga Amazon VPC Lattice.

Apa selanjutnya?

Anda sekarang siap untuk mulai membuat Oracle Database@AWS sumber daya Anda.

1. Pelajari tentang cara Oracle Database@AWS kerja. Untuk informasi selengkapnya, lihat Bagaimana cara Oracle Database@AWS kerja.

   > **Note**
   >
   > Jika Anda sudah familiar dengan AWS dan Oracle Exadata dan ingin segera memulai, lewati langkah ini.

2. Minta penawaran pribadi untuk Oracle Database@AWS melalui Konsol Manajemen AWS, dan kemudian menerima tawaran itu. Untuk informasi selengkapnya, lihat Minta penawaran pribadi untuk Oracle Database@AWS.

   > **Note**
   >
   > Untuk meminta penawaran pribadi dalam pratinjau ini, Anda harus menghubungi AWS untuk Akun AWS menambahkan Anda ke daftar izin.

3. Buat jaringan ODB Anda, infrastruktur Oracle Exadata, dan cluster Exadata VM menggunakan konsol. AWS Buat database Exadata Anda menggunakan alat OCI. Untuk informasi selengkapnya, lihat Memulai dengan Oracle Database @AWS.
4. Bagikan sumber daya Anda di seluruh akun dengan AWS Resource Access Manager (AWS RAM). Lihat informasi yang lebih lengkap di Bekerja dengan Oracle Database@AWS sumber daya bersama di akun tepercaya.

Bagaimana cara Oracle Database@AWS kerja

Oracle Database@AWS mengintegrasikan Oracle Cloud Infrastructure (OCI) dengan file. AWS Cloud Di bagian berikut, Anda dapat mempelajari tentang komponen kunci arsitektur multicloud ini.

Oracle Exadata Database Service on Dedicated Infrastructure adalah layanan OCI yang menyediakan Exadata Database Machine. Oracle Exadata Database Machine adalah platform full-stack terintegrasi, telah dikonfigurasi, dan telah diuji sebelumnya untuk digunakan di pusat data perusahaan. Anda dapat membuat infrastruktur Oracle Exadata dan cluster VM di AWS Availability Zone (AZ) menggunakan konsol AWS , CLI, atau. APIs

Setelah Anda membuat sumber daya AWS, Anda menggunakan OCI APIs untuk membuat dan mengelola database Oracle Exadata. Jaringan ODB, yang Anda peer ke VPC Amazon, memungkinkan server EC2 aplikasi Amazon untuk mengakses database Exadata Anda. Dengan cara ini, database Oracle Exadata diintegrasikan ke dalam lingkungan. AWS

Diagram berikut menunjukkan Oracle Database@AWS arsitektur.

Situs anak OCI

Oracle Cloud Infrastructure di-host di wilayah OCI dan domain ketersediaan. Wilayah OCI terdiri dari domain ketersediaan OCI (ADs), yang merupakan cluster pusat data terisolasi dalam wilayah OCI. Situs anak OCI adalah pusat data yang memperluas domain ketersediaan OCI ke Availability Zone (AZ) di suatu Wilayah. AWS Infrastruktur Exadata secara logis berada di wilayah OCI dan secara fisik berada di suatu Wilayah. AWS

Situs anak OCI untuk Oracle Database@AWS secara fisik berada di pusat AWS data. AWS host infrastruktur Exadata, dan ketentuan OCI dan memelihara perangkat keras infrastruktur Exadata di dalam pusat data. Anda dapat mengonfigurasi infrastruktur Exadata, jaringan pribadi, dan cluster VM menggunakan konsol AWS , CLI, atau. APIs Anda dapat menggunakan AWS layanan seperti Amazon EC2 dan Amazon VPC untuk memungkinkan akses aplikasi ke database Oracle Exadata yang berjalan pada infrastruktur.

Infrastruktur Oracle Exadata

Infrastruktur Oracle Exadata adalah arsitektur dasar server database dan server penyimpanan yang menjalankan database Oracle Exadata. Infrastruktur berada di AWS Availability Zone (AZ). Untuk membuat cluster VM pada infrastruktur Exadata, Anda menggunakan konsol, CLI AWS , atau. APIs

Infrastruktur Oracle Exadata didistribusikan pada mesin fisik yang disebut server database. Server ini menyediakan sumber daya komputasi, mirip dengan server EC2 khusus Amazon. Setiap server database menghosting satu atau lebih mesin virtual (VMs) yang berjalan pada hypervisor. Untuk diagram arsitektur yang menggambarkan hubungan ini, lihat Exadata Database Service on Dedicated Infrastructure Technical Architecture.

Ketika Anda membuat infrastruktur Exadata di Oracle Database @AWS, Anda menentukan informasi seperti berikut:

- Jumlah total server database
- Jumlah total server penyimpanan
- Model sistem Exadata (X11M)
- AZ yang menampung infrastruktur (lihatWilayah yang Didukung untuk Oracle Database@AWS)

Untuk mempelajari cara membuat infrastruktur Oracle Exadata, lihat. Langkah 2: Buat infrastruktur Oracle Exadata di Oracle Database@AWS

Jaringan ODB

Jaringan ODB adalah jaringan terisolasi pribadi yang menampung infrastruktur OCI di AWS Availability Zone (AZ). Jaringan ODB terdiri dari berbagai alamat IP CIDR. Jaringan ODB memetakan langsung ke jaringan yang ada di dalam situs anak OCI, sehingga berfungsi sebagai sarana komunikasi antara AWS dan OCI. Anda harus menentukan jaringan ODB saat membuat cluster Exadata VM Anda (lihat). Langkah 3: Buat cluster Exadata VM atau cluster VM Autonomous di Oracle Database@AWS

Anda menyediakan sumber daya dalam jaringan ODB menggunakan Oracle Database@.AWS APIs Jaringan ODB dikelola oleh AWS, tetapi Anda dapat mengatur koneksi peering ODB untuk menghubungkan VPC Amazon ke jaringan ODB. Untuk informasi lebih lanjut, lihat enODB mengintip.

Saat Anda membuat jaringan ODB, Anda menentukan informasi seperti berikut ini:

- Availability Zone — Jaringan ODB khusus untuk AZ.

  Anda dapat menggunakan Oracle Database@AWS berikut ini Wilayah AWS:

  AS Timur (Virginia Utara)

  Anda dapat menggunakan AZs dengan fisik IDs `use1-az4` dan`use1-az6`.

  AS Barat (Oregon)

  Anda dapat menggunakan AZs dengan fisik IDs `usw2-az3` dan`usw2-az4`.

  Asia Pasifik (Tokyo)

  Anda dapat menggunakan AZs dengan fisik IDs `apne1-az1` dan`apne1-az4`.

  AS Timur (Ohio)

  Anda dapat menggunakan AZs dengan fisik IDs `use2-az1` dan`use2-az2`.

  Eropa (Frankfurt)

  Anda dapat menggunakan AZs dengan fisik IDs `euc1-az1` dan`euc1-az2`.

  Kanada (Pusat)

  Anda dapat menggunakan AZ dengan ID fisik`cac1-az4`.

  Asia Pasifik (Sydney)

  Anda dapat menggunakan AZ dengan ID fisik`apse2-az4`.

  Untuk menemukan nama AZ logis di akun Anda yang memetakan ke AZ fisik sebelumnya IDs, jalankan perintah berikut.

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

- Alamat CIDR klien - Jaringan ODB memerlukan CIDR subnet klien untuk cluster Exadata VM dan cluster VM Autonomous.
- Backup alamat CIDR - Jaringan ODB memerlukan CIDR subnet cadangan untuk backup database terkelola dari cluster VM. Subnet cadangan adalah opsional untuk cluster Exadata VM.

- AWS integrasi layanan - Anda dapat mengonfigurasi jalur jaringan untuk integrasi AWS layanan seperti Amazon S3 dan Zero-ETL dengan Amazon Redshift. Untuk informasi selengkapnya, lihat AWS integrasi layanan.

Untuk informasi selengkapnya, lihat Langkah 1: Buat jaringan ODB di Oracle Database@AWS.

Cloud Privat Virtual (VPC)

Virtual Private Cloud (VPC) adalah jaringan virtual yang Anda buat di cloud. AWS Ini secara logis terisolasi dari jaringan virtual lain di AWS cloud, memberi Anda kontrol penuh atas lingkungan jaringan virtual, termasuk pemilihan rentang alamat IP Anda sendiri, pembuatan subnet, dan konfigurasi tabel rute dan gateway jaringan. Untuk informasi selengkapnya, lihat Apa itu Amazon VPC?

Anda dapat meluncurkan EC2 instans Amazon ke VPC Amazon Anda. EC2 Instans dapat meng-host server aplikasi yang berkomunikasi dengan database Oracle Exadata. Anda dapat mengelola dan meluncurkan server aplikasi seperti halnya EC2 instance lain di VPC Anda. Untuk informasi selengkapnya, lihat Apa itu Amazon EC2?

Secara default, jaringan ODB tidak memiliki konektivitas ke VPCs. Untuk menghubungkan jaringan ODB ke AWS infrastruktur yang ada, buat koneksi peering antara jaringan ODB dan satu VPC. Anda dapat menentukan VPC saat Anda membuat jaringan ODB. Untuk informasi selengkapnya, lihat Langkah 1: Buat jaringan ODB di Oracle Database@AWS.

ODB mengintip

ODB peering adalah koneksi jaringan buatan pengguna yang memungkinkan lalu lintas dirutekan secara pribadi antara VPC Amazon dan jaringan ODB. Ada hubungan 1:1 antara VPC dan jaringan ODB. Setelah mengintip, EC2 instance Amazon dalam VPC dapat berkomunikasi dengan database Oracle Exadata di jaringan ODB seolah-olah mereka berada dalam jaringan yang sama.

> **Note**
>
> ODB peering berbeda dari VPC peering, yang merupakan koneksi peering antara dua VPCs yang mengarahkan lalu lintas di antara mereka.

Anda dapat mengintip jaringan ODB di satu akun dan VPC di akun lain menggunakan. AWS RAM Jika Anda berbagi jaringan ODB dengan akun lain, akun trust dapat langsung memulai peering. Akun yang memulai koneksi peering ODB memiliki dan mengelola koneksi.

Anda dapat menentukan jaringan peer CIDRs saat membuat atau memperbarui koneksi peering ODB. Dengan cara ini, Anda mengontrol subnet mana di VPC rekan yang memiliki akses ke jaringan ODB Anda. Akun VPC dapat memperbarui rentang CIDR tanpa juga memiliki jaringan ODB. Untuk informasi selengkapnya, lihat Mengonfigurasi ODB mengintip ke VPC Amazon di. Oracle Database@AWS

Sumber daya dalam VPC dapat menjangkau Availability Zones ()AZs. Dalam jaringan ODB, sumber daya terikat pada satu AZ. Anda menentukan AZ ini ketika Anda membuat jaringan ODB.

Pembuatan koneksi peering ODB

Koneksi peering ODB bukanlah karakteristik jaringan ODB tetapi merupakan sumber daya independen dengan ID sendiri (diawali dengan) dan siklus hidup. `odbpcx-` Anda mengelola koneksi peering dengan satu set khusus APIs. Misalnya, Anda membuat koneksi peering ODB ke jaringan ODB yang ada menggunakan konsol Oracle AWS Database@ atau API. `CreateOdbPeeringConnection` Untuk informasi selengkapnya, lihat Membuat koneksi peering ODB di Oracle Database@AWS.

Saat Anda membuat koneksi peering ODB, Oracle Database@AWS melakukan tindakan berikut secara otomatis:

1. Memvalidasi konfigurasi jaringan, termasuk memeriksa blok CIDR yang tumpang tindih dengan Oracle VCN CIDR
2. Menyiapkan infrastruktur pengintip jaringan yang mendasarinya
3. Mengonfigurasi tabel rute jaringan ODB (bukan VPC) dengan alamat CIDR VPC

Setelah Anda membuat koneksi peering ODB, perbarui tabel rute VPC Anda secara manual menggunakan perintah Amazon. EC2 `create-route` Untuk informasi selengkapnya, lihat Mengkonfigurasi tabel rute VPC untuk mengintip ODB.

AWS integrasi layanan

Untuk menyediakan opsi fungsionalitas dan konektivitas yang disempurnakan untuk database Oracle Anda, Oracle Database@ terintegrasi dengan AWS menggunakan Amazon VPC Lattice. Layanan

AWS Anda dapat mengonfigurasi jalur jaringan Layanan AWS langsung dari jaringan ODB Anda tanpa memerlukan pengaturan jaringan tambahan VPCs atau kompleks.

Oracle Database@AWS mendukung integrasi layanan AWS terkelola berikut:

Amazon S3

Anda dapat mengintegrasikan Amazon S3 dengan Oracle Database@AWS dengan cara berikut:

- Oracle mengelola backup otomatis ke Amazon S3 - Oracle Database @AWS secara otomatis memungkinkan akses jaringan untuk backup otomatis. Integrasi ini tidak dapat dinonaktifkan. Jika Anda menetapkan Amazon S3 sebagai target pencadangan terkelola di konsol OCI, OCI akan mengunggah cadangan otomatis ke bucket S3.
- Akses langsung ke Amazon S3 dari jaringan ODB Anda - Anda dapat mengaktifkan akses jaringan ODB langsung ke S3 dan kemudian menyimpan skrip, mengimpor dan mengekspor file, dan file terkait dalam bucket S3. Anda dapat menonaktifkan akses ini. Pengaturan ini tidak tergantung pada akses jaringan otomatis untuk backup otomatis yang dikelola Oracle.

Integrasi nol-ETL dengan Amazon Redshift

Anda dapat mengaktifkan integrasi nol-ETL jaringan ODB Anda dengan Amazon Redshift. Integrasi ini memungkinkan Anda untuk mereplikasi data ke Amazon Redshift dari database Oracle Anda yang berjalan di Oracle AWS Database@ tanpa proses ekstrak, transformasi, dan pemuatan (ETL) tradisional. Integrasi ini memungkinkan analitik real-time dan beban kerja AI dengan secara otomatis menyinkronkan data Oracle Anda dengan Amazon Redshift.

Selain integrasi terkelola untuk AWS layanan, Anda juga dapat menggunakan VPC Lattice untuk mengakses layanan dan sumber daya yang dihosting di tempat VPCs lain, atau mengakses instance jaringan ODB dari VPC Anda. Anda dapat mengelola akses dan sumber daya menggunakan konsol VPC Lattice, CLI, dan. APIs Untuk informasi selengkapnya, lihat sumber daya berikut:

- Mencadangkan di Oracle Database @AWS
- Database Oracle@ Integrasi AWS nol-ETL dengan Amazon Redshift
- Apa itu Amazon VPC Lattice? dan VPC Lattice untuk Oracle Database @AWS

Routing lalu lintas dari beberapa VPCs

Untuk memungkinkan beberapa VPCs orang mengakses Oracle Database@AWS sumber daya dalam satu jaringan ODB, Anda dapat menggunakan AWS Transit Gateway atau AWS Cloud WAN.

AWS Transit Gateway

Gateway transit VPC Amazon adalah hub transit jaringan yang digunakan untuk interkoneksi VPCs dan jaringan lokal. Jaringan ODB hanya mendukung peering one-to-one langsung antara jaringan ODB dan satu VPC. Anda dapat mengintip jaringan ODB Anda ke VPC, dan kemudian melampirkan VPC ini ke gateway transit. Gateway dapat terhubung ke beberapa VPCs. Dengan konfigurasi gateway transit ini, Anda dapat merutekan lalu lintas antara beberapa subnet VPC ke satu jaringan ODB.

Untuk informasi selengkapnya, lihat Mengkonfigurasi Gateway Transit VPC Amazon untuk Oracle Database@AWS.

AWS Awan WAN

AWS Cloud WAN adalah layanan jaringan area luas terkelola (WAN) yang memungkinkan Anda membangun, mengelola, dan memantau jaringan global terpadu yang menghubungkan sumber daya di seluruh lingkungan cloud dan lokal Anda. Dengan menggunakan dasbor pusat, Anda dapat menghubungkan kantor cabang lokal, pusat data, dan VPCs di seluruh jaringan AWS global.

Anda dapat mengintip jaringan ODB Anda ke VPC, dan kemudian melampirkan VPC ini ke jaringan inti Cloud WAN. Dengan konfigurasi ini, Anda dapat menggunakan Cloud WAN untuk merutekan lalu lintas antara beberapa VPCs atau jaringan lokal dan jaringan ODB Anda. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS Cloud WAN untuk Oracle Database@AWS.

Cluster Exadata VM

Cluster Exadata VM adalah satu set Exadata yang digabungkan dengan erat. VMs Setiap VM memiliki instalasi database Oracle lengkap yang mencakup semua fitur Oracle Enterprise Edition, termasuk Oracle Real Application Clusters (Oracle RAC) dan Oracle Grid Infrastructure. Anda dapat membuat satu atau lebih database Oracle Exadata pada cluster VM. Untuk diagram yang menunjukkan arsitektur VMs dan klaster VM, lihat Exadata Database Service on Dedicated Infrastructure Technical Architecture.

Saat Anda membuat cluster VM, Anda menentukan informasi yang mencakup yang berikut ini:

- Jaringan ODB
- Infrastruktur Oracle Exadata

- Server database tempat untuk menempatkan VMs di cluster
- Jumlah total penyimpanan Exadata yang dapat digunakan

Anda dapat mengonfigurasi inti CPU, memori, dan penyimpanan lokal untuk setiap VM di cluster VM. Untuk informasi selengkapnya, lihat Langkah 3: Buat cluster Exadata VM atau cluster VM Autonomous di Oracle Database@AWS.

Cluster VM otonom

Cluster VM otonom adalah database yang dikelola sepenuhnya yang mengotomatiskan tugas manajemen utama menggunakan pembelajaran mesin dan AI. Tidak seperti database tradisional, database otonom secara otomatis menyediakan, mengamankan, memperbarui, mencadangkan, dan menyetel database tanpa campur tangan manusia yang diperlukan.

Anda dapat mengonfigurasi jumlah inti ECPU per VM, memori database per CPU, penyimpanan basis data, dan jumlah maksimum database kontainer otonom. Untuk informasi selengkapnya, lihat Langkah 3: Buat cluster Exadata VM atau cluster VM Autonomous di Oracle Database@AWS.

Database Oracle Exadata

Oracle Exadata adalah sistem rekayasa yang menyediakan platform berkinerja tinggi untuk menjalankan database Oracle. Dengan Oracle Database@AWS, Anda menggunakan AWS konsol untuk membuat infrastruktur Oracle Exadata dan cluster VM yang menjadi tuan rumah database Exadata. Anda kemudian menggunakan OCI APIs untuk membuat dan mengelola database Oracle. Lihat informasi yang lebih lengkap di Langkah 4: Buat database Oracle Exadata di Oracle Cloud Infrastructure.

Orientasi ke Oracle Database @AWS

Sebelum Anda dapat mulai menggunakan Oracle Database@AWS, pastikan Anda mendaftar AWS dan membuat pengguna yang diperlukan. Kemudian Anda dapat membeli Oracle Database@AWS dari AWS Marketplace dengan menerima penawaran pribadi dari Oracle.

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke Konsol Manajemen AWSsebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.

2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Minta penawaran pribadi untuk Oracle Database@AWS

Fitur penawaran pribadi AWS Marketplace penjual memungkinkan Anda untuk meminta dan menerima AWS harga Oracle Database @ dan ketentuan EULA dari Oracle. Anda menegosiasikan harga dan persyaratan dengan Oracle, dan kemudian Oracle membuat penawaran pribadi untuk yang Anda tunjuk Akun AWS . Anda menerima penawaran pribadi dan menerima harga yang dinegosiasikan dan ketentuan penggunaan. Saat ini, Anda dapat menggunakan Oracle Database@AWS dasbor. Ketika perjanjian penawaran pribadi mencapai tanggal kedaluwarsa, Anda akan dipindahkan secara otomatis ke harga publik produk atau berhenti berlangganan dari Oracle Database@.AWS Untuk informasi selengkapnya tentang penawaran pribadi, lihat Penawaran pribadi di AWS Marketplace.

Untuk meminta dan menerima penawaran pribadi untuk Oracle Database@AWS

1. Masuk ke Konsol Manajemen AWS.
2. Cari dan kemudian pilih Oracle Database AWS@.
3. Pilih Minta penawaran pribadi.

> **Note**
>
> Oracle Database@AWS Dasbor tidak tersedia sampai setelah Anda menerima penawaran pribadi.

4. Di situs Oracle Cloud Infrastructure (OCI), tentukan detail seperti wilayah dan informasi kontak Anda.
5. Tunggu perwakilan OCI untuk menghubungi Anda dan membuat penawaran pribadi tersedia.
6. Di bagian Konsol Manajemen AWS, pilih Lihat penawaran pribadi.
7. Pilih penawaran dan kemudian pilih Lihat penawaran.
8. Pilih Buat kontrak dan tanggapi permintaan berikutnya untuk menerima penawaran pribadi.
9. Setelah menerima penawaran pribadi, Anda harus mengaktifkan akun OCI Anda. Anda dapat mengakses tautan aktivasi Oracle langsung dari Konsol Manajemen AWS.
    1. Di konsol, arahkan ke bagian Memulai.
    2. Klik tautan aktivasi Oracle yang disediakan di konsol. Atau, Anda juga dapat menggunakan tautan aktivasi yang dikirimkan kepada Anda melalui email.

3. Pada halaman aktivasi Oracle, pilih apakah akan membuat akun cloud Oracle baru atau menambahkan ke akun yang sudah ada.
4. Selesaikan proses aktivasi dengan mengikuti instruksi di layar.
5. Setelah mengirimkan permintaan aktivasi Anda, Anda akan melihat status Aktivasi dalam proses di Konsol Manajemen AWS, dan dasbor akan dinonaktifkan sementara dengan alasan ditampilkan.
6. Setelah aktivasi selesai,AWS dasbor Oracle Database@ menjadi tersedia, memungkinkan Anda untuk mengelola sumber daya Anda.

10. Di bagian Konsol Manajemen AWS, pilih Dasbor.

Berlangganan Oracle Database@AWS di beberapa Wilayah

Saat Anda berlangganan Oracle Database@AWS melalui AWS Marketplace dan menyelesaikan orientasi, Anda Akun AWS ditautkan ke sewa OCI Anda. Tautan ini, bersama dengan sumber daya terkait, secara otomatis direplikasi ke semua AWS Wilayah jika Oracle Database@AWS tersedia. Anda berlangganan dan onboard sekali daripada mengulangi proses untuk setiap Wilayah.

Untuk digunakan Oracle Database@AWS di beberapa Wilayah, lakukan langkah-langkah berikut:

1. Berlangganan Oracle Database@AWS melalui AWS Marketplace dan selesaikan proses orientasi.

   Saat pertama kali berlangganan Oracle Database@AWS, akun Anda diaktifkan di Wilayah rumah. Anda menentukan Wilayah rumah di Oracle Cloud Infrastructure (OCI).
2. Aktifkan Wilayah pilihan Anda melalui konsol OCI.

   Jika Anda tidak mengaktifkan Wilayah di OCI, lalu beralih ke Wilayah ini di Oracle Database@AWS konsol, Anda menerima kesalahan yang menyatakan bahwa Anda belum berlangganan. Dalam hal ini, Anda harus mengaktifkan Wilayah ini di OCI sebelum Anda dapat menggunakan Oracle Database@AWS dasbor di Wilayah ini.
3. Akses Oracle Database@AWS di AWS Wilayah mana pun yang didukung tanpa mengulangi proses berlangganan.

Memulai dengan Oracle Database @AWS

Untuk mulai menggunakan Oracle Database@AWS, Anda dapat membuat sumber daya berikut menggunakan Oracle Database@AWS konsol, CLI, atau: APIs

1. Jaringan ODB
2. Infrastruktur Oracle Exadata
3. Cluster Exadata VM atau cluster VM Otonom
4. Koneksi mengintip ODB

Untuk membuat database Oracle Exadata di infrastruktur Anda, Anda harus menggunakan konsol Oracle Cloud Infrastructure (OCI) atau bukan dasbor. APIs Oracle Database@AWS Dengan demikian, Anda menyebarkan sumber daya di dua lingkungan cloud: sumber daya jaringan dan infrastruktur ada AWS, sedangkan bidang kontrol administrasi database berada di OCI. Untuk informasi selengkapnya, lihat Oracle Database@AWSdi dokumentasi Oracle Cloud Infrastructure.

Prasyarat untuk pengaturan Oracle Database@AWS

Sebelum mengonfigurasi infrastruktur Oracle Exadata Anda, pastikan Anda melakukan hal berikut:

- Lakukan langkah-langkah pada Orientasi ke Oracle Database @AWS. Anda harus menerima penawaran pribadi untuk digunakan Oracle Database@AWS.
- Berikan izin kebijakan kepada kepala IAM Anda yang tercantum di dalamnya. Memungkinkan pengguna untuk menyediakan Oracle Database@AWS sumber daya Izin ini diperlukan untuk digunakan Oracle Database@AWS.

Layanan OCI yang didukung pada Oracle Database@AWS

Oracle Database@AWS mendukung layanan Oracle Cloud Infrastructure (OCI) berikut:

- Layanan Database Oracle Exadata pada Infrastruktur Khusus - Menyediakan lingkungan Exadata khusus yang dikelola sepenuhnya dan dapat diakses di dalamnya. AWS Untuk informasi selengkapnya, lihat Oracle Cloud Exadata Database Service on Dedicated Infrastructure dalam dokumentasi OCI.

- Database Otonom pada Infrastruktur Exadata Khusus - Menyediakan lingkungan database yang sangat otomatis dan dikelola sepenuhnya yang berjalan di OCI dengan sumber daya perangkat keras dan perangkat lunak yang berkomitmen. Untuk informasi selengkapnya, lihat Tentang Database Otonom tentang Infrastruktur Exadata Khusus dalam dokumentasi OCI.

Wilayah yang Didukung untuk Oracle Database@AWS

Anda dapat menggunakan Oracle Database@AWS berikut ini Wilayah AWS:

AS Timur (Virginia Utara)

Anda dapat menggunakan AZs dengan fisik IDs `use1-az4` dan`use1-az6`.

AS Barat (Oregon)

Anda dapat menggunakan AZs dengan fisik IDs `usw2-az3` dan`usw2-az4`.

Asia Pasifik (Tokyo)

Anda dapat menggunakan AZs dengan fisik IDs `apne1-az1` dan`apne1-az4`.

AS Timur (Ohio)

Anda dapat menggunakan AZs dengan fisik IDs `use2-az1` dan`use2-az2`.

Eropa (Frankfurt)

Anda dapat menggunakan AZs dengan fisik IDs `euc1-az1` dan`euc1-az2`.

Kanada (Pusat)

Anda dapat menggunakan AZ dengan ID fisik`cac1-az4`.

Asia Pasifik (Sydney)

Anda dapat menggunakan AZ dengan ID fisik`apse2-az4`.

Untuk menemukan nama AZ logis di akun Anda yang memetakan ke AZ fisik sebelumnya IDs, jalankan perintah berikut.

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

```
  --output table
```

Merencanakan ruang alamat IP di Oracle Database@AWS

Rencanakan dengan hati-hati untuk ruang alamat IP di Oracle Database@AWS. Pertimbangkan konsumsi alamat IP berdasarkan jumlah cluster VM, termasuk jumlah VMs per cluster yang dapat Anda berikan ke dalam jaringan ODB. Untuk informasi selengkapnya, lihat ODB Network Design dalam kokumentasi Oracle Cloud Infrastructure.

Topik

Pembatasan untuk alamat IP di jaringan ODB

Perhatikan batasan berikut mengenai rentang CIDR di jaringan ODB:

- Anda tidak dapat memodifikasi rentang CIDR subnet klien atau cadangan untuk jaringan ODB setelah Anda membuatnya.
- Anda tidak dapat menggunakan rentang CIDR VPC di kolom Asosiasi terbatas dalam tabel di pembatasan asosiasi blok IPv4 CIDR.
- Untuk Exadata X9M, alamat IP 100.106.0.0/16 dan 100.107.0.0/16 dicadangkan untuk interkoneksi cluster oleh otomatisasi OCI, jadi Anda tidak dapat melakukan hal berikut:
  - Tetapkan rentang ini ke klien atau rentang CIDR cadangan dari jaringan ODB.
  - Gunakan rentang ini untuk CIDR VPC yang digunakan untuk terhubung ke jaringan ODB.
- Rentang CIDR berikut dicadangkan untuk Oracle Cloud Infrastructure dan tidak dapat digunakan untuk jaringan ODB:
  - Rentang cadangan Oracle Cloud CIDR 169.254.0.0/16
  - Kelas Cadangan D 224.0.0.0 — 239.255.255.255
  - Kelas Cadangan E 240.0.0.0 — 255.255.255.255
- Anda tidak dapat tumpang tindih dengan rentang CIDR alamat IP untuk klien dan subnet cadangan.

- Anda tidak dapat tumpang tindih dengan rentang CIDR alamat IP yang dialokasikan untuk klien dan subnet cadangan dengan rentang CIDR VPC yang digunakan untuk terhubung ke jaringan ODB.
- Anda tidak dapat menyediakan VMs dalam cluster VM ke jaringan ODB yang berbeda. Jaringan adalah properti dari cluster VM, yang berarti Anda hanya dapat menyediakan di cluster VM ke VMs dalam jaringan ODB yang sama.

Persyaratan CIDR subnet klien untuk jaringan ODB

Dalam tabel berikut, Anda dapat menemukan jumlah alamat IP yang dikonsumsi oleh layanan dan infrastruktur untuk CIDR subnet klien. Ukuran CIDR minimum untuk subnet klien adalah /27, dan ukuran maksimum adalah /16.

Jumlah alamat IP	Dikonsumsi oleh	Catatan
6	Oracle Database@AWS	Alamat IP ini dicadangkan terlepas dari berapa banyak cluster VM yang Anda sediakan di jaringan ODB. Oracle Database@AWS mengkonsumsi yang berikut ini: • 3 alamat IP disediakan untuk sumber daya jaringan ODB di AWS • 3 alamat IP disediakan untuk layanan jaringan OCI
3	Setiap cluster VM	Alamat IP ini dicadangkan untuk Nama Akses Klien Tunggal (SCANs) terlepas dari berapa banyak VMs yang ada di setiap cluster VM.
4	Setiap VM	Alamat IP ini hanya bergantung VMs pada jumlah infrastru ktur.

Backup persyaratan CIDR subnet untuk jaringan ODB

Dalam tabel berikut, Anda dapat menemukan jumlah alamat IP yang dikonsumsi oleh layanan dan infrastruktur untuk subnet cadangan CIDR. Ukuran CIDR minimum untuk subnet cadangan adalah /28, dan ukuran maksimum adalah /16.

Jumlah alamat IP	Dikonsumsi oleh	Catatan
3	Oracle Database@AWS	Alamat IP ini dicadangkan terlepas dari berapa banyak cluster VM yang Anda sediakan di jaringan ODB. Oracle Database@AWS mengkonsumsi yang berikut ini: • 2 alamat IP di awal rentang CIDR • 1 alamat IP di akhir rentang CIDR
3	Setiap VM	Alamat IP ini hanya bergantung VMs pada jumlah infrastru ktur.

Skenario konsumsi IP untuk jaringan ODB

Dalam tabel berikut, Anda dapat melihat alamat IP yang dikonsumsi dalam jaringan ODB untuk konfigurasi yang berbeda dari cluster VM. Sedangkan /28 adalah rentang CIDR minimum teknis untuk subnet klien CIDR untuk menyebarkan 1 cluster VM dengan 2 VMs, kami sarankan Anda menggunakan setidaknya rentang CIDR /27. Dalam hal ini, rentang IP tidak sepenuhnya dikonsumsi oleh cluster VM dan memungkinkan alokasi alamat IP tambahan.

Konfigurasi	Klien IPs dikonsumsi	IPs Minimum klien	Backup IPs dikonsumsi	Backup IPs minimum
1 cluster VM dengan 2 VMs	17 (6 layanan+3 cluster +4* 2)	32 (/27 rentang CIDR)	9 (3 layanan+3* 2)	16 (/28 rentang CIDR)
1 cluster VM dengan 3 VMs	21 (6 layanan+3 cluster +4* 3)	32 (/27 rentang CIDR)	12 (3 layanan+3* 3)	16 (/28 rentang CIDR)
1 cluster VM dengan 4 VMs	25 (6 layanan+3 cluster +4* 4)	32 (/27 rentang CIDR)	15 (3 layanan+3* 4)	16 (/28 rentang CIDR)
1 cluster VM dengan 8 VMs	41 (6 layanan+3 cluster +4* 8)	64 (/26 rentang CIDR)	27 (3 layanan+3* 8)	32 (/27 rentang CIDR)

Tabel berikut menunjukkan berapa banyak contoh dari setiap konfigurasi yang mungkin diberikan rentang CIDR klien tertentu. Misalnya, 1 cluster VM dengan 4 VMs mengkonsumsi 24 alamat IP di subnet klien. Jika rentang CIDR adalah /25, 128 alamat IP tersedia. Dengan demikian, Anda dapat menyediakan 5 cluster VM di subnet.

Konfigurasi cluster VM	Angka dengan/27 (32 IPs)	Angka dengan/26 (64 IPs)	Nomor dengan/25 (128 IPs)	Nomor dengan/24 (256 IPs)	Nomor kapan /23 (512 IPs)	Nomor kapan /22 (IPs1024)
1 cluster VM dengan 2 VMs (16 IPs)	1	3	7	15	30	60
1 cluster VM dengan 3 VMs (20 IPs)	1	3	6	12	24	48
1 cluster VM dengan 4 VMs (24 IPs)	1	2	5	10	20	40
2 cluster VM dengan VMs masing-masing 2 (27) IPs	1	2	4	9	18	36
2 cluster VM dengan VMs masing-masing 3 (35) IPs	0	1	3	7	14	28
2 cluster VM dengan VMs masing-masing 4 (43) IPs	0	1	2	5	11	23

Langkah 1: Buat jaringan ODB di Oracle Database@AWS

Jaringan ODB adalah jaringan terisolasi pribadi yang menampung infrastruktur OCI di Availability Zone (AZ). Jaringan ODB dan infrastruktur Oracle Exadata adalah prasyarat untuk penyediaan cluster VM dan membuat database Exadata. Anda dapat membuat jaringan ODB dan infrastruktur

Oracle Exadata dalam urutan apa pun. Untuk informasi selengkapnya, lihat Jaringan ODB dan ODB mengintip.

Tugas ini mengasumsikan bahwa Anda telah membacaMerencanakan ruang alamat IP di Oracle Database@AWS. Untuk memodifikasi atau menghapus jaringan ODB nanti, lihatMengelola Database Oracle@AWS.

Untuk membuat jaringan ODB

1. Masuk ke Konsol Manajemen AWS dan buka Oracle Database@AWS konsol di https://console.aws.amazon.com/odb/.
2. Pilih AWS Wilayah Anda di kanan atas. Untuk informasi selengkapnya, lihat Wilayah yang Didukung untuk Oracle Database@AWS.
3. Dari panel kiri, pilih jaringan ODB.
4. Pilih Buat jaringan ODB.
5. Untuk nama jaringan ODB, masukkan nama jaringan. Nama harus 1-255 karakter dan dimulai dengan karakter alfabet atau garis bawah. Itu tidak bisa mengandung tanda hubung berturut-turut.
6. Untuk Availability Zone, pilih nama AZ. Untuk didukung AZs, lihatWilayah yang Didukung untuk Oracle Database@AWS.
7. Untuk CIDR subnet Klien, tentukan rentang CIDR untuk koneksi klien. Untuk informasi selengkapnya, lihat Persyaratan CIDR subnet klien untuk jaringan ODB.
8. Untuk CIDR subnet Backup, tentukan rentang CIDR untuk koneksi cadangan. Untuk mengisolasi lalu lintas cadangan dan meningkatkan ketahanan, kami menyarankan Anda untuk tidak tumpang tindih dengan CIDR cadangan dan CIDR klien. Untuk informasi selengkapnya, lihat Backup persyaratan CIDR subnet untuk jaringan ODB.
9. Untuk konfigurasi DNS, pilih salah satu opsi berikut:

   Default

   Untuk awalan nama Domain, masukkan nama yang akan digunakan sebagai awalan domain Anda. Nama domain ditetapkan sebagai oraclevcn.com. Misalnya, jika Anda masuk**`myhost`**, nama domain yang sepenuhnya memenuhi syarat adalah myhost.oraclevcn.com.

   Nama domain kustom

   Untuk nama Domain, masukkan nama domain lengkap. Misalnya, Anda dapat memasukkan myhost.myodb.com.

10. (Opsional) Untuk integrasi Layanan, pilih layanan untuk diintegrasikan dengan jaringan Anda menggunakan VPC Lattice. Oracle Database @AWS terintegrasi dengan berbagai Layanan AWS untuk menyediakan fungsionalitas dan opsi konektivitas yang disempurnakan untuk database Oracle Anda. Pilih salah satu dari integrasi berikut:

    Amazon S3

    Aktifkan akses jaringan ODB langsung ke Amazon S3. Database Anda dapat mengakses S3 untuk impor/ekspor data atau cadangan khusus. Anda dapat memasukkan kebijakan JSON. Untuk informasi selengkapnya, lihat Pencadangan yang dikelola pengguna ke Amazon S3 di Oracle Database @AWS.

    Nol-ETL

    Aktifkan analisis real-time dan pembelajaran mesin pada data transaksional menggunakan Amazon Redshift. Untuk informasi selengkapnya, lihat Database Oracle@ Integrasi AWS nol-ETL dengan Amazon Redshift.

    > **Note**
    >
    > Saat Anda membuat jaringan ODB, Oracle Database@AWS secara otomatis mengkonfigurasi akses jaringan untuk backup terkelola Oracle ke Amazon S3. Anda tidak dapat mengaktifkan atau menonaktifkan integrasi ini. Untuk informasi selengkapnya, lihat AWS integrasi layanan.

11. (Opsional) Untuk Tag, masukkan hingga 50 tag untuk jaringan. Tag adalah pasangan kunci-nilai yang dapat Anda gunakan untuk mengatur dan melacak sumber daya Anda.
12. Pilih Buat jaringan ODB.

Setelah Anda membuat jaringan ODB, Anda dapat mengintip ke VPC. ODB peering adalah koneksi jaringan buatan pengguna yang memungkinkan lalu lintas dirutekan secara pribadi antara VPC Amazon dan jaringan ODB. Setelah mengintip, EC2 instance Amazon dalam VPC dapat berkomunikasi dengan sumber daya di jaringan ODB seolah-olah mereka berada dalam jaringan yang sama. Untuk informasi selengkapnya, lihat Mengonfigurasi ODB mengintip ke VPC Amazon di Oracle Database @AWS.

Langkah 2: Buat infrastruktur Oracle Exadata di Oracle Database@AWS

Infrastruktur Oracle Exadata adalah arsitektur dasar server database, server penyimpanan, dan jaringan yang menjalankan database Oracle Exadata. Pilih Exadata X9M atau X11M sebagai model sistem. Anda kemudian dapat membuat cluster VM pada infrastruktur Exadata menggunakan konsol. AWS

Anda dapat membuat infrastruktur Oracle Exadata dan jaringan ODB dalam urutan apa pun. Anda tidak perlu menentukan informasi jaringan saat membuat infrastruktur.

Anda tidak dapat memodifikasi infrastruktur Oracle Exadata setelah Anda membuatnya. Untuk menghapus infrastruktur Exadata, lihat. Menghapus infrastruktur Oracle Exadata di Oracle Database@AWS

Untuk membuat infrastruktur Exadata

1. Masuk ke Konsol Manajemen AWS dan buka Oracle Database@AWS konsol di https://console.aws.amazon.com/odb/.
2. Dari panel kiri, pilih infrastruktur Exadata.
3. Pilih Buat infrastruktur Exadata.
4. Untuk nama infrastruktur Exadata, masukkan nama. Nama harus 1-255 karakter dan dimulai dengan karakter alfabet atau garis bawah. Itu tidak bisa mengandung tanda hubung berturut-turut.
5. Untuk Availability Zone, pilih salah satu yang didukung AZs. Lalu pilih Selanjutnya.
6. Untuk model sistem Exadata, pilih Exadata.X9M atau Exadata.X11M. Untuk Exadata.X11M, pilih juga jenis server berikut:
   - Untuk jenis server Database, pilih jenis model server database infrastruktur Exadata Anda. Saat ini, satu-satunya pilihan adalah X11M.
   - Untuk jenis server Storage, pilih jenis model server penyimpanan infrastruktur Exadata Anda. Saat ini, satu-satunya pilihan adalah X11M-HC.
7. Untuk server Database, biarkan default 2 atau pindahkan slider untuk memilih hingga 32 server. Untuk menentukan lebih dari 2, minta kenaikan batas dari OCI.

   Setiap server database Exadata X9M mendukung 126. OCPUs Setiap server database Exadata X11M mendukung 760. ECPUs Jumlah komputasi total berubah saat Anda mengubah jumlah

server. Untuk informasi selengkapnya tentang OCPUs dan ECPUs, lihat Compute Models in Autonomous Database dalam dokumentasi Oracle.

8. Untuk server Storage, biarkan default 3 atau pindahkan slider untuk memilih hingga 64 server. Untuk menentukan lebih dari 3, minta kenaikan batas dari OCI. Setiap server penyimpanan X9M menyediakan 64 TB. Setiap server penyimpanan X11m menyediakan 80 TB. Total TB penyimpanan berubah saat Anda mengubah jumlah server. Lalu pilih Selanjutnya.
9. Untuk jendela Pemeliharaan, konfigurasikan kapan pemeliharaan sistem dapat terjadi:

   a. Untuk preferensi Penjadwalan, pilih salah satu opsi berikut:

      - Jadwal yang dikelola Oracle - Oracle menentukan waktu optimal untuk kegiatan pemeliharaan.
      - Jadwal yang dikelola pelanggan - Anda menentukan kapan aktivitas pemeliharaan dapat terjadi.

   b. Untuk mode Patching, pilih salah satu opsi berikut:

      - Bergulir - Pembaruan diterapkan ke satu node pada satu waktu, memungkinkan database tetap tersedia selama penambalan.
      - Non-rolling - Pembaruan diterapkan ke semua node secara bersamaan, yang mungkin memerlukan waktu henti.

   c. Jika Anda memilih Jadwal yang dikelola Pelanggan, konfigurasikan setelan tambahan berikut:

      - Untuk bulan Pemeliharaan, pilih bulan saat pemeliharaan dapat dilakukan.
      - Untuk Minggu dalam sebulan, pilih minggu mana pemeliharaan bulan dapat dilakukan (Pertama, Kedua, Ketiga, Keempat, atau Terakhir).
      - Untuk Hari dalam seminggu, pilih hari ketika pemeliharaan dapat dilakukan (Senin sampai Minggu).
      - Untuk Jam mulai, pilih jam ketika jendela pemeliharaan dimulai. Waktunya di UTC.
      - Untuk waktu tunggu Pemberitahuan, pilih berapa hari sebelumnya Anda ingin diberi tahu tentang pemeliharaan yang akan datang.

> **Note**
>
> Oracle Cloud Infrastructure melakukan pemeliharaan sistem selama jendela ini. Selama pemeliharaan, infrastruktur Exadata Anda tetap tersedia, tetapi Anda mungkin mengalami periode singkat latensi yang lebih tinggi.

10. (Opsional) Untuk kontak pemberitahuan pemeliharaan OCI, masukkan hingga 10 alamat email. AWS meneruskan alamat email ini ke OCI. Ketika pembaruan terjadi, OCI mengirimkan pemberitahuan ke alamat yang terdaftar.
11. (Opsional) Untuk Tag, masukkan hingga 50 tag untuk infrastruktur. Tag adalah pasangan kunci-nilai yang dapat Anda gunakan untuk mengatur dan melacak sumber daya Anda.
12. Pilih Berikutnya dan tinjau pengaturan infrastruktur Anda.
13. Pilih Buat infrastruktur Exadata.

Langkah 3: Buat cluster Exadata VM atau cluster VM Autonomous di Oracle Database@AWS

Cluster Exadata VM adalah satu set VMs di mana Anda dapat membuat database Oracle Exadata. Anda membuat cluster VM pada infrastruktur Exadata. Anda dapat menyebarkan beberapa cluster VM dengan infrastruktur Oracle Exadata yang berbeda di jaringan ODB yang sama. Anda memiliki kontrol administratif penuh atas database yang Anda buat di klaster Exadata VM.

Cluster VM Autonomous adalah kumpulan sumber daya komputasi dan penyimpanan Oracle Exadata yang telah dialokasikan sebelumnya, yang divirtualisasikan pada tingkat VM, yang menjalankan Autonomous Databases (ADB). Tidak seperti database yang dikelola pengguna yang Anda buat di cluster Exadata VM, database Autonomous adalah self-tuning, self-patching, dan dikelola oleh Oracle daripada administrator database.

Pertimbangkan batasan berikut saat Anda membuat cluster VM:

- Anda dapat menyebarkan cluster VM hanya ke AZ tempat Anda membuat jaringan ODB dan infrastruktur Oracle Exadata.
- Jika Anda tidak berbagi cluster VM di seluruh akun, itu harus Akun AWS sama dengan infrastruktur Oracle Exadata. Jika Anda menggunakan AWS RAM untuk berbagi jaringan ODB dan infrastruktur

Oracle Exadata dari satu AWS akun dengan akun tepercaya, akun tepercaya dapat membuat cluster VM di akunnya sendiri.

- Anda hanya dapat menerapkan cluster VM di jaringan ODB Anda. Tidak ada sumber daya lain yang diizinkan.
- Anda tidak dapat mengubah alokasi penyimpanan setelah membuat cluster VM.

> **Important**
>
> Proses pembuatan dapat memakan waktu lebih dari 6 jam, tergantung pada ukuran cluster VM.

Exadata VM cluster

Untuk membuat cluster Exadata VM

1. Masuk ke Konsol Manajemen AWS dan buka Oracle Database@AWS konsol di https://console.aws.amazon.com/odb/.
2. Dari panel kiri, pilih klaster Exadata VM.
3. Pilih Buat cluster VM.
4. Untuk nama cluster VM, masukkan nama. Nama harus 1-255 karakter dan dimulai dengan karakter alfabet atau garis bawah. Itu tidak bisa mengandung tanda hubung berturut-turut.
5. (Opsional) Untuk nama cluster Infrastruktur Grid, masukkan versi infrastruktur Grid untuk cluster VM Anda yang cocok dengan versi Oracle Database yang Anda gunakan. Nama harus 1-11 karakter dan tidak dapat berisi tanda hubung.
6. Untuk zona waktu, masukkan zona waktu.
7. Untuk opsi Lisensi, pilih Bawa Lisensi Anda Sendiri (BYOL) atau Termasuk Lisensi, lalu pilih Berikutnya. Lisensi ini adalah lisensi OCI yang disediakan oleh Oracle, bukan lisensi yang disediakan oleh. AWS
8. Konfigurasikan pengaturan infrastruktur Exadata sebagai berikut:

    a. Untuk Infrastruktur, pilih yang berikut ini:

    - Untuk nama infrastruktur Exadata, pilih infrastruktur yang akan digunakan untuk klaster VM ini.
    - Untuk versi Infrastruktur Grid, pilih versi yang akan digunakan untuk cluster VM ini.

- Untuk versi gambar Exadata, pilih versi yang akan digunakan untuk cluster VM ini. Kami menyarankan Anda memilih versi yang ditampilkan, yang merupakan versi tertinggi yang tersedia.

b. Untuk server Database, pilih satu atau beberapa server database untuk meng-host cluster VM Anda.

c. Untuk Konfigurasi, lakukan hal berikut:

- Pilih jumlah inti CPU, Memori, dan penyimpanan lokal untuk setiap VM, atau terima defaultnya.
- Pilih jumlah total penyimpanan Exadata untuk cluster VM, atau terima default.

d. (Opsional) Untuk alokasi Penyimpanan, pilih salah satu opsi berikut:

- Aktifkan alokasi penyimpanan untuk snapshot Exadata sparse
- Aktifkan alokasi penyimpanan untuk backup lokal

Alokasi penyimpanan yang dapat digunakan berubah saat Anda memilih opsi. Anda tidak dapat mengubah alokasi penyimpanan ini nanti. Tinjau pilihan Anda, lalu pilih Berikutnya.

9. Konfigurasikan konektivitas sebagai berikut:

a. Untuk jaringan ODB, pilih jaringan ODB yang ada.

b. Untuk awalan nama Host, masukkan awalan untuk cluster VM. Pastikan untuk tidak menyertakan nama domain. Awalan membentuk bagian pertama dari nama host cluster Oracle Exadata VM.

> **Note**
>
> Nama domain Host ditetapkan sebagai oraclevcn.com.

c. Untuk port pendengar SCAN (TCP/IP), masukkan nomor port yang untuk akses TCP ke pendengar nama akses klien tunggal (SCAN). Port default adalah 1521. Atau Anda dapat memasukkan port SCAN khusus di kisaran 1024—8999, tidak termasuk nomor port berikut: 2484, 6100, 6200, 7060, 7070, 7085, dan 7879. Lalu pilih Selanjutnya.

d. Untuk pasangan kunci SSH, masukkan bagian kunci publik dari satu atau lebih pasangan kunci yang digunakan untuk akses SSH ke cluster VM. Lalu pilih Selanjutnya.

10. (Opsional) Pilih diagnostik dan tag sebagai berikut:

a. Pilih apakah akan mengaktifkan pengumpulan diagnostik untuk peristiwa Diagnostik, Monitor Kesehatan, dan log Insiden dan koleksi jejak. Oracle dapat menggunakan informasi diagnostik ini untuk mengidentifikasi, melacak, dan menyelesaikan masalah.

b. Untuk Tag, masukkan hingga 50 tag untuk cluster VM. Tag adalah pasangan kunci-nilai yang dapat Anda gunakan untuk mengatur dan melacak sumber daya Anda. Lalu pilih Selanjutnya.

11. Meninjau pengaturan Anda. Kemudian pilih Buat cluster VM.

Autonomous VM cluster

Untuk membuat cluster VM Autonomous

1. Masuk ke Konsol Manajemen AWS dan buka Oracle Database@AWS konsol di https://console.aws.amazon.com/odb/.
2. Dari panel kiri, pilih cluster VM otonom.
3. Pilih Buat cluster VM Otonom.
4. Untuk nama cluster VM, masukkan nama. Nama harus 1-255 karakter dan dimulai dengan karakter alfabet atau garis bawah. Itu tidak bisa mengandung tanda hubung berturut-turut.
5. Untuk zona waktu, masukkan zona waktu.
6. Untuk opsi Lisensi, pilih Bawa Lisensi Anda Sendiri (BYOL) atau Termasuk Lisensi, lalu pilih Berikutnya. Lisensi ini adalah lisensi OCI yang disediakan oleh Oracle, bukan lisensi yang disediakan oleh. AWS
7. Konfigurasikan pengaturan infrastruktur Exadata sebagai berikut:

   a. Untuk nama infrastruktur Exadata, pilih infrastruktur yang akan digunakan untuk cluster VM Autonomous ini.

   b. Untuk server Database, pilih satu atau beberapa server database untuk meng-host cluster VM Autonomous Anda.

   c. Untuk Konfigurasi, lakukan hal berikut:

      - Pilih jumlah inti ECPU per VM, memori Database per CPU, penyimpanan Database, dan Jumlah maksimum Autonomous Container Database atau terima defaultnya.
      - Pilih jumlah total penyimpanan Exadata untuk cluster VM Autonomous, atau terima default.

8. Konfigurasikan konektivitas sebagai berikut:

    a. Untuk jaringan ODB, pilih jaringan ODB yang ada.

    b. Untuk port pendengar SCAN (TCP/IP), masukkan nomor port untuk Port (non-TLS). Port default adalah 1521. Atau Anda dapat memasukkan Port (TLS) di kisaran 1024—8999, tidak termasuk nomor port berikut: 2484, 6100, 6200, 7060, 7070, 7085, dan 7879. Lalu pilih Selanjutnya.

    Pilih Aktifkan otentikasi TLS (mTLS) bersama untuk memungkinkan otentikasi TLS timbal balik.

9. (Opsional) Pilih diagnostik dan tag sebagai berikut:

    a. Pilih apakah akan menjadwalkan konfigurasi modifikasi ke jadwal yang dikelola Oracle atau jadwal yang dikelola Pelanggan. Jika Anda memilih jadwal yang dikelola Pelanggan, tetapkan bulan Pemeliharaan, Minggu dalam sebulan, Hari dalam seminggu, dan Jam mulai (UTC).

    b. Untuk Tag, masukkan hingga 50 tag untuk cluster VM Autonomous. Tag adalah pasangan kunci-nilai yang dapat Anda gunakan untuk mengatur dan melacak sumber daya Anda. Lalu pilih Selanjutnya.

10. Meninjau pengaturan Anda. Kemudian pilih Create Autonomous VM cluster.

Langkah 4: Buat database Oracle Exadata di Oracle Cloud Infrastructure

Di Oracle Database@AWS, Anda dapat membuat dan mengelola sumber daya berikut menggunakan AWS konsol, CLI, atau: APIs

- Jaringan ODB
- Infrastruktur Oracle Exadata
- Cluster Exadata VM dan kluster VM Otonom
- Koneksi mengintip ODB

Untuk membuat dan mengelola database Oracle Exadata pada infrastruktur yang Anda buat, Anda harus menggunakan konsol Oracle Cloud Infrastructure daripada dasbor. Oracle Database@AWS Anda dapat membuat database Exadata yang dikelola pengguna pada cluster Exadata VM dan

Autonomous Database pada cluster Autonomous Exadata VM. Untuk informasi tentang membuat database Oracle di OCI, lihat Exadata Database dalam dokumentasi Oracle Cloud Infrastructure.

Untuk membuat database Oracle Exadata

1. Masuk ke Konsol Manajemen AWS dan buka Oracle Database@AWS konsol di https://console.aws.amazon.com/odb/.
2. Dari panel kiri, pilih klaster Exadata VM atau cluster VM otonom.
3. Pilih cluster VM untuk melihat halaman detail.
4. Pilih Kelola di OCI untuk diarahkan ke konsol Oracle Cloud Infrastructure.
5. Buat database Exadata yang dikelola pengguna atau Database Otonom di OCI.

Mengonfigurasi ODB mengintip ke VPC Amazon di Oracle Database @AWS

ODB peering adalah koneksi jaringan buatan pengguna yang memungkinkan lalu lintas dirutekan secara pribadi antara VPC Amazon dan jaringan ODB. Ada one-to-one hubungan antara VPC dan jaringan ODB. Setelah Anda membuat koneksi peering menggunakan konsol, CLI, atau API, pastikan untuk memperbarui tabel rute VPC Anda dan mengonfigurasi resolusi DNS. Untuk gambaran konseptual tentang peering ODB, lihat. ODB mengintip

Membuat koneksi peering ODB di Oracle Database@AWS

Dengan koneksi peering ODB, Anda dapat membangun konektivitas jaringan pribadi antara infrastruktur Oracle Exadata Anda dan aplikasi yang berjalan di Amazon Anda. VPCs Setiap koneksi peering ODB adalah sumber daya terpisah yang dapat Anda buat, lihat, dan hapus secara independen dari jaringan ODB.

Saat membuat koneksi peering ODB, Anda dapat menentukan rentang CIDR jaringan rekan. Teknik ini membatasi akses jaringan ke subnet yang diperlukan, mengurangi target potensial untuk serangan, dan memungkinkan segmentasi jaringan yang lebih terperinci untuk persyaratan kepatuhan.

Anda dapat membuat jenis koneksi peering ODB berikut:

Pengintip ODB akun yang sama

Anda dapat membuat koneksi peering ODB antara jaringan ODB dan VPC Amazon di akun yang sama. AWS

Peering ODB lintas akun

Anda dapat membuat koneksi peering ODB antara jaringan ODB dalam satu akun dan VPC Amazon di akun yang berbeda, setelah jaringan ODB dibagikan menggunakan. AWS RAM Akun pemilik VPC dapat mengelola rentang CIDR yang ditentukan dalam koneksi peering tanpa juga memiliki jaringan ODB.

Ada hubungan 1:1 antara VPC dan jaringan ODB. Anda tidak dapat membuat koneksi peering ODB antara VPC dan beberapa jaringan ODB atau antara jaringan ODB dan beberapa. VPCs

Konsol

1. Masuk ke Konsol Manajemen AWS dan buka Oracle Database@AWS konsol di https://console.aws.amazon.com/odb/.
2. Di panel navigasi, pilih koneksi peering ODB.
3. Pilih Buat koneksi peering ODB.
4. (Opsional) Untuk nama peering ODB, masukkan nama unik untuk koneksi Anda.
5. Untuk jaringan ODB, pilih jaringan ODB ke peer.
6. Untuk jaringan Peer, pilih Amazon VPC untuk mengintip dengan jaringan ODB Anda.
7. (Opsional) Untuk jaringan Peer CIDRs, tentukan blok CIDR tambahan dari VPC rekan yang dapat mengakses jaringan ODB. Jika Anda tidak menentukan CIDRs, semua CIDRs dari VPC rekan diizinkan akses.
8. (Opsional) Di Tag, tambahkan pasangan kunci dan nilai.
9. Pilih Buat koneksi peering ODB.

Setelah membuat koneksi peering ODB, konfigurasikan tabel rute VPC Amazon Anda untuk merutekan lalu lintas ke jaringan ODB yang diintip. Untuk informasi selengkapnya, lihat Mengkonfigurasi tabel rute VPC untuk mengintip ODB. Perhatikan bahwa Oracle Database@AWS secara otomatis mengkonfigurasi tabel rute jaringan ODB.

AWS CLI

Untuk membuat koneksi peering ODB, gunakan perintah. `create-odb-peering-connection`

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

Untuk membatasi akses ke jaringan ODB ke rentang CIDR tertentu, gunakan parameter. `--peer-network-cidrs-to-be-added` Jika Anda tidak menentukan rentang CIDR, semua rentang memiliki akses.

```
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"
```

Untuk membuat daftar koneksi peering ODB Anda, gunakan perintah. `list-odb-peering-connections`

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

Untuk mendapatkan detail tentang koneksi peering ODB tertentu, gunakan perintah. `get-odb-peering-connection`

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

Memperbarui koneksi peering ODB

Anda dapat memperbarui koneksi peering ODB yang ada untuk menambah atau menghapus jaringan rekan. CIDRs Anda mengontrol subnet mana di VPC rekan yang memiliki akses ke jaringan ODB Anda.

Konsol

1. Masuk ke Konsol Manajemen AWS dan buka Oracle Database@AWS konsol di https://console.aws.amazon.com/odb/.
2. Di panel navigasi, pilih koneksi peering ODB.
3. Pilih koneksi peering ODB yang ingin Anda perbarui.
4. Pilih Tindakan, lalu pilih Perbarui koneksi peering.
5. Di CIDRs bagian jaringan Peer, tambahkan atau hapus blok CIDR sesuai kebutuhan:
   - Untuk menambahkan CIDRs, pilih Tambahkan CIDR dan masukkan blok CIDR.
   - Untuk menghapus CIDRs, pilih X di sebelah blok CIDR yang ingin Anda hapus.
6. Pilih Perbarui koneksi peering.

AWS CLI

Untuk menambahkan jaringan peer CIDRs ke koneksi peering ODB, tentukan parameter `--peer-network-cidrs-to-be-added` dalam perintah. `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"
```

Untuk menghapus jaringan peer CIDRs dari koneksi peering ODB, tentukan parameter `--peer-network-cidrs-to-be-removed` dalam perintah. `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"
```

Mengkonfigurasi tabel rute VPC untuk mengintip ODB

Tabel rute berisi seperangkat aturan, yang disebut rute, yang menentukan ke mana lalu lintas jaringan dari subnet atau gateway Anda diarahkan. CIDR tujuan dalam tabel rute adalah rentang alamat IP tempat Anda ingin lalu lintas pergi. Jika Anda menentukan VPC untuk ODB yang mengintip ke jaringan ODB Anda, perbarui tabel rute VPC Anda dengan rentang IP tujuan di jaringan ODB Anda. Untuk informasi lebih lanjut tentang peering ODB, lihat. ODB mengintip

Untuk memperbarui tabel rute, gunakan AWS CLI `ec2 create-route` perintah. Contoh berikut memperbarui tabel rute Amazon VPC. Untuk informasi selengkapnya, lihat Mengkonfigurasi tabel rute VPC untuk mengintip ODB.

```
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
```

Tabel rute jaringan ODB diperbarui secara otomatis dengan VPC CIDRs. Untuk mengizinkan akses ke jaringan ODB hanya untuk subnet tertentu CIDRs daripada semua CIDRs di VPC, Anda dapat menentukan jaringan rekan CIDRs saat membuat koneksi peering ODB atau memperbarui koneksi peering ODB yang ada untuk menambah atau menghapus rentang CIDR yang dipeered. Untuk informasi selengkapnya, lihat Membuat koneksi peering ODB di Oracle Database@AWS dan Memperbarui koneksi peering ODB.

Untuk informasi selengkapnya tentang tabel rute VPC, lihat Tabel rute subnet di Panduan Pengguna Amazon Virtual Private Cloud dan ec2 create-route di Referensi Perintah.AWS CLI

Mengkonfigurasi DNS untuk Oracle Database@AWS

Amazon Route 53 adalah layanan web Sistem Nama Domain (DNS) yang sangat tersedia dan dapat diskalakan yang dapat Anda gunakan untuk perutean DNS. Saat Anda membuat koneksi peering ODB antara jaringan ODB dan VPC, Anda memerlukan mekanisme untuk menyelesaikan kueri DNS untuk sumber daya jaringan ODB dari dalam VPC. Anda dapat menggunakan Amazon Route 53 untuk mengonfigurasi sumber daya berikut:

- Titik akhir keluar

  Titik akhir diperlukan untuk mengirim kueri DNS ke jaringan ODB.
- Aturan resolver

  Aturan ini menentukan nama domain dari kueri DNS yang diteruskan oleh Resolver Route 53 ke DNS untuk jaringan ODB.

Bagaimana DNS bekerja di Oracle Database@AWS

Oracle Database@AWS mengelola konfigurasi Domain Name System (DNS) untuk jaringan ODB secara otomatis. Untuk nama domain, Anda dapat menentukan awalan kustom untuk nama domain default `oraclevcn.com` atau nama domain yang sepenuhnya kustom. Untuk informasi selengkapnya, lihat Langkah 1: Buat jaringan ODB di Oracle Database@AWS.

Ketika Oracle Database@AWS menyediakan jaringan ODB, itu menciptakan sumber daya berikut:

- Jaringan cloud virtual (VCN) Oracle Cloud Infrastructure (OCI) dengan blok CIDR yang sama dengan jaringan ODB

  VCN ini berada dalam penyewaan OCI terkait pelanggan. Ada pemetaan 1:1 antara jaringan ODB dan OCI VCN. Setiap jaringan ODB dikaitkan dengan OCI VCN.
- Penyelesai DNS pribadi dalam OCI VCN

  DNS resolver ini menangani query DNS dalam OCI VCN. Otomatisasi OCI membuat catatan untuk cluster VM. Pemindaian menggunakan nama domain yang `*.oraclevcn.com` sepenuhnya memenuhi syarat (FQDN).
- Titik akhir mendengarkan DNS dalam OCI VCN untuk penyelesai DNS pribadi

Anda dapat menemukan titik akhir mendengarkan DNS di halaman detail jaringan ODB di konsol. Oracle Database@AWS

Mengkonfigurasi titik akhir keluar dalam jaringan ODB di Oracle Database@AWS

Titik akhir keluar memungkinkan kueri DNS dikirim dari VPC Anda ke jaringan atau alamat IP. Endpoint menentukan alamat IP dari mana query berasal. Untuk meneruskan kueri DNS dari VPC Anda ke jaringan ODB Anda, buat titik akhir keluar menggunakan konsol Route 53. Untuk informasi selengkapnya, lihat Meneruskan kueri DNS keluar ke jaringan Anda.

Untuk mengkonfigurasi titik akhir keluar dalam jaringan ODB

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di https://console.aws.amazon.com/route53/.
2. Dari panel kiri, pilih Titik akhir Outbound.
3. Pada bilah navigasi, pilih Wilayah untuk VPC tempat Anda ingin membuat titik akhir keluar.
4. Pilih Buat titik akhir keluar.
5. Lengkapi bagian Pengaturan umum untuk titik akhir keluar sebagai berikut:
   a. Pilih grup Keamanan yang memungkinkan konektivitas TCP dan UDP keluar ke yang berikut:
      - Alamat IP yang digunakan resolver untuk kueri DNS di jaringan ODB Anda
      - Port yang digunakan resolver untuk kueri DNS di jaringan ODB Anda
   b. Untuk Jenis Titik Akhir, pilih IPv4.
   c. Untuk Protokol untuk titik akhir ini, pilih Do53.
6. Di alamat IP, berikan informasi berikut:
   - Entah menentukan alamat IP atau biarkan Route 53 Resolver memilih alamat IP untuk Anda dari alamat yang tersedia di subnet. Pilih minimal 2 hingga maksimal 6 alamat IP untuk kueri DNS. Kami menyarankan Anda memilih alamat IP di setidaknya dua Availability Zone yang berbeda.
   - Untuk Subnet, pilih subnet yang memiliki berikut ini:
     - Rute tabel yang menyertakan rute ke alamat IP pendengar DNS di jaringan ODB

- Daftar kontrol akses jaringan (ACLs) yang memungkinkan lalu lintas UDP dan TCP ke alamat IP dan port yang digunakan resolver untuk kueri DNS di jaringan ODB
- Jaringan ACLs yang memungkinkan lalu lintas dari resolver pada rentang port tujuan 1024-65535

7. (Opsional) Untuk Tag, tentukan tag untuk titik akhir.
8. Pilih Kirim.

Mengkonfigurasi aturan resolver di Oracle Database@AWS

Aturan resolver adalah seperangkat kriteria yang menentukan cara merutekan kueri DNS. Baik menggunakan kembali atau membuat aturan yang menentukan nama domain dari kueri DNS yang diteruskan oleh resolver ke DNS untuk jaringan ODB.

Menggunakan aturan resolver yang ada

Untuk menggunakan aturan resolver yang ada, tindakan Anda bergantung pada jenis aturan:

Aturan untuk domain yang sama di AWS Wilayah yang sama dengan VPC di wilayah Anda Akun AWS

Kaitkan aturan dengan VPC Anda alih-alih membuat aturan baru. Pilih aturan dari dasbor aturan dan kaitkan dengan aturan yang berlaku VPCs di AWS Wilayah.

Aturan untuk domain yang sama di Wilayah yang sama dengan VPC Anda tetapi di akun yang berbeda

Gunakan AWS Resource Access Manager untuk membagikan aturan dari akun jarak jauh ke akun Anda. Saat Anda membagikan aturan, Anda juga membagikan titik akhir keluar yang sesuai. Setelah Anda membagikan aturan dengan akun Anda, pilih aturan dari dasbor aturan dan kaitkan dengan VPCs di akun Anda. Untuk informasi selengkapnya, lihat Mengelola aturan penerusan.

Membuat aturan resolver baru

Jika Anda tidak dapat menggunakan kembali aturan resolver yang ada, buat aturan baru menggunakan konsol Amazon Route 53.

Untuk membuat aturan resolver baru

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di https://console.aws.amazon.com/route53/.
2. Dari panel kiri, pilih Aturan.
3. Pada bilah navigasi, pilih Wilayah untuk VPC tempat titik akhir keluar ada.
4. Pilih Buat aturan.
5. Lengkapi Aturan untuk bagian lalu lintas keluar sebagai berikut:
   a. Untuk jenis Aturan, pilih Aturan teruskan.
   b. Untuk nama Domain, tentukan nama domain lengkap dari jaringan ODB.
   c. Untuk VPCs itu gunakan aturan ini, kaitkan dengan VPC dari mana kueri DNS diteruskan ke jaringan ODB Anda.
   d. Untuk titik akhir Outbound, pilih titik akhir keluar yang Anda buat. Mengkonfigurasi titik akhir keluar dalam jaringan ODB di Oracle Database@AWS

   > **Note**
   >
   > VPC yang terkait dengan aturan ini tidak harus VPC yang sama tempat Anda membuat titik akhir keluar.

6. Lengkapi bagian Alamat IP Target sebagai berikut:
   a. Untuk alamat IP, tentukan alamat IP IP pendengar DNS di jaringan ODB Anda.
   b. Untuk Port, tentukan 53. Ini adalah port yang digunakan resolver untuk kueri DNS.

   > **Note**
   >
   > Route 53 Resolver meneruskan kueri DNS yang cocok dengan aturan ini dan berasal dari VPC yang terkait dengan aturan ini ke titik akhir keluar yang direferensikan. Kueri ini diteruskan ke alamat IP target yang Anda tentukan di alamat IP Target.

   c. Untuk protokol Transmisi, pilih Do53.
7. (Opsional) Untuk Tag, tentukan tag untuk aturan.
8. Pilih Kirim.

Menguji konfigurasi DNS Anda di Oracle Database@AWS

Setelah Anda membuat titik akhir keluar dan aturan resolver, uji untuk memastikan bahwa DNS menyelesaikan dengan benar. Menggunakan EC2 instans Amazon di VPC aplikasi Anda, lakukan resolusi DNS sebagai berikut:

Untuk Linux atau macOS

- Gunakan perintah formulir`dig` *`record-name record-type`*.

Untuk Windows

- Gunakan perintah formulir`nslookup -type=`*`record-name record-type`*.

Mengkonfigurasi Gateway Transit VPC Amazon untuk Oracle Database@AWS

Amazon VPC Transit Gateways adalah hub transit jaringan yang menghubungkan virtual private cloud () VPCs dan jaringan lokal. Setiap VPC dalam hub-and-spoke arsitektur dapat terhubung ke gateway transit untuk mendapatkan akses ke koneksi lain. VPCs AWS Transit Gateway mendukung lalu lintas untuk keduanya IPv4 dan IPv6.

Di Oracle Database@AWS, jaringan ODB mendukung koneksi peering ke hanya satu VPC. Jika Anda menghubungkan gateway transit ke VPC yang diintip ke jaringan ODB, Anda dapat menghubungkan beberapa VPCs ke gateway ini. Aplikasi yang berjalan di berbagai ini VPCs dapat mengakses cluster Exadata VM yang berjalan di jaringan ODB Anda.

Diagram berikut menunjukkan gateway transit yang terhubung ke dua VPCs dan satu jaringan lokal.

Pada diagram sebelumnya, satu VPC diintip ke jaringan ODB. Dalam konfigurasi ini, jaringan ODB dapat merutekan lalu lintas ke semua yang VPCs terpasang pada gateway transit. Tabel rute untuk setiap VPC mencakup rute lokal dan rute yang mengirim lalu lintas yang ditujukan untuk jaringan ODB ke gateway transit.

Di AWS Transit Gateway, Anda dikenakan biaya untuk jumlah koneksi yang Anda buat ke gateway transit per jam dan jumlah lalu lintas yang mengalir AWS Transit Gateway. Untuk informasi biaya, lihat AWS Transit Gateway harga.

Persyaratan

Pastikan Oracle Database@AWS lingkungan Anda memenuhi persyaratan berikut:

- VPC yang diintip ke jaringan ODB Anda harus sama. Akun AWS Jika VPC peered berada di akun yang berbeda dari jaringan ODB, lampiran gateway transit gagal terlepas dari konfigurasi berbagi.
- VPC yang diintip ke jaringan ODB Anda harus memiliki lampiran gateway transit.

> **Note**
>
> Jika gateway transit dikonfigurasi untuk berbagi, itu dapat berada di akun apa pun. Dengan demikian, gateway itu sendiri tidak perlu berada di akun yang sama dengan jaringan VPC dan ODB.

- Lampiran gateway transit harus berada di Availability Zone (AZ) yang sama dengan jaringan ODB.

Batasan

Perhatikan batasan berikut dari Amazon VPC Transit Gateways untuk: Oracle Database@AWS

- Amazon VPC Transit Gateways tidak menawarkan integrasi asli untuk menggunakan jaringan ODB sebagai lampiran. Oleh karena itu, fitur VPC seperti berikut ini tidak tersedia:
  - Resolusi nama host DNS publik ke alamat IP pribadi
  - Pemberitahuan acara untuk perubahan topologi jaringan ODB, routing, dan status koneksi
- Lalu lintas multicast ke jaringan ODB tidak didukung.

Menyiapkan dan mengonfigurasi gateway transit

Anda membuat dan mengonfigurasi gateway transit menggunakan konsol atau `aws ec2` perintah Amazon VPC. Prosedur berikut mengasumsikan bahwa Anda tidak memiliki jaringan ODB yang diintip ke VPC di Anda. Akun AWS Jika jaringan ODB dan VPC sudah diintip di akun Anda, lewati langkah 1-3.

> **Note**
>
> Jika Anda melampirkan atau memasang kembali lampiran pada VPC Anda, pastikan Anda memasukkan kembali rentang CIDR ke jaringan ODB ODB.

Untuk mengatur dan mengkonfigurasi gateway transit untuk Oracle Database@AWS

1. Buat jaringan ODB. Untuk informasi selengkapnya, lihat Langkah 1: Buat jaringan ODB di Oracle Database@AWS.
2. Buat VPC, menggunakan akun yang sama yang berisi jaringan ODB. Untuk informasi selengkapnya, lihat Membuat VPC di Panduan Pengguna Amazon VPC.
3. Buat koneksi peering ODB antara jaringan ODB Anda dan VPC Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi ODB mengintip ke VPC Amazon di Oracle Database @AWS.
4. Siapkan gateway transit dengan mengikuti langkah-langkah di Memulai menggunakan Amazon VPC Transit Gateways. Gateway harus sama dengan jaringan ODB dan VPC, atau dibagikan oleh akun lain. Akun AWS

   > **Important**
   >
   > Buat lampiran gateway transit di AZ yang sama dengan jaringan ODB.

5. Tambahkan rentang CIDR ke jaringan ODB Anda untuk jaringan lokal VPCs dan lokal yang Anda rencanakan untuk dilampirkan ke jaringan inti Anda. Untuk informasi selengkapnya, lihat Memperbarui jaringan ODB di Oracle Database@AWS.

   Jika Anda menggunakan CLI, jalankan perintah `update-odb-network` dengan `--peered-cidrs-to-be-added` dan. `--peered-cidrs-to-be-removed` Untuk informasi selengkapnya, lihat Referensi Perintah AWS AWS CLI.

Mengkonfigurasi AWS Cloud WAN untuk Oracle Database@AWS

AWS Cloud WAN adalah layanan Managed Wide-Area Networking (WAN). Anda dapat menggunakan AWS Cloud WAN untuk membangun, mengelola, dan memantau jaringan global terpadu yang menghubungkan sumber daya yang berjalan di lingkungan cloud dan lokal Anda.

Di AWS Cloud WAN, jaringan global adalah jaringan pribadi tunggal yang bertindak sebagai wadah tingkat tinggi untuk objek jaringan Anda. Jaringan inti adalah bagian dari jaringan global Anda yang dikelola oleh AWS.

AWS Cloud WAN memberikan manfaat utama berikut:

- Manajemen jaringan terpusat yang menyederhanakan operasi sambil menjaga keamanan di beberapa Wilayah
- Jaringan inti dengan segmentasi bawaan untuk mengisolasi lalu lintas melalui beberapa domain perutean
- Support untuk kebijakan untuk mengotomatiskan manajemen jaringan dan menentukan konfigurasi yang konsisten di seluruh jaringan global Anda

Di Oracle Database@AWS, jaringan ODB mendukung peering ke hanya satu VPC. Jika Anda menghubungkan jaringan inti AWS Cloud WAN ke VPC peered, ini memungkinkan perutean lalu lintas global. Aplikasi yang terpasang VPCs di beberapa Wilayah dapat mengakses klaster Exadata VM di jaringan ODB Anda. Anda dapat mengisolasi lalu lintas jaringan ODB di segmennya sendiri atau mengaktifkan akses ke segmen lain.

Diagram berikut menunjukkan jaringan inti AWS Cloud WAN yang terhubung ke tiga VPCs dan satu jaringan lokal.

AWS Cloud WAN tidak menawarkan integrasi asli untuk menggunakan jaringan ODB sebagai lampiran. Oleh karena itu, fitur VPC seperti berikut ini tidak tersedia:

- Resolusi nama host DNS publik ke alamat IP pribadi
- Pemberitahuan acara untuk perubahan topologi jaringan ODB, routing, dan status koneksi

Di AWS Cloud WAN, Anda dikenakan biaya per jam untuk hal-hal berikut:

- Jumlah Wilayah (tepi jaringan inti)
- Jumlah lampiran jaringan inti
- Jumlah lalu lintas yang mengalir melalui jaringan inti Anda melalui lampiran

Untuk informasi detail harga, lihat harga AWS Cloud WAN.

Untuk mengkonfigurasi jaringan inti untuk Oracle Database@AWS

1. Tambahkan rentang CIDR ke jaringan ODB Anda untuk jaringan lokal VPCs dan lokal yang Anda rencanakan untuk dilampirkan ke jaringan inti Anda. Untuk informasi selengkapnya, lihat Memperbarui jaringan ODB di Oracle Database@AWS.

   > **Note**
   >
   > Jika Anda melampirkan atau memasang kembali lampiran pada VPC Anda, pastikan Anda memasukkan kembali rentang CIDR ke jaringan ODB ODB.

2. Ikuti langkah-langkah di Buat jaringan global AWS Cloud WAN dan jaringan inti.

Berbagi hak di Oracle Database @AWS

Dengan Oracle Database@AWS, Anda dapat berbagi hak AWS Marketplace untuk Oracle Database AWS @ di organisasi yang sama. Akun AWS AWS Ini memungkinkan akun lain untuk menyediakan infrastruktur Oracle Exadata mereka sendiri dan sumber daya jaringan ODB menggunakan langganan Anda.

Metode berbagi

Oracle Database@AWS mendukung dua metode untuk berbagi:

Berbagi hak dengan AWS License Manager

- Berikan akun lain kemampuan untuk menyediakan infrastruktur Oracle Exadata dan sumber daya jaringan ODB mereka sendiri
- Setiap akun beroperasi secara independen dengan kontrol siklus hidup sumber daya penuh
- Terbaik untuk memungkinkan penyediaan layanan mandiri di seluruh tim atau unit bisnis

Berbagi sumber daya dengan AWS Resource Access Manager (AWS RAM)

- Bagikan infrastruktur Oracle Exadata dan sumber daya jaringan ODB yang sudah disediakan
- Memusatkan manajemen infrastruktur sambil memungkinkan akun penerima untuk membuat klaster VM
- Optimalkan biaya dengan memiliki beberapa akun menggunakan infrastruktur yang sama

Anda dapat menggunakan kedua metode berbagi secara bersamaan berdasarkan kebutuhan organisasi Anda.

Batasan untuk Oracle Database@ berbagi hak AWS

Saat berbagi AWS hak Oracle Database@, ingatlah batasan berikut:

- Anda hanya dapat berbagi dengan Akun AWS dalam AWS organisasi Anda
- Anda tidak dapat berbagi dengan seluruh unit organisasi (OU) atau seluruh organisasi
- Akun dapat menerima hak hanya dari satu akun pembeli (dari satu penawaran pribadi)

- Akun pembeli tidak dapat berbagi hak dengan akun pembeli lain
- Akun penerima harus menginisialisasi AWS layanan Oracle Database@ sebelum mereka dapat menggunakan hak bersama
- Operasi hibah hak hanya dapat dilakukan dari Wilayah AS Timur (Virginia N.)

Berbagi hak Oracle Database@AWS di seluruh akun

Untuk mengaktifkan kolaborasi sambil mengoptimalkan biaya, bagikan AWS hak Oracle Database@ dengan orang lain dalam organisasi yang sama. Akun AWS AWS Topik ini menjelaskan cara berbagi hak menggunakan AWS License Manager.

Prasyarat untuk berbagi hak

Sebelum Anda membagikan AWS hak Oracle Database@, pastikan Anda memiliki yang berikut:

- AWS Langganan Oracle Database@ aktif (Anda harus menjadi akun pembeli yang menerima penawaran pribadi melalui) AWS Marketplace
- AWS Akun di organisasi Anda yang ingin Anda bagikan haknya IDs
- Izin yang diperlukan bagi pemberi dan penerima hibah untuk menggunakan sumber daya dan operasi AWS License Manager (untuk informasi selengkapnya, lihat Identitas dan manajemen akses untuk License Manager di Panduan Pengguna License Manager AWS)
- Izin yang tercantum di bawah ini untuk Anda (pemberi) dan penerima hak (penerima hibah)

Izin yang diperlukan untuk berbagi hak

Selain AWS izin License Manager, Oracle Database@AWS memerlukan izin berikut:

Izin pemberi

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

Izin penerima hibah

- `odb:UpdateGrantShare`

- `odb:DeleteGrantShare`

Berbagi AWS hak Oracle Database@ dengan akun lain menggunakan License Manager AWS

Untuk berbagi hak dengan AWS akun lain, Anda membuat hibah menggunakan AWS License Manager. Untuk informasi selengkapnya, lihat Mendistribusikan hak License Manager di Panduan Pengguna AWS License Manager.

Setelah Anda membuat hibah, penerima (penerima hibah) harus:

- Terima dan aktifkan hibah. Untuk informasi selengkapnya, lihat Penerimaan dan aktivasi hibah di License Manager di Panduan Pengguna AWS License Manager.
- Ikuti petunjuk inisialisasi untuk Oracle Database @.AWS

Setelah inisialisasi selesai, penerima hibah dapat menyediakan sumber daya Oracle AWS Database@ menggunakan hak bersama.

Berbagi sumber daya di Oracle Database @AWS

Dengan Oracle Database@AWS, Anda dapat berbagi infrastruktur Exadata dan jaringan ODB Anda di beberapa di organisasi yang sama. Akun AWS AWS Ini memungkinkan Anda untuk menyediakan infrastruktur sekali dan menggunakannya kembali di seluruh akun tepercaya, memungkinkan Anda mengurangi biaya sambil memisahkan tanggung jawab.

Saat Anda berbagi sumber daya:

- Akun yang memiliki sumber daya (akun pemilik) mempertahankan kendali atas siklus hidup sumber daya.
- Akun yang menerima akses ke sumber daya bersama (akun tepercaya) dapat melihat dan menggunakan sumber daya ini berdasarkan izin yang diberikan.
- Akun tepercaya dapat membuat sumber dayanya sendiri di infrastruktur bersama tetapi tidak dapat menghapus sumber daya bersama yang mendasarinya.

Oracle Database @integrasi AWS dengan AWS RAM

Oracle Database@AWS menggunakan AWS Resource Access Manager (AWS RAM) untuk mengaktifkan berbagi sumber daya yang aman dan terkontrol di seluruh akun. Dengan AWS RAM, Anda dapat berbagi AWS sumber daya Oracle Database@ dengan aman di beberapa AWS akun dalam organisasi yang sama. AWS AWS RAM menyederhanakan berbagi sumber daya, mengurangi overhead operasional, dan memberikan keamanan dan visibilitas ke sumber daya Oracle Database @ bersama.AWS

Dengan AWS RAM, Anda berbagi sumber daya yang Anda miliki dengan membuat pembagian sumber daya. Pembagian sumber daya menentukan sumber daya untuk dibagikan, dan Akun AWS dengan siapa membagikannya.

Manfaat berbagi sumber daya di Oracle Database @AWS

Berbagi AWS sumber daya Oracle Database@ di seluruh akun memberikan manfaat berikut:

- Optimalisasi biaya — Menyediakan infrastruktur Exadata yang mahal sekali melalui akun administratif dan membagikannya dengan banyak akun, mengurangi biaya keseluruhan.
- Pemisahan tanggung jawab - Pertahankan batasan yang jelas antara administrator infrastruktur dan pengguna database sambil memungkinkan kolaborasi.

- Manajemen yang disederhanakan - Memusatkan penyediaan dan manajemen infrastruktur sambil memungkinkan operasi basis data terdistribusi.
- Tata kelola yang konsisten — Menerapkan kebijakan dan kontrol yang konsisten di seluruh sumber daya bersama.

Misalnya, administrator dapat menyediakan infrastruktur Oracle Exadata dan jaringan ODB di dalamnya Akun AWS dan membagikannya dengan akun pengembang. Pengembang kemudian dapat membuat cluster VM pada infrastruktur bersama ini tanpa perlu menyediakan perangkat keras mahal mereka sendiri. Pendekatan ini secara signifikan mengurangi biaya sambil mempertahankan pemisahan tanggung jawab yang tepat antar akun.

Cara kerja berbagi sumber daya di Oracle Database@AWS

Anda dapat membagikan sumber daya Oracle Database@AWS berikut:

- Infrastruktur Oracle Exadata
- Jaringan ODB

Oracle Database@AWS membagikan sumber daya sebelumnya melalui proses berikut:

1. Akun pembeli (akun yang menerima AWS penawaran pribadi Oracle Database@ melalui AWS Marketplace) menyediakan AWS sumber daya Oracle Database @, seperti infrastruktur Exadata dan jaringan ODB.
2. Akun pembeli membuat pembagian sumber daya menggunakan AWS RAM, menentukan sumber daya untuk dibagikan dan akun tepercaya untuk dibagikan.
3. Pembagian sumber daya untuk akun tepercaya dalam organisasi yang sama diterima secara otomatis.
4. Sebelum menggunakan sumber daya bersama, akun tepercaya harus menginisialisasi AWS layanan Oracle Database@ di akun mereka dengan menggunakan `aws odb initialize-service` perintah atau dengan memilih Activate account di konsol Oracle Database@.AWS
5. Setelah inisialisasi, akun tepercaya dapat membuat sumber daya mereka sendiri di infrastruktur bersama, seperti kluster VM pada infrastruktur Exadata bersama dan jaringan ODB.

Izin pada sumber daya bersama untuk akun tepercaya

Saat Anda berbagi sumber daya, Oracle Database@AWS secara otomatis memilih tindakan tertentu (izin terkelola) untuk setiap jenis sumber daya:

Untuk infrastruktur Exadata

Oracle Database@AWS memberikan izin berikut ke akun tepercaya:

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

Untuk jaringan ODB

Izin berikut diberikan ke akun tepercaya:

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

Berbagi sumber daya menghormati sifat hierarkis sumber daya Oracle Database@.AWS Misalnya, jika Anda berbagi infrastruktur Exadata, akun tepercaya dapat membuat klaster VM di infrastruktur ini, tetapi akun tersebut tidak dapat memodifikasi atau menghapus infrastruktur Exadata itu sendiri.

Ketika sumber daya tidak dibagikan, akun tepercaya kehilangan kemampuan untuk membuat sumber daya baru di infrastruktur bersama. Namun, sumber daya apa pun yang telah mereka buat tetap dapat diakses dan berfungsi.

Batasan untuk Oracle Database @berbagi sumber daya AWS

Sebelum berbagi sumber daya, ingatlah batasan berikut.

Keterbatasan untuk berbagi sumber daya

Saat berbagi AWS sumber daya Oracle Database@, ingatlah batasan berikut:

- Anda dapat berbagi sumber daya hanya dengan Akun AWS IDs.
- Anda dapat berbagi sumber daya hanya untuk Akun AWS dalam AWS organisasi yang sama.
- Anda berbagi sumber daya dalam AWS Wilayah tertentu. Untuk berbagi sumber daya di seluruh Wilayah, Anda harus membuat pembagian sumber daya terpisah di setiap Wilayah.
- Saat Anda membuat pembagian sumber daya, tindakan (izin terkelola) untuk setiap jenis sumber daya dipilih secara otomatis dan tidak dapat diubah.
- Anda tidak dapat menggunakan Oracle Database@AWS sebagai sumber daya dan berbagi dengan yang lain. Akun AWS
- Akun tepercaya dapat menggunakan sumber daya bersama hanya dari satu akun pembeli (dari satu penawaran pribadi). Dengan demikian, dua akun pembeli tidak dapat berbagi sumber daya dengan akun tepercaya yang sama.
- Akun pembeli tidak dapat berbagi sumber daya dengan akun pembeli lain.
- Sumber daya yang dibagikan dengan akun tepercaya harus dibagikan oleh akun pembeli di wilayah asal pembeli terlebih dahulu.
- Saat Anda membatalkan pembagian sumber daya, kami sarankan Anda menunggu sekitar 15 menit sebelum membagikan kembali sumber daya yang sama dengan akun tepercaya yang sama.

Keterbatasan untuk membuat dan menggunakan sumber daya bersama

Saat membuat atau menggunakan AWS sumber daya Oracle Database@, ingatlah batasan berikut:

- Hanya akun pembeli yang dapat membuat infrastruktur Exadata dan sumber daya jaringan ODB. Akun pembeli adalah akun yang menerima penawaran pribadi Oracle Database @AWS .
- Akun tepercaya hanya dapat membuat sumber daya pada infrastruktur Exadata yang dibagikan oleh akun pembeli.
- Akun tepercaya harus menginisialisasi AWS layanan Oracle Database@ di akun mereka sebelum mereka dapat menggunakan sumber daya bersama.

Batasan untuk menghapus sumber daya bersama

- Anda tidak dapat menghapus infrastruktur Exadata yang memiliki kluster VM yang dibuat oleh akun tepercaya hingga cluster VM tersebut dihapus.
- Anda tidak dapat menghapus jaringan ODB yang memiliki koneksi peering ODB yang dibuat oleh akun tepercaya hingga koneksi peering ODB telah dihapus.
- Akun pembeli tidak dapat menghapus AWS sumber daya Oracle Database@ yang dibuat oleh akun tepercaya.
- Akun tepercaya dapat melihat sumber daya bersama tetapi tidak dapat mengubah atau menghapus sumber AWS daya Oracle Database@ yang dimiliki oleh akun pembeli.

Berbagi Oracle Database@AWS sumber daya di seluruh akun

Untuk mengaktifkan kolaborasi sambil mengoptimalkan biaya, bagikan AWS sumber daya Oracle Database@ dengan orang lain Akun AWS dalam organisasi yang sama. AWS Topik ini menjelaskan cara berbagi sumber daya menggunakan AWS Resource Access Manager (AWS RAM).

Topik

Prasyarat untuk berbagi sumber daya

Sebelum Anda membagikan AWS sumber daya Oracle Database@, pastikan Anda memiliki yang berikut ini:

- AWS Langganan Oracle Database@ aktif (Anda harus menjadi akun pembeli yang menerima penawaran pribadi melalui) AWS Marketplace
- Nama IDs atau sumber daya yang ingin Anda bagikan, seperti infrastruktur Exadata atau jaringan ODB
- AWS Akun di organisasi Anda yang ingin Anda bagikan sumber daya IDs
- Izin yang diperlukan untuk membuat pembagian sumber daya di AWS RAM

- Kemampuan untuk berbagi sumber daya dengan AWS Organizations menggunakan AWS RAM (untuk informasi selengkapnya, lihat Mengaktifkan berbagi sumber daya AWS Organizations di dalam Panduan AWS Resource Access Manager Pengguna)

Berbagi AWS sumber daya Oracle Database@ dengan akun lain menggunakan AWS RAM

Untuk berbagi infrastruktur Exadata atau jaringan ODB dengan AWS akun lain, Anda membuat pembagian sumber daya menggunakan. AWS RAM Ini memungkinkan akun tepercaya untuk membuat klaster VM di infrastruktur Exadata Anda.

Konsol

1. Buka AWS RAM konsol di https://console.aws.amazon.com/ram/.
2. Pilih Buat berbagi sumber daya.
3. Untuk Nama, masukkan nama deskriptif untuk berbagi sumber daya Anda.
4. Di bawah Pilih jenis sumber daya, salah satu sumber daya berikut:
   - Oracle Database @jaringan ODB AWS
   - Database Oracle@ Infrastruktur Exadata AWS
5. Pilih sumber daya infrastruktur Exadata yang ingin Anda bagikan. Pilih Berikutnya sampai Anda mendapatkan akses Grant ke kepala sekolah.
6. Di bawah Prinsipal, pilih Akun AWS, lalu masukkan AWS akun yang ingin IDs Anda bagikan.
7. Di bawah Izin terkelola, pilih izin berikut untuk mengizinkan akun tepercaya membuat kluster VM di infrastruktur Exadata bersama:
   - AWSRAMDefaultIzin ODBNetwork
   - AWSRAMDefaultIzin ODBCloud ExadataInfrastructure
8. Pilih Buat berbagi sumber daya.

AWS CLI

Untuk berbagi sumber daya menggunakan AWS CLI, gunakan `aws ram create-resource-share` perintah. Contoh berikut membuat pembagian sumber daya bernama `ExadataInfraShare` yang berbagi infrastruktur Exadata yang ditentukan dengan akun 222222222222, yang memungkinkan akun ini membuat kluster VM pada infrastruktur bersama.

```
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
```

Melihat pembagian sumber daya Anda

Untuk melihat sumber daya yang telah Anda bagikan dan akun yang Anda bagikan:

Konsol

1. Buka AWS RAM konsol di https://console.aws.amazon.com/ram/.
2. Pilih Sumber daya bersama untuk melihat sumber daya yang telah Anda bagikan dengan akun lain.
3. Pilih pembagian sumber daya untuk melihat detailnya, termasuk sumber daya yang dibagikan dan prinsipal yang dibagikan.

AWS CLI

Untuk melihat pembagian sumber daya Anda menggunakan AWS CLI, gunakan `get-resource-shares` perintah:

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

Untuk melihat sumber daya dalam berbagi sumber daya tertentu, gunakan `list-resources` perintah:

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

Untuk melihat prinsipal (akun) tempat berbagi sumber daya dibagikan, gunakan perintah: `list-principals`

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

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

Memperbarui atau menghapus pembagian sumber daya menggunakan AWS RAM

Untuk berhenti berbagi sumber daya dengan akun tepercaya menggunakan AWS RAM, lakukan salah satu tindakan berikut:

- Hapus sumber daya dari pembagian sumber daya.
- Hapus akun tepercaya dari pembagian sumber daya.
- Hapus pembagian sumber daya.

Sebelum Anda mencabut akses ke atau menghapus sumber daya bersama, pertimbangkan implikasi berikut:

- Akun tepercaya tidak dapat lagi membuat sumber daya baru pada infrastruktur yang tidak dibagikan.
- Sumber daya yang ada yang dibuat oleh akun tepercaya pada infrastruktur Exadata bersama terus berfungsi dan tetap dapat diakses oleh akun tersebut. Akun AWS
- Anda tidak dapat menghapus infrastruktur Exadata yang memiliki kluster VM yang dibuat oleh akun tepercaya hingga cluster VM tersebut dihapus.

Sebelum berhenti berbagi sumber daya, sebaiknya Anda berkoordinasi dengan akun tepercaya untuk memastikan transisi yang lancar.

Untuk informasi selengkapnya, lihat Memperbarui bagian sumber daya AWS RAM dan Menghapus bagian sumber daya AWS RAM di Panduan AWS Resource Access Manager Pengguna.

Inisialisasi Oracle Database@AWS di akun tepercaya

Akun tepercaya adalah akun Akun AWS yang Anda tetapkan sebagai memenuhi syarat untuk menerima pembagian sumber daya. Itu harus individu lain Akun AWS di AWS organisasi Anda. Sebelum Anda dapat menggunakan AWS sumber daya Oracle Database@ bersama di akun tepercaya, Anda harus menginisialisasi layanan. Inisialisasi menciptakan metadata yang diperlukan dan menetapkan koneksi antara Infrastruktur Cloud Anda Akun AWS dan Oracle.

Topik

Apa itu inisialisasi Oracle Database @?AWS

Setelah sumber daya dibagikan dengan akun Anda, Anda harus menginisialisasi AWS layanan Oracle Database @ sebelum Anda dapat mengakses atau menggunakan sumber daya bersama. Jika Anda mencoba menggunakan Oracle Database @AWS APIs tanpa menginisialisasi layanan terlebih dahulu, Anda menerima kesalahan.

Inisialisasi adalah proses satu kali. Ini menciptakan metadata yang diperlukan dan membuat koneksi antara Infrastruktur Cloud Anda Akun AWS dan Oracle.

Anda dapat menginisialisasi layanan menggunakan AWS Management Console atau. AWS CLI

Konsol

1. Buka konsol Oracle Database@AWS di. https://console.aws.amazon.com/odb/
2. Jika ini adalah pertama kalinya Anda mengakses AWS konsol Oracle Database@ di akun ini, Anda akan melihat halaman selamat datang.
3. Pilih Aktifkan akun.
4. Proses inisialisasi layanan dimulai. Proses ini mungkin memakan waktu beberapa menit untuk menyelesaikannya.
5. Segarkan halaman selamat datang secara berkala hingga tombol Aktifkan akun berubah menjadi tombol Dasbor.
6. Pilih Dasbor untuk mulai menggunakan Oracle Database AWS@.

AWS CLI

Untuk menginisialisasi Oracle Database@AWS di akun tepercaya Anda menggunakan AWS CLI, gunakan perintah. `initialize-service`

```
aws odb initialize-service
```

Untuk memeriksa status inisialisasi, gunakan `get-oci-onboarding-status` perintah.

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

Ketika inisialisasi selesai, output menunjukkan statusACTIVE_LIMITED, yang menunjukkan bahwa akun Anda dapat mengakses sumber daya bersama tetapi tidak dapat membuat infrastruktur Exadata baru atau jaringan ODB.

Langkah selanjutnya

Setelah Anda menginisialisasi Oracle Database@AWS di akun tepercaya Anda, Anda dapat melakukan hal berikut:

- Lihat sumber daya bersama menggunakan `get` perintah `list` dan atau di AWS konsol.
- Buat cluster VM dan cluster VM Otonom pada infrastruktur Exadata bersama dan jaringan ODB.
- Buat koneksi peering ODB pada jaringan ODB bersama.

Untuk informasi selengkapnya tentang bekerja dengan sumber daya bersama, lihatBekerja dengan Oracle Database@AWS sumber daya bersama di akun tepercaya.

Bekerja dengan Oracle Database@AWS sumber daya bersama di akun tepercaya

Setelah sumber daya dibagikan dengan akun tepercaya Anda dan Anda telah menginisialisasi AWS layanan Oracle Database@, Anda dapat melihat dan menggunakan sumber daya bersama. Topik ini menjelaskan cara bekerja dengan sumber daya bersama di akun tepercaya.

Topik

- Batasan untuk sumber daya bersama di akun tepercaya
- Membuat cluster VM pada infrastruktur Exadata bersama
- Melihat sumber daya bersama di akun tepercaya
- Menyiapkan peering ODB dengan jaringan ODB bersama

Batasan untuk sumber daya bersama di akun tepercaya

Saat bekerja dengan AWS sumber daya Oracle Database@ bersama, perhatikan batasan berikut:

- Berbagi sumber daya hanya didukung dalam AWS organisasi yang sama.
- Hanya akun pembeli (akun yang menerima penawaran AWS pribadi Oracle Database @) yang dapat membuat infrastruktur Exadata dan sumber daya jaringan ODB.
- Anda dapat membuat sumber daya hanya pada infrastruktur bersama dan hanya jika Anda memiliki izin yang diperlukan.
- Tindakan spesifik (izin terkelola) untuk setiap jenis sumber daya dipilih secara otomatis selama pembuatan berbagi sumber daya dan tidak dapat dimodifikasi.
- Anda tidak dapat mengubah atau menghapus sumber daya yang dimiliki oleh akun lain.
- Sumber daya yang Anda buat pada infrastruktur bersama dimiliki oleh akun Anda dan dihitung dalam kuota OCI Anda. Hal yang sama berlaku untuk sumber daya induk.
- Jika akun pemilik membatalkan pembagian sumber daya, Anda tidak dapat lagi membuat sumber daya baru di infrastruktur bersama ini. Namun, sumber daya Anda yang ada terus berfungsi.
- Berbagi sumber daya Lintas Wilayah tidak didukung. Anda hanya dapat berbagi sumber daya dalam AWS Wilayah yang sama.
- Sumber daya akun tepercaya ditagih ke pembeli langganan Oracle AWS Database@.
- Saat menggunakan sumber daya yang dibagikan, Anda harus memberikan Nama Sumber Daya Amazon (ARN).

Membuat cluster VM pada infrastruktur Exadata bersama

Jika akun tepercaya Anda memiliki akses ke infrastruktur Exadata bersama dan jaringan ODB, Anda dapat membuat klaster Exadata VM, kluster VM Otonom, atau peering ODB pada infrastruktur ini.

> **Note**
>
> Saat menggunakan sumber daya yang dibagikan kepada Anda, alih-alih hanya menentukan ID sumber daya, Anda harus menentukan Nama Sumber Daya Amazon (ARN).

Konsol

1. Buka konsol Oracle Database@AWS di. https://console.aws.amazon.com/odb/
2. Di panel navigasi, pilih Exadata VM cluster atau Autonomous VM cluster.
3. Pilih Create VM cluster atau Create Autonomous VM cluster.

4. Untuk infrastruktur Exadata, pilih infrastruktur Exadata bersama tempat Anda ingin membuat cluster VM.
5. Lengkapi bidang yang tersisa seperti yang diperlukan untuk konfigurasi cluster VM Anda.
6. Pilih Create VM cluster atau Create Autonomous VM cluster.

AWS CLI

Untuk membuat cluster VM pada infrastruktur Exadata bersama menggunakan AWS CLI, gunakan perintah: `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..." \
```

Untuk membuat cluster VM Autonomous pada infrastruktur Exadata bersama menggunakan AWS CLI, gunakan perintah: `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
```

Kluster VM dibuat pada infrastruktur Exadata bersama yang ditentukan dan dimiliki oleh akun tepercaya Anda.

Melihat sumber daya bersama di akun tepercaya

Anda dapat melihat sumber daya yang telah dibagikan dengan akun Anda menggunakan Konsol AWS Manajemen atau AWS CLI.

Konsol

1. Buka konsol Oracle Database@AWS di. https://console.aws.amazon.com/odb/
2. Di panel navigasi, pilih jenis sumber daya yang ingin Anda lihat: Infrastruktur Exadata atau jaringan ODB.
3. Konsol menampilkan sumber daya yang dibagikan dengan Anda.
4. Pilih sumber daya bersama untuk melihat detailnya.

AWS CLI

Untuk melihat sumber daya bersama menggunakan AWS CLI, gunakan `list` perintah yang sesuai untuk jenis sumber daya. Misalnya, untuk membuat daftar infrastruktur Exadata:

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

Respons menunjukkan sumber daya yang dibagikan dengan Anda.

Untuk mendapatkan informasi terperinci tentang sumber daya bersama tertentu, gunakan `get` perintah yang sesuai dengan ID sumber daya:

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

Menyiapkan peering ODB dengan jaringan ODB bersama

Untuk mengaktifkan komunikasi antara aplikasi dan database pada jaringan ODB bersama, Anda dapat mengatur ODB peering antara VPC dan jaringan ODB bersama. Untuk informasi lebih lanjut tentang pengintipan ODB, lihat. Membuat koneksi peering ODB di Oracle Database@AWS

Konsol

1. Buka konsol Oracle Database@AWS di. https://console.aws.amazon.com/odb/
2. Di panel navigasi, pilih ODB peering.
3. Pilih Buat peering jaringan ODB.
4. Untuk jaringan ODB, pilih jaringan ODB bersama yang ingin Anda peer.
5. Untuk jaringan Peer, pilih VPC Anda.
6. Pilih Buat peering jaringan ODB.

AWS CLI

Untuk membuat koneksi peering jaringan antara VPC Anda dan jaringan ODB bersama menggunakan, gunakan AWS CLI perintah. `create-odb-peering-connection`

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

Setelah membuat koneksi peering, perbarui tabel rute Anda untuk mengaktifkan lalu lintas antara jaringan peered.

```
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
```

Mengelola Database Oracle@AWS

Anda dapat memodifikasi dan menghapus beberapa Oracle Database@AWS sumber daya setelah Anda membuatnya.

Memperbarui jaringan ODB di Oracle Database@AWS

Anda dapat memperbarui sumber daya jaringan ODB berikut:

- Nama jaringan ODB
- VPC Amazon yang digunakan untuk membuat koneksi peering ODB ke jaringan ODB
- Rentang VPC CIDR yang dapat mengakses sumber daya Exadata di jaringan ODB

> **Note**
>
> Dengan menentukan rentang CIDR, Anda membatasi konektivitas ke subnet VPC yang diperlukan alih-alih membuat seluruh VPC tersedia untuk jaringan ODB.

Bagian ini mengasumsikan bahwa Anda telah membuat jaringan ODB di. Langkah 1: Buat jaringan ODB di Oracle Database@AWS

Untuk memperbarui jaringan ODB

1. Masuk ke Konsol Manajemen AWS dan buka Oracle Database@AWS konsol di https://console.aws.amazon.com/odb/.
2. Dari panel kiri, pilih jaringan ODB.
3. Pilih jaringan yang ingin Anda modifikasi.
4. Pilih Ubah.
5. (Opsional) Untuk nama jaringan ODB, masukkan nama jaringan baru. Nama harus 1-255 karakter dan dimulai dengan karakter alfabet atau garis bawah. Itu tidak bisa mengandung tanda hubung berturut-turut.
6. (Opsional) Untuk Peered CIDRs, tentukan rentang CIDR dari VPC peered yang memerlukan konektivitas ke jaringan ODB. Untuk membatasi akses, kami menyarankan Anda menentukan rentang CIDR minimum yang diperlukan.

7. (Opsional) Untuk Mengonfigurasi integrasi layanan, pilih atau batalkan pilihan Amazon S3 atau Nol-ETL.
8. Pilih Lanjutkan, lalu pilih Ubah.

Menghapus jaringan ODB di Oracle Database@AWS

Anda dapat menghapus jaringan ODB. Bagian ini mengasumsikan bahwa Anda telah membuat jaringan ODB di. Langkah 1: Buat jaringan ODB di Oracle Database@AWS Anda tidak dapat menghapus jaringan ODB yang saat ini digunakan oleh cluster VM.

Untuk menghapus jaringan ODB

1. Masuk ke Konsol Manajemen AWS dan buka Oracle Database@AWS konsol di https://console.aws.amazon.com/odb/.
2. Dari panel kiri, pilih jaringan ODB.
3. Pilih jaringan yang ingin Anda hapus.
4. Pilih Hapus.
5. (Opsional) Pilih Hapus sumber daya OCI terkait untuk menghapus sumber daya OCI yang dibuat bersama dengan jaringan ODB.
6. Di kotak teks, masukkan**`delete me`**.
7. Pilih Hapus.

Menghapus cluster VM di Oracle Database@AWS

Anda dapat menghapus cluster Exadata VM atau cluster VM Autonomous. Bagian ini mengasumsikan bahwa Anda telah membuat cluster VM di. Langkah 3: Buat cluster Exadata VM atau cluster VM Autonomous di Oracle Database@AWS

Untuk menghapus cluster VM

1. Masuk ke Konsol Manajemen AWS dan buka Oracle Database@AWS konsol di https://console.aws.amazon.com/odb/.
2. Dari panel kiri, pilih cluster Exadata VM atau cluster VM otonom.
3. Pilih cluster VM untuk dihapus.
4. Pilih Hapus.

5. Saat diminta, masukkan lalu **`delete me`** pilih Hapus.

Menghapus infrastruktur Oracle Exadata di Oracle Database@AWS

Anda dapat menghapus infrastruktur Oracle Exadata. Bagian ini mengasumsikan bahwa Anda telah membuat infrastruktur Oracle Exadata di. Langkah 2: Buat infrastruktur Oracle Exadata di Oracle Database@AWS Anda tidak dapat menghapus infrastruktur Exadata yang saat ini digunakan oleh klaster VM.

Untuk menghapus infrastruktur Oracle Exadata

1. Masuk ke Konsol Manajemen AWS dan buka Oracle Database@AWS konsol di https://console.aws.amazon.com/odb/.
2. Dari panel kiri, pilih infrastruktur Exadata.
3. Pilih infrastruktur Exadata untuk dihapus.
4. Pilih Hapus.
5. Saat diminta, masukkan lalu **`delete me`** pilih Hapus.

Menghapus koneksi peering ODB

Ketika Anda tidak lagi membutuhkan koneksi peering ODB, Anda dapat menghapusnya. Anda harus menghapus semua koneksi peering ODB sebelum Anda dapat menghapus jaringan ODB.

Konsol

1. Masuk ke Konsol Manajemen AWS dan buka Oracle Database@AWS konsol di https://console.aws.amazon.com/odb/.
2. Di panel navigasi, pilih koneksi peering ODB.
3. Pilih koneksi peering ODB untuk dihapus.
4. Pilih Hapus.
5. Untuk mengonfirmasi penghapusan, masukkan **`delete me`** dan pilih Hapus.

AWS CLI

Untuk menghapus koneksi peering ODB, gunakan perintah. `delete-odb-peering-connection`

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

Mencadangkan di Oracle Database @AWS

Oracle Database @AWS menyediakan beberapa opsi cadangan untuk melindungi database Oracle Anda. Anda dapat menggunakan cadangan terkelola Oracle yang terintegrasi secara mulus dengan Amazon S3 atau membuat cadangan yang dikelola pengguna sendiri menggunakan Oracle Recovery Manager (RMAN).

Pencadangan terkelola Oracle ke Amazon S3

Saat Anda membuat jaringan ODB, Oracle Database@AWS secara otomatis mengonfigurasi akses jaringan untuk cadangan terkelola Oracle ke Amazon S3. OCI mengonfigurasi entri DNS dan daftar keamanan yang diperlukan. Konfigurasi ini memungkinkan lalu lintas antara OCI Virtual Cloud Network (VCN) dan Amazon S3. Jaringan ODB tidak mengaktifkan atau mengontrol backup otomatis.

Backup terkelola Oracle sepenuhnya dikelola oleh OCI. Ketika Anda membuat database Oracle Exadata Anda, Anda dapat mengaktifkan backup otomatis dengan memilih Aktifkan backup otomatis di konsol OCI. Pilih salah satu tujuan pencadangan berikut:

- Amazon S3
- Penyimpanan Objek OCI
- Layanan Pemulihan Otonom

Untuk informasi selengkapnya, lihat Backup Database Exadata dalam dokumentasi OCI.

Pencadangan yang dikelola pengguna ke Amazon S3 di Oracle Database @AWS

Dengan Oracle Database@AWS, Anda dapat membuat backup database yang dikelola pengguna menggunakan Exadata Database Service on Dedicated Infrastructure. Anda mencadangkan data Anda dengan Oracle Recovery Manager (RMAN) dan menyimpannya di bucket Amazon S3 Anda. Anda memiliki kontrol penuh atas penjadwalan cadangan, kebijakan penyimpanan, dan biaya penyimpanan sambil mempertahankan manfaat layanan terkelola dari Oracle Database @.AWS

> **Note**
>
> Oracle Database@AWS tidak mendukung backup yang dikelola pengguna untuk Autonomous Database pada Infrastruktur Khusus.

Pencadangan yang dikelola pengguna melengkapi solusi cadangan AWS terkelola yang disediakan oleh Oracle Database @.AWS Anda dapat menggunakan cadangan manual untuk persyaratan kepatuhan, pemulihan bencana lintas wilayah, atau integrasi dengan alur kerja manajemen cadangan yang ada.

Anda dapat menggunakan teknik pencadangan yang dikelola pengguna berikut:

Cadangan Aman Oracle

: Streaming backup langsung ke Amazon S3 dengan kinerja optimal.

Storage Gateway

: Gunakan Storage Gateway untuk backup berbasis file yang menggunakan share NFS.

Titik pemasangan S3

: Gunakan klien file untuk memasang bucket Amazon S3 sebagai sistem file lokal.

Prasyarat untuk backup yang dikelola pengguna ke Amazon S3 di Oracle Database @AWS

Sebelum Anda dapat mencadangkan database Oracle Exadata Anda ke Amazon S3, lakukan hal berikut:

1. Aktifkan akses langsung ke Amazon S3 dari jaringan ODB Anda.
2. Konfigurasikan konektivitas jaringan dan perutean antara Oracle Database@ dan Amazon AWS S3.

Mengaktifkan akses dari jaringan ODB Anda ke Amazon S3

Untuk mencadangkan database Anda secara manual ke Amazon S3, aktifkan akses langsung ke S3 dari jaringan ODB Anda. Teknik ini memungkinkan database Anda mengakses Amazon S3 untuk

kebutuhan bisnis Anda, seperti impor/ekspor data atau cadangan yang dikelola pengguna. Anda memiliki kontrol penuh atas tujuan target penyimpanan cadangan dan dapat menggunakan kebijakan untuk membatasi akses ke Amazon S3 menggunakan VPC Lattice.

Akses langsung ke Amazon S3 dari jaringan ODB Anda tidak diaktifkan secara default. Anda dapat mengaktifkan akses S3 saat Anda membuat atau memodifikasi jaringan ODB Anda.

Konsol

Untuk mengaktifkan akses langsung ke Amazon S3 dari jaringan ODB Anda

1. Buka konsol Oracle Database@AWS di. https://console.aws.amazon.com/odb/
2. Di panel navigasi, pilih jaringan ODB.
3. Pilih jaringan ODB yang ingin Anda aktifkan akses Amazon S3.
4. Pilih Ubah.
5. Pilih Amazon S3.
6. (Opsional) Konfigurasikan dokumen kebijakan Amazon S3 untuk mengontrol akses ke Amazon S3. Jika Anda tidak menentukan kebijakan, kebijakan default akan memberikan akses penuh.
7. Pilih Lanjutkan dan kemudian Ubah.

AWS CLI

Untuk mengaktifkan akses Amazon S3 langsung dari jaringan ODB Anda, gunakan `update-odb-network` perintah dengan parameter: `s3-access`

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

Untuk mengonfigurasi dokumen kebijakan Amazon S3, gunakan parameter: `--s3-policy-document`

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

Saat akses Amazon S3 diaktifkan, Anda dapat mengakses Amazon S3 dari jaringan ODB Anda dengan menggunakan DNS regional. `s3.region.amazonaws.com` OCI mengonfigurasi nama DNS

ini secara default. Untuk menggunakan nama DNS kustom, ubah DNS VCN Anda untuk memastikan DNS kustom diselesaikan ke alamat IP titik akhir jaringan layanan.

Mengkonfigurasi konektivitas jaringan antara Oracle AWS Database@ dan Amazon S3

Untuk mengizinkan pencadangan yang dikelola pengguna ke Amazon S3, VM Anda harus dapat mengakses titik akhir VPC Amazon S3. Di konsol OCI, Anda dapat mengedit aturan keamanan di grup keamanan jaringan (NSG) untuk mengontrol lalu lintas masuk dan keluar. Untuk cadangan yang dikelola pengguna, lalu lintas mengalir melalui subnet klien daripada subnet cadangan. Dalam langkah-langkah berikut, Anda memperbarui subnet NSGs untuk klien untuk menambahkan aturan keluar untuk alamat IP titik akhir VPC.

Untuk mengizinkan akses VM ke titik akhir Amazon S3

1. Buka konsol Oracle Database@AWS di. https://console.aws.amazon.com/odb/
2. Pilih jaringan ODB.
3. Pilih nama jaringan ODB.
4. Pilih sumber daya OCI.
5. Pilih tab Integrasi layanan.
6. Di bawah Amazon S3, perhatikan informasi berikut:
   - IPv4 Alamat titik akhir Amazon VPC S3. Anda memerlukan informasi ini nanti. Misalnya, alamat IP mungkin`192.168.12.223`.
   - Nama domain dari titik akhir Amazon VPC S3. Anda memerlukan informasi ini nanti. Misalnya, nama domain mungkin`s3.us-east-1.amazonaws.com`.
7. Di panel navigasi kiri, pilih klaster Exadata VM lalu pilih nama cluster VM Anda.
8. Di bagian atas halaman, pilih tab Ringkasan.
9. Pilih mesin Virtual dan kemudian pilih nama VM Anda.
10. Perhatikan nilai dalam Nama DNS. Ini adalah nama host yang Anda tentukan saat Anda terhubung ke VM Anda menggunakan`ssh`.
11. Di kanan atas, pilih Kelola di OCI. Ini membuka konsol OCI.
12. Pada halaman daftar Virtual Cloud Networks, pilih VCN yang berisi grup keamanan jaringan (NSG) untuk subnet klien jaringan ODB (). `exa_static_nsg` Untuk informasi selengkapnya, lihat Mengelola Aturan Keamanan untuk NSG dalam dokumentasi OCI.
13. Pada halaman detail, lakukan salah satu tindakan berikut tergantung pada opsi yang Anda lihat:

- Pada tab Keamanan, buka Grup Keamanan Jaringan.
- Di bawah Sumber Daya, pilih Grup Keamanan Jaringan.

14. Pilih NSG untuk subnet klien ()`exa_static_nsg`.
15. Tambahkan aturan jalan keluar untuk alamat titik akhir VPC yang Anda catat sebelumnya.

Untuk menguji konektivitas ke S3 dari VM Anda

1. Gunakan `ssh` untuk menghubungkan `root` ke VM yang nama DNSNYA Anda peroleh sebelumnya. Saat Anda terhubung, tentukan `.pem` file dengan kunci SSH Anda.
2. Jalankan perintah berikut untuk memastikan bahwa VM dapat mengakses titik akhir Amazon S3 Amazon VPC. Gunakan nama domain S3 yang Anda catat sebelumnya.

```
# 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
```

Mencadangkan ke Amazon S3 menggunakan Oracle Secure Backup

Oracle Secure Backup bertindak sebagai antarmuka SBT untuk digunakan dengan Recovery Manager (RMAN). Anda dapat menggunakan RMAN dengan Oracle Secure Backup untuk mencadangkan database Oracle Database @ Anda AWS langsung ke Amazon S3. Oracle Secure Backup menawarkan manfaat berikut:

- Oracle Secure Backup mengoptimalkan transfer data antara RMAN dan S3.
- Tidak diperlukan penyimpanan cadangan perantara.
- Oracle Secure Backup mengelola siklus hidup media cadangan Anda.

Untuk mencadangkan ke Amazon S3 menggunakan Oracle Secure Backup

1. Instal modul Oracle Secure Backup di server Exadata VM Anda. Ganti nilai placeholder dengan kunci AWS akses dan kunci akses rahasia Anda. Untuk informasi selengkapnya, lihat dokumentasi Oracle di 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 ke RMAN dan konfigurasikan saluran cadangan dan jenis perangkat default.

```
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. Verifikasi konfigurasi.

```
RMAN> SHOW ALL;
```

4. Cadangkan database.

```
RMAN> BACKUP DATABASE;
```

5. Verifikasi bahwa pencadangan berhasil diselesaikan.

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

Mencadangkan ke Amazon S3 AWS Storage Gateway menggunakan di Amazon EC2

AWS Storage Gateway adalah layanan hybrid yang menghubungkan lingkungan lokal Anda ke layanan AWS Cloud penyimpanan. Untuk AWS backup Oracle Database@, Anda dapat menggunakan Storage Gateway untuk membuat alur kerja cadangan berbasis file yang menulis langsung ke Amazon S3. Tidak seperti teknik Oracle Secure Backup, Anda mengelola siklus hidup backup.

Dalam solusi ini, Anda membuat EC2 instance Amazon terpisah untuk mengonfigurasi Storage Gateway. Anda juga menambahkan volume Amazon EBS untuk menyimpan cache pembacaan dan penulisan ke Amazon S3.

Teknik ini menawarkan manfaat sebagai berikut:

- Anda tidak memerlukan manajer media seperti Oracle Secure Backup.

- Tidak diperlukan penyimpanan cadangan perantara.

Untuk menerapkan Storage Gateway Anda dan membuat file share

1. Buka Konsol Manajemen AWS di https://console.aws.amazon.com/storagegateway/rumah/, dan pilih AWS Wilayah tempat Anda ingin membuat gateway Anda.
2. Menerapkan dan mengaktifkan gateway file Amazon S3, menggunakan instans EC2 Amazon sebagai hub. Ikuti petunjuk di Menerapkan EC2 host Amazon yang disesuaikan untuk S3 File Gateway di Panduan Pengguna Storage Gateway.

   Saat Anda mengonfigurasi gateway file Anda, pastikan Anda melakukan hal berikut:

   - Tambahkan setidaknya satu volume Amazon EBS untuk penyimpanan cache, dengan ukuran minimal 150 GiB.
   - Buka TCP/UDP port 2049 untuk akses NFS di grup keamanan Anda. Ini memungkinkan Anda untuk membuat berbagi file NFS.
   - Buka port TCP 80 untuk lalu lintas masuk untuk memungkinkan akses HTTP satu kali selama aktivasi gateway. Setelah aktivasi, Anda dapat menutup port ini.
3. Buat endpoint Amazon VPC untuk konektivitas pribadi antara jaringan ODB dan Storage Gateway. Untuk informasi selengkapnya, lihat Mengakses AWS layanan menggunakan titik akhir VPC antarmuka.
4. Buat berbagi file untuk bucket Amazon S3 Anda melalui konsol Storage Gateway. Untuk informasi selengkapnya, lihat Membuat berbagi file.

Untuk mencadangkan database Anda ke Amazon S3 menggunakan Storage Gateway

1. Di terminal, gunakan `ssh` untuk menghubungkan ke nama DNS dari Exadata VM. Untuk menemukan nama DNS, lihatPrasyarat untuk backup yang dikelola pengguna ke Amazon S3 di Oracle Database @AWS.
2. Buat direktori di server cluster Exadata VM untuk pemasangan NFS. Contoh berikut membuat direktori `/home/oracle/sgw_mount/`.

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

3. Pasang share NFS di direktori yang baru saja Anda buat. Contoh berikut membuat share pada direktori/home/oracle/sgw_mount/. Ganti *SG-IP-address* dengan alamat IP Storage Gateway Anda dan *your-bucket-name* dengan nama bucket S3 Anda.

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

4. Connect ke RMAN dan backup database ke direktori yang dipasang. Contoh berikut membuat saluran rman_local_bkp dan menggunakan jalur mount point untuk memformat potongan cadangan.

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

5. Verifikasi bahwa file cadangan dibuat di direktori mount. Contoh berikut menunjukkan dua bagian cadangan.

```
$ 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
```

Mencadangkan ke Amazon S3 menggunakan titik pemasangan S3

Anda dapat menggunakan titik pemasangan Amazon S3 untuk membuat cadangan secara lokal terlebih dahulu dan kemudian menyalinnya ke Amazon S3. Teknik ini membuat cadangan pada penyimpanan lokal dan kemudian mentransfernya ke Amazon S3 menggunakan antarmuka mount point. Waktu pencadangan lebih lama daripada teknik lain karena Anda perlu membuat cadangan data dua kali.

> **Note**
>
> Pencadangan langsung ke Amazon S3 menggunakan titik pemasangan, tanpa pementasan, tidak didukung. RMAN memerlukan izin sistem file tertentu yang tidak kompatibel dengan antarmuka titik pemasangan Amazon S3.

Teknik ini tidak mengharuskan Anda untuk melisensikan manajer media seperti Oracle Secure Backup. Anda mengelola siklus hidup backup Anda.

Untuk mencadangkan ke Amazon S3 menggunakan titik pemasangan S3

1. Di terminal, gunakan `ssh` untuk menghubungkan ke nama DNS dari Exadata VM. Untuk menemukan nama DNS, lihatPrasyarat untuk backup yang dikelola pengguna ke Amazon S3 di Oracle Database @AWS.
2. Instal titik pemasangan Amazon S3 di server cluster Exadata VM. Untuk informasi selengkapnya tentang penginstalan dan konfigurasi, lihat Mountpoint untuk Amazon S3 di Panduan Pengguna Amazon S3.

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

3. Verifikasi instalasi dengan menjalankan `mount-s3` perintah.

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

4. Buat direktori cadangan perantara di penyimpanan lokal server cluster Exadata VM. Anda akan mencadangkan database Anda ke direktori lokal ini dan kemudian menyalin cadangan ke bucket S3 Anda. Contoh berikut menciptakan direktori`/u02/rman_bkp_local`.

   ```
   mkdir /u02/rman_bkp_local
   ```

5. Buat direktori untuk titik pemasangan Amazon S3. Contoh berikut menciptakan direktori`/home/oracle/s3mount`.

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

6. Pasang bucket Amazon S3 Anda menggunakan titik pemasangan. Contoh berikut memasang bucket S3 pada direktori. `/home/oracle/s3mount` Ganti *`your-s3-bucket-name`* dengan nama bucket Amazon S3 Anda yang sebenarnya.

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

7. Pastikan Anda dapat mengakses konten bucket Amazon S3.

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

8. Connect RMAN ke database target Anda dan cadangkan ke direktori pementasan lokal Anda. Contoh berikut membuat saluran `rman_local_bkp` dan menggunakan jalur `/u02/rman_bkp_local/` untuk memformat potongan cadangan.

```
$ rman TARGET /

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

9. Verifikasi bahwa cadangan dibuat di direktori lokal:

```
$ 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. Salin file cadangan dari direktori staging lokal ke titik pemasangan Amazon S3.

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

11. Verifikasi bahwa Anda berhasil menyalin file ke Amazon S3.

```
$ 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
```

Menonaktifkan akses langsung ke Amazon S3

Jika Anda tidak lagi memerlukan akses langsung ke Amazon S3 dari jaringan ODB Anda, Anda dapat menonaktifkannya. Mengaktifkan atau menonaktifkan akses jaringan langsung ke S3 tidak memengaruhi akses jaringan ke cadangan terkelola Oracle ke Amazon S3.

Konsol

Untuk menonaktifkan akses langsung ke Amazon S3

1. Buka konsol Oracle Database@AWS di. https://console.aws.amazon.com/odb/
2. Di panel navigasi, pilih jaringan ODB.
3. Pilih jaringan ODB yang ingin Anda nonaktifkan akses Amazon S3.
4. Pilih Ubah.
5. Kosongkan kotak centang Aktifkan akses S3.
6. Pilih Ubah jaringan ODB.

AWS CLI

Gunakan `update-odb-network` perintah dengan `s3-access` parameter.

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

Memecahkan masalah integrasi Amazon S3

Jika Anda mengalami masalah dengan cadangan terkelola Oracle ke Amazon S3 atau akses langsung ke Amazon S3, pertimbangkan langkah-langkah pemecahan masalah berikut:

Tidak dapat mengakses Amazon S3 dari database Anda

Periksa hal-hal berikut:

- Verifikasi bahwa akses Amazon S3 diaktifkan untuk jaringan ODB Anda. Gunakan `GetOdbNetwork` tindakan untuk memeriksa apakah `s3Access` statusnya`Enabled`.
- Pastikan Anda menggunakan nama DNS regional yang benar: `s3.region.amazonaws.com`
- Periksa apakah database Oracle Anda memiliki izin yang diperlukan untuk mengakses Amazon S3.

Pencadangan terkelola Oracle gagal

Periksa hal-hal berikut:

- Pencadangan terkelola Oracle ke Amazon S3 diaktifkan secara default dan tidak dapat dinonaktifkan. Jika backup gagal, periksa log database Oracle untuk pesan kesalahan tertentu.

- Verifikasi bahwa sumber daya Amazon VPC Lattice dikonfigurasi dengan benar dengan melihat sumber daya integrasi layanan.
- Hubungi Oracle Support untuk bantuan dengan masalah backup otomatis terkelola Oracle. Lihat informasi yang lebih lengkap di Mendapatkan dukungan untuk Oracle Database @AWS.

Database Oracle@ Integrasi AWS nol-ETL dengan Amazon Redshift

Integrasi nol-ETL adalah solusi yang dikelola sepenuhnya yang membuat data transaksional dan operasional tersedia di Amazon Redshift dari berbagai sumber. Dengan solusi ini, Anda dapat mereplikasi data ke Amazon Redshift dari database Oracle Anda yang berjalan di Oracle Exadata atau Autonomous Database pada Infrastruktur Exadata Khusus. Sinkronisasi otomatis menghindari proses ekstrak, transformasi, dan beban (ETL) tradisional. Ini juga memungkinkan analitik real-time dan beban kerja AI. Untuk informasi selengkapnya, lihat Integrasi nol-ETL di Panduan Manajemen Pergeseran Merah Amazon.

Integrasi nol-ETL memberikan manfaat sebagai berikut:

- Replikasi data real-time - Sinkronisasi data berkelanjutan dari database Oracle ke Amazon Redshift dengan latensi minimal
- Penghapusan jaringan pipa ETL yang kompleks - Tidak perlu membangun dan memelihara solusi integrasi data khusus
- Mengurangi overhead operasional - Pengaturan dan manajemen otomatis melalui AWS APIs
- Arsitektur integrasi data yang disederhanakan - Integrasi mulus antara Oracle Database AWS @ dan layanan analitik AWS
- Keamanan yang ditingkatkan - Enkripsi bawaan dan AWS kontrol akses IAM

Amazon Redshift tidak mengenakan biaya tambahan untuk integrasi nol-ETL dengan Oracle Database@.AWS Anda membayar sumber daya Amazon Redshift yang ada yang digunakan untuk membuat dan memproses data perubahan yang dibuat sebagai bagian dari integrasi Nol-ETL. Untuk informasi selengkapnya, lihat harga Amazon Redshift.

Versi database yang didukung untuk integrasi nol-ETL di Oracle Database @AWS

Integrasi nol-ETL mendukung versi database Oracle berikut:

- Oracle Exadata - Database Oracle 19c
- Database Otonom pada Infrastruktur Khusus - Oracle Database 19c dan 23ai

Bagaimana integrasi nol-ETL bekerja di Oracle Database @AWS

Integrasi nol-ETL memungkinkan Oracle Database@ untuk mereplikasi AWS data ke Amazon Redshift. Integrasi ini memanfaatkan Amazon VPC Lattice untuk menciptakan konektivitas jaringan yang aman. Teknologi Change Data Capture (CDC) memastikan sinkronisasi data real-time. Anda mengelola integrasi melalui AWS Glue APIs.

Arsitektur integrasi nol-ETL meliputi:

- Konektivitas aman — Menggunakan SSL/TLS enkripsi melalui port TLS 2484 untuk transfer data
- AWS Secrets Manager - Menyimpan kredensyal database dan sertifikat dengan aman menggunakan Layanan Manajemen Kunci AWS
- AWS Integrasi Glue - Menyediakan antarmuka manajemen terpadu untuk integrasi nol-ETL

Replikasi berlangsung melalui langkah-langkah berikut:

1. Membangun koneksi aman ke database Oracle menggunakan SSL pada port 2484
2. Melakukan dump penuh awal dari database, skema, dan tabel yang dipilih
3. Menyiapkan pengambilan data perubahan (CDC) untuk replikasi real-time yang sedang berlangsung
4. Menulis data yang direplikasi ke cluster Amazon Redshift target

> **Important**
>
> Integrasi nol-ETL tidak diaktifkan secara default. Anda harus mengkonfigurasinya menggunakan AWS Glue APIs. Anda tidak dapat mengatur integrasi nol-ETL secara langsung menggunakan Oracle Database @.AWS APIs

Prasyarat untuk integrasi nol-ETL di Oracle Database @AWS

Sebelum menyiapkan integrasi nol-ETL, pastikan Anda memenuhi prasyarat berikut.

Prasyarat umum

- AWS Pengaturan Oracle Database@ - Pastikan Anda memiliki setidaknya satu cluster VM yang disediakan dan berjalan.
- Integrasi dengan Zero-ETL diaktifkan - Pastikan cluster VM atau cluster VM Autonomous Anda dikaitkan dengan jaringan ODB yang mengaktifkan nol-ETL.
- Versi Oracle Database yang didukung - Anda harus menggunakan Oracle Database 19c (Oracle Exadata) atau Oracle Database 19c/23ai (Autonomous Database on Dedicated Infrastructure).
- AWS Wilayah yang Sama — Database Oracle sumber dan kluster Amazon Redshift target harus berada di Wilayah yang AWS sama.

Prasyarat basis data Oracle

Anda harus mengkonfigurasi database Oracle Anda dengan pengaturan berikut.

Penyiapan pengguna replikasi

Buat pengguna replikasi khusus di setiap database pluggable (PDB) yang ingin Anda tiru:

- Untuk Oracle Exadata — Buat pengguna `ODBZEROETLADMIN` dengan kata sandi yang aman.
- Untuk Database Otonom pada Infrastruktur Khusus - Gunakan `GGADMIN` pengguna yang ada.

Berikan izin berikut kepada pengguna replikasi.

```
-- 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";
```

Penebangan tambahan

Aktifkan pencatatan tambahan pada database Oracle Anda untuk menangkap data perubahan.

```
-- 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;
```

Untuk mengatur integrasi nol-ETL antara Oracle Database@ dan AWS Amazon Redshift, Anda harus mengonfigurasi SSL.

Untuk database Oracle Exadata

Anda harus mengkonfigurasi SSL secara manual pada port 2484. Tugas ini melibatkan hal-hal berikut:

- Mengkonfigurasi di `(PROTOCOL=tcps)(PORT=2484)` `listener.ora`
- Menyiapkan dompet menggunakan `sqlnet.ora`
- Membuat dan mengonfigurasi sertifikat SSL (lihat Cara Mengkonfigurasi SSL/TCPS Untuk Exadata Cloud Database (ExACC/Exacs) (Doc ID 2947301.1) dalam dokumentasi Dukungan Oracle Saya)

Untuk Database Otonom

SSL pada port 2484 diaktifkan secara default. Tidak diperlukan konfigurasi tambahan.

> **Important**
>
> Port SSL ditetapkan sebagai 2484.

AWS prasyarat layanan

Sebelum menyiapkan integrasi nol-ETL, siapkan Secrets Manager dan konfigurasikan AWS izin IAM.

Mengatur AWS Secrets Manager

Simpan kredensi database Oracle Anda di AWS Secrets Manager sebagai berikut:

1. Buat Customer Managed Key (CMK) di Layanan Manajemen AWS Kunci.
2. Simpan kredensi database di AWS Secrets Manager menggunakan CMK.
3. Konfigurasikan kebijakan sumber daya untuk mengizinkan akses Oracle Database@AWS .

Untuk mendapatkan ID kunci dan kata sandi TDE Anda, gunakan teknik yang dijelaskan dalam metode enkripsi yang didukung untuk menggunakan Oracle sebagai sumber untuk AWS Database Migration Service. Perintah berikut menghasilkan dompet base64.

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

Contoh berikut menunjukkan rahasia untuk Oracle Exadata. Untuk*asm_service_name*, *111.11.11.11* mewakili IP virtual untuk node VM. Anda juga dapat mendaftarkan pendengar ASM dengan SCAN.

```
{
  "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"
  }
}
```

Contoh berikut menunjukkan rahasia untuk 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"
    }
  ]
}
```

Mengonfigurasi izin IAM

Buat kebijakan IAM yang memungkinkan operasi integrasi nol-ETL. Contoh kebijakan berikut memungkinkan mendeskripsikan, membuat, memperbarui, dan menghapus operasi untuk klaster Exadata VM. Untuk cluster VM Autonomous, gunakan nilai `cloud-autonomous-vm-cluster` bukan `cloud-vm-cluster` untuk ARN sumber daya.

Pertimbangan untuk integrasi nol-ETL di Oracle Database @AWS

Saat menyiapkan integrasi nol-ETL antara dan Amazon Oracle Database@AWS Redshift, pertimbangkan pedoman berikut:

Waktu muat data awal

Waktu muat penuh awal tergantung pada ukuran database Anda. Database besar mungkin membutuhkan waktu beberapa jam atau hari untuk menyelesaikan sinkronisasi awal.

Kinerja database Oracle

Perubahan pengambilan data dapat memengaruhi kinerja database Oracle, terutama selama volume transaksi yang tinggi. Setelah mengaktifkan integrasi nol-ETL, pantau kinerja database Anda.

Perubahan skema

Perubahan Data Definition Language (DDL) dalam database Oracle sumber mungkin mengharuskan Anda untuk melakukan intervensi secara manual untuk membuat ulang integrasi. Rencanakan perubahan skema dengan hati-hati.

Untuk pertimbangan umum, lihat Pertimbangan saat menggunakan integrasi Nol-ETL dengan Amazon Redshift.

Batasan untuk integrasi nol-ETL di Oracle Database @AWS

Perhatikan batasan umum berikut:

PDB tunggal per integrasi

Setiap integrasi nol-ETL hanya dapat mereplikasi data dari satu database pluggable (PDB). Filter data seperti `include: pdb1.*.*, include: pdb2.*.*` tidak didukung.

Integrasi tunggal per Database Otonom atau Infrastruktur Exadata

Setiap integrasi nol-ETL hanya dapat mereplikasi data dari satu Database Otonom pada Infrastruktur Khusus.

Port SSL tetap

Koneksi SSL harus menggunakan port 2484.

Persyaratan Wilayah yang Sama

Cluster sumber Oracle Database@AWS VM dan target cluster Amazon Amazon Redshift harus berada di Wilayah yang sama. AWS Replikasi lintas wilayah tidak didukung.

Tidak ada dukungan mTLS

Mutual TLS (mTLS) tidak didukung. Jika database OCI Anda mengaktifkan mTL, Anda harus menonaktifkannya untuk menggunakan integrasi nol-ETL.

Pengaturan integrasi yang tidak dapat diubah

Setelah Anda membuat kunci ARN atau KMS rahasia yang terkait dengan integrasi, Anda tidak dapat memodifikasinya. Anda harus menghapus dan membuat ulang integrasi untuk mengubah pengaturan ini.

Enkripsi tingkat kolom TDE

Enkripsi Data Transparan (TDE) tingkat kolom tidak didukung untuk database Oracle Exadata. Hanya TDE tingkat tablespace yang didukung.

Dukungan tipe data

Beberapa tipe data khusus Oracle mungkin tidak sepenuhnya didukung atau mungkin memerlukan transformasi selama replikasi. Uji tipe data spesifik Anda secara menyeluruh sebelum Anda menyebarkan database Anda ke produksi.

Menyiapkan AWS integrasi Oracle Database@ dengan Amazon Redshift

Untuk mengatur integrasi nol-ETL antara database Oracle dan Amazon Redshift, selesaikan langkah-langkah berikut:

1. Aktifkan Nol-ETL di jaringan ODB Anda.
2. Konfigurasikan prasyarat database Oracle.
3. Siapkan AWS Secrets Manager dan AWS Key Management Service.
4. Konfigurasikan izin IAM.
5. Siapkan kebijakan sumber daya Amazon Redshift.
6. Buat integrasi nol-ETL.
7. Buat database target di Amazon Redshift.

Langkah 1: Aktifkan nol-ETL untuk jaringan ODB Anda

Anda dapat mengaktifkan integrasi nol-ETL untuk jaringan ODB yang terkait dengan cluster VM sumber Anda. Secara default, integrasi ini dinonaktifkan.

Konsol

Untuk mengaktifkan integrasi nol-ETL

1. Buka konsol Oracle Database@AWS di. https://console.aws.amazon.com/odb/
2. Di panel navigasi, pilih jaringan ODB.
3. Pilih jaringan ODB yang ingin Anda aktifkan integrasi nol-ETL.
4. Pilih Ubah.
5. Pilih Nol-ETL.
6. Pilih Lanjutkan dan kemudian Ubah.

AWS CLI

Untuk mengaktifkan integrasi nol-ETL, gunakan `update-odb-network` perintah dengan parameter: `--zero-etl-access`

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

Untuk mengaktifkan integrasi nol-ETL untuk jaringan ODB yang terkait dengan cluster VM sumber Anda, gunakan perintah. `update-odb-network` Perintah ini mengkonfigurasi infrastruktur jaringan yang diperlukan untuk integrasi nol-ETL.

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

Langkah 2: Konfigurasikan database Oracle Anda

Lengkapi konfigurasi database Oracle seperti yang dijelaskan dalam Prasyarat:

- Buat pengguna replikasi dan berikan izin yang diperlukan.
- Aktifkan log redo yang diarsipkan.
- Konfigurasikan SSL (hanya Oracle Exadata).
- Siapkan pengguna ASM jika berlaku (hanya Oracle Exadata).

Langkah 3: Siapkan AWS Secrets Manager dan AWS Key Management Service

Buat Customer Managed Key (CMK) dan simpan kredensi database Anda.

1. Buat CMK di Layanan Manajemen AWS Kunci menggunakan `create-key` perintah.

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

2. Simpan kredensi database Anda di 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. Lampirkan kebijakan sumber daya ke rahasia untuk mengizinkan akses Oracle Database@AWS .

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

Pada perintah sebelumnya, `secret-resource-policy.json` berisi JSON berikut.

JSON

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

4. Lampirkan kebijakan sumber daya ke CMK. Kebijakan sumber daya CMK harus menyertakan izin untuk prinsipal layanan Oracle Database@ dan prinsipal AWS layanan Amazon Redshift untuk mendukung integrasi nol-ETL terenkripsi.

```
aws kms put-key-policy \
```

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

`cmk-resource-policy.json`File harus menyertakan pernyataan kebijakan berikut. Pernyataan pertama memungkinkan akses AWS layanan Oracle Database@, dan pernyataan kedua memungkinkan Amazon Redshift untuk membuat hibah pada kunci KMS untuk operasi data terenkripsi.

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"
          ]
        }
      }
    }
  ]
}
```

Langkah 4: Konfigurasikan izin IAM

Buat dan lampirkan kebijakan IAM yang memungkinkan operasi integrasi nol-ETL.

```
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
```

Kebijakan berikut memberikan izin yang diperlukan.

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": "*"
    }
  ]
}
```

Langkah 5: Konfigurasikan kebijakan sumber daya Amazon Redshift

Siapkan kebijakan sumber daya di klaster Amazon Redshift Anda untuk mengotorisasi integrasi masuk.

```
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**
>
> Atau, Anda dapat menggunakan opsi Perbaiki untuk saya di AWS konsol. Opsi ini secara otomatis mengonfigurasi kebijakan Amazon Redshift yang diperlukan tanpa Anda perlu melakukannya secara manual.

Langkah 6: Buat integrasi nol-ETL menggunakan AWS Glue

Buat integrasi nol-ETL menggunakan perintah. AWS Glue `create-integration` Dalam perintah ini, Anda menentukan cluster VM sumber dan namespace Amazon Redshift target.

Contoh berikut membuat integrasi dengan PDB bernama `pdb1` berjalan di cluster Exadata VM. Anda juga dapat membuat cluster VM otonom dengan mengganti `cloud-vm-cluster` dengan `cloud-autonomous-vm-cluster` ARN sumber. Menentukan kunci KMS adalah opsional. Jika Anda menentukan kunci, itu bisa berbeda dari yang Anda buatLangkah 3: Siapkan AWS Secrets Manager dan AWS Key Management Service.

```
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"
```

Perintah mengembalikan ARN integrasi dan menetapkan status ke. `creating` Anda dapat memantau status integrasi menggunakan `describe-integrations` perintah.

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

> **Important**
>
> Hanya satu PDB per integrasi yang didukung. Filter data harus menentukan satu PDB, misalnya,`include: pdb1.*.*`. Sumber harus berada di AWS Wilayah dan akun yang sama di mana integrasi sedang dibuat.

Langkah 7: Buat database target di Amazon Redshift

Setelah integrasi aktif, buat database target di cluster Amazon Redshift Anda.

```
-- 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";
```

Setelah membuat database target, Anda dapat menanyakan data yang direplikasi.

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

-- Connect to the new database
\c target_database_name

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

Verifikasi integrasi nol-ETL

Verifikasi bahwa integrasi berfungsi dengan menanyakan status integrasi AWS Glue dan memastikan bahwa perubahan Oracle Anda direplikasi ke Amazon Redshift.

Untuk memverifikasi bahwa integrasi nol-ETL Anda berfungsi dengan benar

1. Periksa status integrasi.

```
aws glue describe-integrations \
```

```
  --integration-identifier integration-id
```

Statusnya harus `ACTIVE` atau`REPLICATING`.

2. Verifikasi replikasi data dengan membuat perubahan dalam database Oracle Anda dan memeriksa apakah mereka muncul di Amazon Redshift.
3. Pantau metrik replikasi di Amazon CloudWatch (jika tersedia).

Pemfilteran data untuk integrasi nol-ETL di Oracle Database@AWS

Oracle Database@AWS Integrasi nol-ETL mendukung penyaringan data. Anda dapat menggunakannya untuk mengontrol data mana yang direplikasi oleh database Oracle Exadata sumber Anda ke gudang data target Anda. Alih-alih mereplikasi seluruh database, Anda dapat menerapkan satu atau beberapa filter untuk secara selektif menyertakan atau mengecualikan tabel tertentu. Ini membantu Anda mengoptimalkan kinerja penyimpanan dan kueri dengan memastikan bahwa hanya data yang relevan yang ditransfer. Pemfilteran terbatas pada tingkat database dan tabel. Pemfilteran tingkat kolom dan baris tidak didukung.

Oracle Database dan Amazon Redshift menangani casing nama objek secara berbeda, yang memengaruhi konfigurasi filter data dan kueri target. Perhatikan hal-hal berikut:

- Oracle Database menyimpan database, skema, dan nama objek dalam huruf besar kecuali secara eksplisit dikutip dalam pernyataan. `CREATE` Misalnya, jika Anda membuat `mytable` (tanpa tanda kutip), kamus data Oracle menyimpan nama tabel sebagai`MYTABLE`. Jika Anda mengutip nama objek dalam pernyataan pembuatan Anda, kamus data Oracle mempertahankan kasus ini.
- Filter data nol-ETL peka huruf besar/kecil dan harus sesuai dengan kasus nama objek yang tepat seperti yang muncul di kamus data Oracle. Misalnya, jika kamus Oracle menyimpan skema dan nama tabel`REINVENT.MYTABLE`, maka buat filter menggunakan. `include: ORCL.REINVENT.MYTABLE`
- Amazon Redshift menanyakan default ke nama objek huruf kecil kecuali dikutip secara eksplisit. Misalnya, kueri `MYTABLE` (tanpa tanda kutip) mencari`mytable`.

Perhatikan perbedaan kasus saat Anda membuat filter Amazon Redshift dan menanyakan datanya. Pertimbangan penyaringan untuk Oracle Database@AWS sama dengan Amazon RDS for Oracle. Untuk contoh bagaimana kasus dapat memengaruhi filter data dalam database Oracle, lihat contoh RDS untuk Oracle di Panduan Pengguna Layanan Amazon Relational Database Service.

Memantau integrasi nol-ETL

Pemantauan reguler integrasi nol-ETL Anda memastikan kinerja optimal dan membantu mengidentifikasi masalah lebih awal.

Pemantauan status integrasi

Pantau status integrasi nol-ETL Anda menggunakan 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
```

Status integrasi meliputi:

- membuat - Integrasi sedang diatur
- aktif — Integrasi berjalan dan mereplikasi data
- memodifikasi - Konfigurasi integrasi sedang diperbarui
- needs_attention - Integrasi membutuhkan intervensi manual
- gagal - Integrasi mengalami kesalahan
- menghapus - Integrasi sedang dihapus

Pemantauan kinerja

Pantau aspek-aspek berikut dari kinerja integrasi nol-ETL Anda:

- Replikasi lag - Perbedaan waktu antara saat perubahan terjadi di Oracle dan saat muncul di Amazon Redshift
- Data throughput — Volume data yang direplikasi per unit waktu
- Tingkat kesalahan — Frekuensi kesalahan replikasi atau kegagalan
- Pemanfaatan sumber daya — CPU, memori, dan penggunaan jaringan pada sistem sumber dan target

Gunakan Amazon CloudWatch untuk memantau metrik ini dan mengatur alarm untuk ambang batas kritis.

Mengelola integrasi nol-ETL di Oracle Database@AWS

Setelah membuat integrasi nol-ETL, Anda dapat melakukan berbagai operasi manajemen termasuk memodifikasi dan menghapus integrasi. Bagian ini mencakup manajemen berkelanjutan dari integrasi nol-ETL Anda.

Memodifikasi integrasi nol-ETL

Anda hanya dapat memodifikasi nama, deskripsi, dan opsi pemfilteran data untuk integrasi nol-ETL di gudang data yang didukung. Anda tidak dapat mengubah AWS kunci Layanan Manajemen Kunci yang digunakan untuk mengenkripsi integrasi, atau basis data sumber atau target.

Prasyarat untuk memodifikasi integrasi

Sebelum Anda memodifikasi integrasi nol-ETL, pastikan Anda memiliki yang berikut:

- Izin yang diperlukan - Pengguna atau peran IAM Anda harus memiliki `odb:UpdateOutboundIntegration` izin selain izin standar AWS Glue .
- Integrasi dalam keadaan aktif — Integrasi harus dalam `ACTIVE` keadaan, bukan dalam`CREATING`,`MODIFYING`,`DELETING`, atau`FAILED`.
- Sintaks filter data yang valid - Filter data baru harus mengikuti sintaks include/exclude pola yang didukung.

Memodifikasi filter data

Anda dapat mengubah tabel atau skema mana yang direplikasi dengan memodifikasi filter data. Dengan cara ini, Anda dapat menambah atau menghapus objek database dari replikasi tanpa membuat ulang seluruh integrasi.

Untuk memodifikasi filter data untuk integrasi, gunakan `modify-integration` perintah.

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

Anda juga dapat memodifikasi nama dan deskripsi integrasi secara bersamaan. Dalam contoh berikut, Anda memodifikasi nama integrasi, deskripsi, dan filter untuk dua skema. 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

Saat Anda memodifikasi filter data, integrasi memasuki `modifying` status dan melakukan sinkronisasi ulang data. Integrasi menghentikan replikasi, menerapkan pengaturan filter baru, dan melanjutkan replikasi dengan operasi reload-target. Pantau status integrasi untuk memastikan modifikasi selesai dengan sukses.

Pertimbangan untuk modifikasi filter data ke integrasi nol-ETL

Pertimbangkan hal berikut saat memodifikasi filter data:

- Batasan PDB tunggal - Anda hanya dapat menentukan satu database pluggable (PDB) per integrasi. Filter data seperti `include: pdb1.*.*, include: pdb2.*.*` tidak didukung
- Gangguan replikasi — Replikasi data berhenti selama proses modifikasi dan dilanjutkan setelah filter baru diterapkan.
- Muat ulang data — Integrasi melakukan pemuatan ulang data penuh yang sesuai dengan kriteria filter baru.
- Dampak kinerja — Perubahan filter data yang besar mungkin membutuhkan waktu yang signifikan untuk diselesaikan dan dapat memengaruhi kinerja basis data sumber selama pemuatan ulang.

Batasan untuk modifikasi pengaturan integrasi nol-ETL

Anda tidak dapat mengubah pengaturan berikut setelah membuat integrasi nol-ETL:

- Rahasia ARN - AWS Rahasia Secrets Manager yang berisi kredensil database
- Kunci KMS — Kunci terkelola pelanggan yang digunakan untuk enkripsi
- Sumber ARN - Basis Data Oracle@ Kluster VM AWS

- Target ARN - Cluster atau namespace Amazon Redshift

Untuk mengubah pengaturan ini, hapus integrasi nol-ETL yang ada dan buat yang baru.

Menghapus integrasi nol-ETL

Bila Anda tidak lagi memerlukan integrasi nol-ETL, Anda dapat menghapusnya untuk menghentikan replikasi dan membersihkan sumber daya terkait.

Penghapusan menggunakan Glue AWS

Hapus integrasi nol-ETL menggunakan Glue API. AWS

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

Anda dapat menghapus integrasi dalam status berikut:

- aktif
- kebutuhan_perhatian
- gagal
- sinkronisasi

Efek penghapusan

Saat Anda menghapus integrasi nol-ETL, pertimbangkan efek berikut:

Replikasi berhenti.

Oracle Database@AWS tidak mereplikasi perubahan baru dari Amazon Redshift.

Data yang ada dipertahankan.

Data yang sudah direplikasi ke Amazon Redshift tetap tersedia.

Database target tetap ada.

Basis data Amazon Redshift yang dibuat dari integrasi tidak dihapus secara otomatis.

> **Important**
>
> Penghapusan tidak dapat diubah. Jika Anda perlu melanjutkan replikasi setelah penghapusan, buat integrasi baru, yang melakukan beban awal penuh.

Praktik terbaik untuk manajemen nol-ETL

Ikuti praktik terbaik ini untuk memastikan kinerja, keamanan, dan efektivitas biaya yang optimal dari integrasi nol-ETL Anda.

Praktik terbaik operasional

Praktik operasional ini membantu mempertahankan integrasi nol-ETL yang andal dan efisien.

Pemantauan rutin

: Siapkan CloudWatch alarm untuk memantau metrik kesehatan dan kinerja integrasi.

Rotasi kredensi

: Putar kata sandi database secara teratur dan perbarui di AWS Secrets Manager.

Verifikasi Backup

: Verifikasi secara teratur bahwa backup database Oracle Anda mencakup komponen yang diperlukan untuk pemulihan bencana.

Pengujian kinerja

: Uji dampak integrasi nol-ETL pada kinerja database Oracle Anda, terutama selama periode penggunaan puncak.

Perencanaan perubahan skema

: Merencanakan dan menguji perubahan skema dalam lingkungan pengembangan sebelum menerapkannya pada produksi.

Praktik terbaik keamanan

Terapkan langkah-langkah keamanan ini untuk melindungi integrasi dan data nol-ETL Anda.

Akses hak istimewa paling sedikit

Berikan hanya izin minimum yang diperlukan untuk pengguna replikasi dan peran AWS IAM.

Keamanan jaringan

Gunakan grup keamanan dan NACLs untuk membatasi akses jaringan hanya ke port dan sumber yang diperlukan.

Enkripsi saat diam

Pastikan database Oracle dan cluster Amazon Redshift menggunakan enkripsi saat istirahat.

Pencatatan audit

Aktifkan pencatatan audit di Oracle dan Amazon Redshift untuk melacak akses dan perubahan data.

Manajemen rahasia

Gunakan fitur rotasi otomatis AWS Secrets Manager jika memungkinkan.

Optimalisasi biaya

Terapkan strategi ini untuk mengoptimalkan biaya sambil mempertahankan kinerja integrasi nol-ETL yang efektif.

Pemfilteran data

Gunakan filter data yang tepat untuk mereplikasi hanya data yang Anda butuhkan, mengurangi biaya penyimpanan dan komputasi.

Optimalisasi Amazon Redshift

Gunakan jenis node Amazon Redshift yang sesuai dan terapkan kompresi data untuk mengoptimalkan biaya.

Pemantauan penggunaan

Tinjau secara teratur penggunaan dan biaya integrasi nol-ETL Anda melalui Cost Explorer. AWS

Membersihkan integrasi yang tidak digunakan

Hapus integrasi yang tidak lagi diperlukan untuk menghindari tagihan yang sedang berlangsung.

Pemecahan masalah integrasi nol-ETL

Bagian ini memberikan panduan untuk menyelesaikan masalah umum dengan integrasi nol-ETL.

Kegagalan pengaturan integrasi nol-ETL

Kegagalan otentikasi

- Verifikasi bahwa pengguna replikasi ada dan memiliki kata sandi yang benar di AWS Secrets Manager.
- Pastikan bahwa semua izin yang diperlukan telah diberikan kepada pengguna replikasi.
- Periksa apakah ARN rahasia sudah benar dan dapat diakses oleh Oracle Database @.AWS
- Verifikasi bahwa kebijakan sumber daya CMK memungkinkan akses oleh Oracle AWS Database@ service principal.

Masalah konektivitas jaringan

- Pastikan jaringan ODB Anda mengaktifkan integrasi nol-ETL.
- Verifikasi bahwa SSL dikonfigurasi dengan benar pada port 2484 (hanya Exadata).
- Periksa apakah pendengar database Oracle berjalan dan menerima koneksi.
- Pastikan bahwa kelompok keamanan jaringan dan NACLs memungkinkan lalu lintas pada port 2484.
- Verifikasi bahwa nama layanan dalam rahasia Anda cocok dengan nama layanan Oracle yang sebenarnya.

Kesalahan izin

- Periksa apakah pengguna atau peran IAM Anda memiliki izin yang diperlukan untuk operasi AWS Glue integrasi.
- Verifikasi bahwa kebijakan sumber daya Amazon Redshift memungkinkan integrasi masuk dari klaster VM Anda.
- Pastikan bahwa Oracle Database@AWS telah diberikan akses ke rahasia dan AWS kunci Layanan Manajemen Kunci Anda.

Masalah replikasi

Kegagalan beban awal

- Verifikasi bahwa database Oracle memiliki sumber daya yang cukup untuk mendukung operasi beban penuh.

- Pastikan bahwa logging tambahan diaktifkan pada database sumber.
- Periksa kunci atau kendala tingkat tabel yang mungkin mencegah ekstraksi data.

Ubah masalah pengambilan data

- Verifikasi bahwa database Oracle memiliki ruang redo log dan retensi yang memadai.
- Periksa apakah pengguna replikasi memiliki akses ke log redo yang diarsipkan.
- Untuk sistem yang mendukung ASM, pastikan bahwa pengguna ASM dikonfigurasi dengan benar.
- Pantau kinerja database Oracle untuk memastikan CDC tidak menyebabkan perselisihan sumber daya.

Kelambatan replikasi tinggi

- Pantau metrik lag replikasi di. CloudWatch
- Periksa volume transaksi tinggi atau transaksi besar di database sumber.
- Verifikasi bahwa klaster Amazon Redshift memiliki kapasitas yang memadai untuk menangani data yang masuk.

Masalah konsistensi data

Data yang hilang atau tidak lengkap

- Verifikasi bahwa filter data mencakup semua skema dan tabel yang diperlukan.
- Periksa tipe data yang tidak didukung yang mungkin menyebabkan kegagalan replikasi.
- Pastikan bahwa pengguna replikasi memiliki izin SELECT pada semua tabel yang diperlukan.

Kesalahan konversi tipe data

- Tinjau pemetaan tipe data yang didukung antara Oracle dan Redshift.
- Periksa tipe data khusus Oracle yang mungkin memerlukan penanganan khusus.
- Pertimbangkan untuk memodifikasi skema Oracle Anda untuk menggunakan tipe data yang lebih kompatibel.

Pemantauan dan debugging

Gunakan pendekatan berikut untuk memantau dan men-debug masalah integrasi Zero-ETL:

- Pemantauan status integrasi - Secara teratur memeriksa status integrasi menggunakan`aws glue describe-integrations`.

- CloudWatch metrik — Pantau CloudWatch metrik yang tersedia untuk kinerja replikasi dan kesalahan.
- Pemantauan database Oracle - Memantau kinerja database Oracle dan pemanfaatan sumber daya.
- Pemantauan Redshift — Pantau kinerja klaster Amazon Redshift dan pemanfaatan penyimpanan.

Untuk masalah kompleks yang tidak dapat diselesaikan menggunakan panduan pemecahan masalah ini, hubungi AWS Dukungan dengan informasi berikut:

- Integrasi ARN dan status saat ini.
- Pesan kesalahan dari integrasi menggambarkan operasi.
- Database Oracle dan konfigurasi cluster Amazon Redshift.
- Garis waktu kapan masalah mulai terjadi.

Keamanan di Oracle Database@AWS

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS, OCI, dan Anda. Model tanggung jawab bersama menggambarkan hal ini sebagai keamanan dari cloud dan keamanan di dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang berjalan Layanan AWS di dalamnya AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi keefektifan keamanan kami sebagai bagian dari program kepatuhan AWS.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor-faktor lain, termasuk sensitivitas data Anda, persyaratan organisasi Anda, dan hukum dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama model saat menggunakan Oracle Database@AWS. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan Oracle Database@AWS sumber daya Anda.

Anda dapat mengelola akses ke Oracle Database@AWS sumber daya Anda. Metode yang Anda gunakan untuk mengelola akses tergantung pada jenis tugas yang perlu Anda lakukan dengan Oracle Database@AWS:

- Gunakan kebijakan AWS Identity and Access Management (IAM) untuk menetapkan izin yang menentukan siapa yang diizinkan mengelola sumber daya. Oracle Database@AWS Misalnya, Anda dapat menggunakan IAM untuk menentukan siapa yang diizinkan untuk membuat, mendeskripsikan, memodifikasi, dan menghapus infrastruktur Exadata, klaster VM, atau sumber daya tag.
- Gunakan fitur keamanan mesin database Oracle Anda untuk mengontrol siapa yang dapat masuk ke database pada instans DB. Fitur ini berfungsi seolah-olah basis data berada di jaringan lokal Anda.

- Gunakan koneksi Secure Socket Layers (SSL) atau Transport Layer Security (TLS) dengan database Exadata. Untuk informasi selengkapnya, lihat Mempersiapkan Koneksi Tanpa Dompet TLS.
- Oracle Database@AWS tidak segera dapat diakses dari internet dan digunakan hanya pada subnet pribadi. AWS
- Oracle Database@AWS menggunakan banyak port Transmission Control Protocol (TCP) default untuk berbagai operasi. Untuk daftar lengkap port, lihat Penetapan port default.
- Untuk menyimpan dan mengelola kunci dengan menggunakan Transparent Data Encryption (TDE), yang diaktifkan secara default, Oracle Database@AWS menggunakan brankas OCI atau Oracle Key Vault. Oracle Database@AWS tidak mendukung AWS Key Management Service.
- Secara default, database dikonfigurasi dengan menggunakan kunci enkripsi yang dikelola Oracle. Basis data juga mendukung kunci yang dikelola pelanggan.
- Untuk meningkatkan perlindungan data, gunakan Oracle Data Safe dengan Oracle Database@AWS.

Topik berikut menunjukkan cara mengonfigurasi Oracle Database@AWS untuk memenuhi tujuan keamanan dan kepatuhan Anda.

Topik

Perlindungan data di Oracle Database@AWS

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensi dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk ketika Anda bekerja dengan Oracle Database@AWS atau lainnya Layanan AWS menggunakan konsol, API, AWS CLI atau. AWS SDKs Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi data

Database Exadata menggunakan Oracle Transparent Data Encryption (TDE) untuk mengenkripsi data Anda. Data Anda juga dilindungi di ruang tabel sementara, undo segment, redo log dan selama operasi database internal seperti JOIN dan SORT. Untuk informasi selengkapnya, lihat Keamanan Data.

Enkripsi saat bergerak

Database Exadata menggunakan enkripsi Oracle Net Services asli dan kemampuan integritas untuk mengamankan koneksi ke database. Untuk informasi selengkapnya, lihat Keamanan data dalam perjalanan.

Manajemen kunci

Enkripsi Data Transparan mencakup keystore untuk menyimpan kunci enkripsi master dengan aman, dan kerangka kerja manajemen untuk mengelola keystore dengan aman dan efisien dan melakukan operasi pemeliharaan kunci. Untuk informasi selengkapnya, lihat Untuk mengelola kunci enkripsi Vault.

Manajemen identitas dan akses untuk Oracle Database@AWS

AWS Identity and Access Management (IAM) adalah AWS layanan yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Oracle Database@.AWS IAM adalah AWS layanan yang dapat Anda gunakan tanpa biaya tambahan.

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat Memecahkan masalah Oracle Database@AWS identitas dan akses)
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat Bagaimana Oracle Database@AWS bekerja dengan IAM)

- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat Kebijakan berbasis identitas untuk Oracle Database@AWS)

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredensional dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensional. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat Cara masuk ke Akun AWS Anda dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensyal sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensi dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat Apa itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensi sementara di Panduan Pengguna IAM.

Grup IAM menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan beralih dari pengguna ke peran IAM (konsol) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna gabungan, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon. EC2 Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada banyak identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus menentukan principal dalam kebijakan berbasis sumber daya.

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCPs) — Tentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCPs) — Tetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.

- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana Oracle Database@AWS bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Oracle Database @AWS, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Oracle Database @.AWS

Fitur IAM	Oracle Database@AWS dukungan
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara Oracle Database@AWS dan AWS layanan lain bekerja dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Oracle Database@AWS

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Oracle Database@AWS

Untuk melihat contoh kebijakan AWS berbasis identitas Oracle Database@, lihat. Kebijakan berbasis identitas untuk Oracle Database@AWS

Kebijakan berbasis sumber daya dalam Oracle Database@AWS

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk Oracle Database@AWS

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar Oracle Database@AWS tindakan, lihat Tindakan yang Ditentukan oleh Oracle Database @AWS di Referensi Otorisasi Layanan.

Tindakan kebijakan Oracle Database@AWS menggunakan awalan berikut sebelum tindakan:

```
odb
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

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

Untuk melihat contoh kebijakan AWS berbasis identitas Oracle Database@, lihat. Kebijakan berbasis identitas untuk Oracle Database@AWS

Sumber daya kebijakan untuk Oracle Database@AWS

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar jenis Oracle Database@AWS sumber daya dan mereka ARNs, lihat Resources Defined by Oracle Database @AWS di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang Ditentukan oleh Oracle Database @.AWS

Untuk melihat contoh kebijakan AWS berbasis identitas Oracle Database@, lihat. Kebijakan berbasis identitas untuk Oracle Database@AWS

Kunci kondisi kebijakan untuk Oracle Database@AWS

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci Oracle Database@AWS kondisi, lihat Condition Keys for Oracle Database@AWS di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang Ditentukan oleh Oracle Database AWS@.

Untuk melihat contoh kebijakan AWS berbasis identitas Oracle Database@, lihat. Kebijakan berbasis identitas untuk Oracle Database@AWS

ACLs di Oracle Database@AWS

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan Oracle Database@AWS

Mendukung ABAC (tag dalam kebijakan): Sebagian

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut tanda. Anda dapat melampirkan tag ke entitas dan AWS sumber daya IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi saat tag prinsipal cocok dengan tag pada sumber daya.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Tentukan izin dengan otorisasi ABAC dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensi sementara dengan Oracle Database@AWS

Mendukung kredensial sementara: Ya

Kredensyal sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensyal sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM dan Layanan AWS yang berfungsi dengan IAM dalam Panduan Pengguna IAM.

Izin utama lintas layanan untuk Oracle Database@AWS

Mendukung sesi akses terusan (FAS): Ya

Sesi akses teruskan (FAS) menggunakan izin dari prinsipal yang memanggil AWS layanan, dikombinasikan dengan layanan yang meminta untuk membuat permintaan ke AWS layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses terusan.

Peran layanan untuk Oracle Database@AWS

Mendukung peran layanan: Tidak

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke AWS layanan di Panduan Pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak Oracle Database@AWS fungsionalitas. Edit peran layanan hanya jika Oracle Database@AWS memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Oracle Database@AWS

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke layanan. AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran Oracle Database@AWS terkait layanan, lihat. Menggunakan peran terkait layanan untuk Oracle Database@AWS

Kebijakan berbasis identitas untuk Oracle Database@AWS

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Oracle Database @AWS . Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM (konsol) di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Oracle Database@AWS, termasuk format ARNs untuk setiap jenis sumber daya, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk Oracle Database @AWS di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Oracle Database@AWS
- Memungkinkan pengguna untuk menyediakan Oracle Database@AWS sumber daya
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Oracle AWS Database@ di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui AWS layanan tertentu, seperti

CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.

- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Menggunakan konsol Oracle Database@AWS

Untuk mengakses AWS konsol Oracle Database@, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk daftar dan melihat rincian tentang sumber daya Oracle Database@AWS di Anda. Akun AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Memungkinkan pengguna untuk menyediakan Oracle Database@AWS sumber daya

Kebijakan ini memungkinkan pengguna akses penuh ke Oracle Database@AWS sumber daya penyediaan. Untuk mengatur resolusi DNS dari VPC Anda, buat resolver Route 53 keluar dan tambahkan aturan untuk meneruskan lalu lintas DNS dengan nama domain OCI ke IP pendengar DNS OCI.

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": "*"
        }
    ]
}
```

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. 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 kebijakan terkelola untuk Oracle Database@AWS

Untuk menambahkan izin ke set dan peran izin, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan yang dikelola pelanggan IAM yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di Akun AWS Anda. Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan Pengguna IAM.

Layanan AWS memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan AWS terkelola untuk mendukung fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan AWS terkelola saat fitur baru diluncurkan atau saat operasi baru tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan `ReadOnlyAccess` AWS terkelola menyediakan akses hanya-baca ke semua Layanan AWS dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk melihat daftar dan deskripsi dari kebijakan fungsi tugas, lihat kebijakan yang dikelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

Topik

- AWS kebijakan terkelola: Amazon ODBService RolePolicy

AWS kebijakan terkelola: Amazon ODBService RolePolicy

Anda tidak dapat melampirkan kebijakan `AmazonODBServiceRolePolicy` ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Oracle Database@AWS untuk melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Oracle Database@AWS.

Untuk melihat detail selengkapnya tentang kebijakan, termasuk versi terbaru dari dokumen kebijakan JSON, lihat Amazon ODBService RolePolicy di Panduan Referensi Kebijakan AWS Terkelola.

Oracle Database@AWS otentikasi dan otorisasi di OCI

Saat Anda menggunakannya AWS APIs untuk membuat sumber daya Oracle Database@AWS, sumber daya tersebut secara logis berada dalam penyewaan Oracle Cloud Infrastructure (OCI) Anda yang tertaut. Untuk menyebarkan sumber daya ini, AWS berkomunikasi dengan OCI APIs atas nama Anda. Untuk mengurangi masalah deputi yang membingungkan, OCI dan Oracle Database@AWS gunakan AWS STS sebagai entitas tepercaya dan meneruskan sesi akses untuk mengotorisasi maksud Anda untuk menggunakan APIs OCI dalam penyewaan tertaut Anda. Akibatnya, peristiwa direkam untuk `sts:getCallerIdentity` API dari ruang IP OCI di AWS CloudTrail jejak dan riwayat peristiwa Anda. Harapkan acara ini saat Anda menggunakannya Oracle Database@AWS APIs.

Memecahkan masalah Oracle Database@AWS identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Oracle Database@AWS dan IAM.

Topik

Saya tidak berwenang untuk melakukan tindakan di Oracle Database@AWS

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin odb:*`GetWidget`* rekaan.

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

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan odb:*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Oracle AWS Database@.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Oracle Database@.AWS Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

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

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses Oracle Database@AWS sumber daya saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Oracle Database@AWS mendukung fitur-fitur ini, lihat. Bagaimana Oracle Database@AWS bekerja dengan IAM
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Validasi kepatuhan untuk Oracle Database @AWS

Tanggung jawab kepatuhan Anda saat menggunakan Oracle Database@AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. Dokumentasi Oracle tentang kepatuhan di cloud tersedia di situs web Oracle

Ketahanan di Oracle Database@AWS

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Selain infrastruktur AWS global, Oracle Database @AWS menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda.

Menggunakan peran terkait layanan untuk Oracle Database@AWS

Oracle Database@AWS menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. Oracle Database@AWS Peran terkait layanan telah ditentukan sebelumnya oleh Oracle Database@AWS dan menyertakan semua izin yang diperlukan layanan untuk memanggil orang lain Layanan AWS atas nama Anda.

Peran terkait layanan membuat penggunaan Oracle Database@AWS lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Oracle Database@AWS mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya Oracle Database@AWS dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran hanya setelah terlebih dahulu menghapus sumber daya terkaitnya. Ini melindungi Oracle Database@AWS sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Izin peran terkait layanan untuk Oracle Database@AWS

Oracle Database@AWS menggunakan peran terkait layanan bernama AWSService RoleFor ODB Oracle Database@AWS untuk memungkinkan panggilan Layanan AWS atas nama sumber daya Anda.

Peran terkait layanan AWSService RoleFor ODB mempercayai layanan berikut untuk mengambil peran:

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

Peran terkait layanan ini memiliki kebijakan izin yang menyertainya bernama `AmazonODBServiceRolePolicy` yang memberikannya izin untuk beroperasi di akun Anda. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola: Amazon ODBService RolePolicy.

> **Note**
>
> Anda harus mengonfigurasi izin agar entitas IAM (seperti pengguna, grup, atau peran) dapat membuat, mengedit, atau menghapus peran terkait layanan. Jika Anda menemukan pesan kesalahan berikut:
> Tidak dapat membuat sumber daya. Verifikasi bahwa Anda memiliki izin untuk membuat peran terkait layanan. Jika tidak, tunggu dan coba lagi nanti.
> Pastikan Anda telah mengaktifkan izin berikut:

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

Untuk informasi selengkapnya, lihat Izin peran yang terkait dengan layanan dalam Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Oracle Database@AWS

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat database Exadata, Oracle Database@AWS buat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda membuat database Exadata, Oracle Database@AWS buat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk Oracle Database@AWS

Oracle Database@AWS tidak mengizinkan Anda mengedit peran terkait layanan AWSService RoleFor ODB. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit deskripsi peran menggunakan IAM Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan di Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Oracle Database@AWS

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Namun, Anda harus menghapus semua sumber daya sebelum dapat menghapus peran terkait layanan.

Membersihkan peran terkait layanan untuk Oracle Database@AWS

Sebelum dapat menggunakan IAM untuk menghapus peran tertaut layanan, Anda harus mengonfirmasi terlebih dahulu bahwa peran tersebut tidak memiliki sesi aktif dan menghapus sumber daya yang digunakan oleh peran tersebut.

Untuk memeriksa apakah peran terkait layanan memiliki sesi aktif di konsol IAM

1. Masuk ke Konsol Manajemen AWS dan buka konsol IAM di https://console.aws.amazon.com/iam/.

2. Di panel navigasi konsol IAM, pilih Peran. Kemudian pilih nama (bukan kotak centang) dari peran AWSService RoleFor ODB.
3. Di halaman Ringkasan untuk peran yang dipilih, pilih tab Penasihat Akses.
4. Di tab Penasihat Akses, tinjau aktivitas terbaru untuk peran terkait layanan tersebut.

> **Note**
>
> Jika Anda tidak yakin Oracle Database@AWS apakah menggunakan peran AWSService RoleFor ODB, Anda dapat mencoba menghapus peran tersebut. Jika layanan menggunakan peran, maka penghapusan gagal dan Anda dapat melihat Wilayah AWS di mana peran tersebut digunakan. Jika peran tersebut sedang digunakan, Anda harus menunggu hingga sesi ini berakhir sebelum dapat menghapus peran tersebut. Anda tidak dapat mencabut sesi untuk peran terkait layanan.

Jika Anda ingin menghapus peran AWSService RoleFor ODB, Anda harus terlebih dahulu menghapus semua Oracle Database@AWS sumber daya Anda.

Wilayah yang Didukung untuk Oracle Database@AWS peran terkait layanan

Oracle Database@AWS mendukung penggunaan peran terkait layanan di semua Wilayah AWS tempat layanan tersedia. Untuk informasi lebih lanjut, lihat Wilayah AWS dan Titik Akhir.

Oracle Database@AWS pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola Oracle Database@AWS sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat Oracle Database@AWS dokumen.

Ubah	Deskripsi	Date
Izin peran terkait layanan untuk Oracle Database@AWS –	Oracle Database@AWS menambahkan izin baru ke `AmazonODBServiceRolePolicy` peran `AWSServiceRoleForODB` terkait layanan. Izin	Juni 30, 2025

Ubah	Deskripsi	Date
Pembaruan ke kebijakan yang sudah ada	ini memungkinkan Oracle Database@AWS untuk melakukan hal berikut: • Jelaskan lampiran Amazon VPC Transit Gateways • Jelaskan EC2 lampiran Amazon • Aktifkan EventBridge sumber Amazon Untuk informasi selengkapnya, lihat Izin peran terkait layanan untuk Oracle Database@AWS.	
Izin peran terkait layanan untuk Oracle Database@AWS – Pembaruan ke kebijakan yang sudah ada	Oracle Database@AWS menambahkan izin baru ke `AmazonODBServiceRolePolicy` peran `AWSServiceRoleForODB` terkait layanan. Izin ini memungkinkan Oracle Database@AWS untuk melakukan hal berikut: • Jelaskan EventBridge sumber Amazon • Jelaskan dan buat bus acara Untuk informasi selengkapnya, lihat Izin peran terkait layanan untuk Oracle Database@AWS.	Juni 26, 2025
AWS kebijakan terkelola: Amazon ODBService RolePolicy— Kebijakan peran terkait layanan baru	Oracle Database@AWS menambahkan `AmazonODBServiceRolePolicy` untuk peran `AWSServiceRoleForODB` terkait layanan. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola: Amazon ODBService RolePolicy.	Desember 2, 2024
Oracle Database@AWS mulai melacak perubahan	Oracle Database@AWS mulai melacak perubahan untuk kebijakan yang AWS dikelola.	Desember 2, 2024

Memantau Database Oracle@AWS

Pemantauan adalah bagian penting dari menjaga keandalan, ketersediaan, dan kinerja Oracle Database@AWS dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk menonton Oracle Database@AWS, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- Amazon CloudWatch memantau AWS sumber daya Anda dan dan aplikasi yang Anda jalankan AWS secara real time. Anda dapat mengumpulkan dan melacak metrik, membuat dasbor yang disesuaikan, dan mengatur alarm yang memberi tahu Anda atau mengambil tindakan saat metrik tertentu mencapai ambang batas yang ditentukan. Misalnya, Anda dapat CloudWatch melacak penggunaan CPU atau metrik lain dari EC2 instans Amazon Anda dan secara otomatis meluncurkan instans baru bila diperlukan. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.
- Amazon CloudWatch Logs memungkinkan Anda memantau, menyimpan, dan mengakses file log Anda dari EC2 instans Amazon CloudTrail, dan sumber lainnya. CloudWatch Log dapat memantau informasi dalam file log dan memberi tahu Anda ketika ambang batas tertentu terpenuhi. Anda juga dapat mengarsipkan data log dalam penyimpanan yang sangat durabel. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon CloudWatch Logs.
- Amazon EventBridge dapat digunakan untuk mengotomatiskan AWS layanan Anda dan merespons secara otomatis peristiwa sistem, seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Acara dari AWS layanan dikirim ke EventBridge dalam waktu dekat. Anda dapat menuliskan aturan sederhana untuk menunjukkan peristiwa mana yang sesuai kepentingan Anda, dan tindakan otomatis mana yang diambil ketika suatu peristiwa sesuai dengan suatu aturan. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.
- AWS CloudTrailmenangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama AWS akun Anda dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS CloudTrail.

Pemantauan Oracle Database@AWS dengan Amazon CloudWatch

Anda dapat memantau Oracle Database@AWS penggunaan CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca, mendekati waktu nyata. Statistik ini disimpan untuk jangka waktu 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang performa aplikasi atau layanan web Anda. Anda juga dapat mengatur alarm yang memperhatikan ambang batas tertentu dan mengirim notifikasi atau mengambil tindakan saat ambang batas tersebut terpenuhi. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

CloudWatch Metrik Amazon untuk Oracle Database@AWS

Oracle Database@AWS Layanan melaporkan metrik ke Amazon CloudWatch di `AWS/ODB` namespace untuk cluster VM, database container, dan database pluggable.

Topik

Metrik untuk klaster VM cloud

Oracle Database@AWS Layanan melaporkan metrik berikut di `AWS/ODB` namespace untuk klaster VM cloud.

Metrik	Deskripsi	Unit
`ASMDiskgroupUtilization`	Persentase ruang yang dapat digunakan dalam Disk Group. Ruang yang dapat digunakan adalah ruang yang tersedia untuk pertumbuhan. Grup disk DATA menyimpan file database Oracle kami. Grup disk RECO berisi file database	Persentase

Metrik	Deskripsi	Unit
	untuk pemulihan seperti arsip dan log kilas balik.	
`CpuUtilization`	Persentase pemanfaatan CPU.	Persentase
`FilesystemUtilization`	Persentase pemanfaatan sistem file yang disediakan.	Persentase
`LoadAverage`	Rata-rata beban sistem selama 5 menit.	Bilangan Bulat
`MemoryUtilization`	Persentase memori yang tersedia untuk memulai aplikasi baru, tanpa bertukar. Memori yang tersedia dapat diperoleh melalui perintah berikut: `cat /proc/meminfo`	Persentase
`NodeStatus`	Menunjukkan apakah host dapat dijangkau.	Bilangan Bulat
`OcpusAllocated`	Jumlah yang OCPUs dialokasikan.	Bilangan Bulat
`SwapUtilization`	Persentase pemanfaatan total ruang swap.	Persentase

Metrik untuk database kontainer

Oracle Database@AWS Layanan melaporkan metrik berikut di `AWS/ODB` namespace untuk database container.

Metrik	Deskripsi	Unit
`BlockChanges`	Jumlah rata-rata blok berubah per detik.	Perubahan per detik
`CpuUtilization`	Pemanfaatan CPU dinyataka n sebagai persentase, dikumpulkan di semua kelompok konsumen. Persentase pemanfaat an dilaporkan sehubunga n dengan jumlah CPUs database yang diizinkan untuk digunakan, yaitu dua kali jumlah OCPUs.	Persentase
`CurrentLogons`	Jumlah login yang berhasil selama interval yang dipilih.	Hitungan
`ExecuteCount`	Jumlah panggilan pengguna dan rekursif yang mengeksek usi pernyataan SQL selama interval yang dipilih.	Hitungan
`ParseCount`	Jumlah parse keras dan lunak selama interval yang dipilih.	Hitungan
`StorageAllocated`	Jumlah total ruang penyimpan an yang dialokasikan ke database pada waktu pengumpulan.	GB
`StorageAllocatedBy Tablespace`	Jumlah total ruang penyimpan an yang dialokasikan ke ruang meja pada waktu pengumpulan. Dalam kasus database kontainer, metrik	GB

Metrik	Deskripsi	Unit
	ini menyediakan ruang tabel kontainer root.	
StorageUsed	Jumlah total ruang penyimpanan yang digunakan oleh database pada waktu pengumpulan.	GB
StorageUsedByTablespace	Jumlah total ruang penyimpanan yang digunakan oleh tablespace pada waktu pengumpulan. Dalam kasus database kontainer, metrik ini menyediakan ruang tabel kontainer root.	GB
StorageUtilization	Persentase kapasitas penyimpanan yang disediakan saat ini digunakan. Merupakan total ruang yang dialokasikan untuk semua ruang tabel.	Persentase
StorageUtilizationByTablespace	Ini menunjukkan persentase ruang penyimpanan yang digunakan oleh tablespace pada waktu pengumpulan. Dalam kasus database kontainer, metrik ini menyediakan ruang tabel kontainer root..	Persentase
TransactionCount	Jumlah gabungan komit pengguna dan rollback pengguna selama interval yang dipilih.	Hitungan

Metrik	Deskripsi	Unit
`UserCalls`	Jumlah gabungan login, parses, dan mengeksekusi panggilan selama interval yang dipilih.	Hitungan

Metrik untuk database pluggable

Oracle Database@AWS Layanan melaporkan metrik berikut di `AWS/ODB` namespace untuk database pluggable.

Metrik	Deskripsi	Unit
`AllocatedStorageUtilizationByTablespace`	Persentase ruang yang digunakan oleh tablespace, dari semua yang dialokasikan. Untuk database kontainer, metrik ini menyediakan data untuk ruang tabel kontainer root. (Statistik: Rata-rata, Interval: 30 menit)	Persen
`AvgGCCRBlockReceiveTime`	Rata-rata blok CR cache global (pembacaan konsisten) menerima waktu. Hanya untuk database RAC/cluster. (Statistik: Rata-rata, Interval: 5 menit)	Milidetik
`AvgGCCurrentBlockReceiveTime`	Rata-rata blok cache global saat ini menerima waktu. Statistik melaporkan nilai rata-rata. Hanya untuk database Real Application Cluster (RAC). (Statistik: Rata-rata, Interval: 5 menit)	Milidetik

Metrik	Deskripsi	Unit
`BlockChanges`	Jumlah rata-rata blok berubah per detik. (Statistik: Rata-rata, Interval: 1 menit)	perubahan per detik
`BlockingSessions`	Sesi pemblokiran saat ini. Tidak berlaku untuk database kontainer. (Statistik: Maks, Interval: 15 menit)	Hitungan
`CPUTimeSeconds`	Tingkat rata-rata akumulasi waktu CPU oleh sesi latar depan dalam instance database selama interval waktu. Komponen waktu CPU dari Sesi Aktif Rata-rata. (Statistik: Rata-rata, Interval: 1 menit)	Detik per detik
`CpuCount`	Jumlah CPUs selama interval yang dipilih.	Hitungan
`CpuUtilization`	Pemanfaatan CPU dinyataka n sebagai persentase, dikumpulkan di semua kelompok konsumen. Persentase pemanfaat an dilaporkan sehubunga n dengan jumlah CPUs database yang diizinkan untuk digunakan, yaitu dua kali jumlah OCPUs. (Statistik: Rata-rata, Interval: 1 menit)	Persen

Metrik	Deskripsi	Unit
`CurrentLogons`	Jumlah login yang berhasil selama interval yang dipilih. (Statistik: Jumlah, Interval: 1 menit)	Hitungan
`DBTimeSeconds`	Tingkat rata-rata akumulasi waktu database (CPU + Wait) oleh sesi latar depan dalam instance database selama interval waktu. Juga dikenal sebagai Average Active Sessions. (Statistik: Rata-rata, Interval: 1 menit)	Detik per detik
`DbmgmtJobExecutionsCount`	Jumlah eksekusi pekerjaan SQL pada database terkelola tunggal atau grup database, dan statusnya. Dimensi status dapat berupa nilai-nilai berikut: “Berhasil,” “Gagal,” “”InProgress.” (Statistik: Jumlah, Interval: 1 menit)	Hitungan
`ExecuteCount`	Jumlah panggilan pengguna dan rekursif yang mengeksekusi pernyataan SQL selama interval yang dipilih. (Statistik: Jumlah, Interval: 1 menit)	Hitungan
`FRASpaceLimit`	Batas ruang area pemulihan flash. Tidak berlaku untuk database pluggable. (Statistik: Maks, Interval: 15 menit)	GB

Metrik	Deskripsi	Unit
FRAUtilization	Pemanfaatan area pemulihan flash. Tidak berlaku untuk database pluggable. (Statistik: Rata-rata, Interval: 15 menit)	Persen
GCCRBlocksReceived	Blok CR cache global (pembacaan konsisten) yang diterima per detik. Hanya untuk database RAC/cluster. (Statistik: Rata-rata, Interval: 5 menit)	Blok per detik
GCCurrentBlocksReceived	Merupakan blok cache global saat ini yang diterima per detik. Statistik melaporkan nilai rata-rata. Hanya untuk database Real Application Cluster (RAC). (Statistik: Rata-rata, Interval: 5 menit)	Blok per detik
IOPS	Jumlah rata-rata operasi input-output per detik. (Statistik: Rata-rata, Interval: 1 menit)	Operasi per detik
IOThroughputMB	Throughput rata-rata dalam MB per detik. (Statistik: Rata-rata, Interval: 1 menit)	MB per detik
InterconnectTrafficMB	Rata-rata kecepatan transfer data internode. Hanya untuk database RAC/cluster. (Statistik: Rata-rata, Interval: 5 menit)	MB per detik

Metrik	Deskripsi	Unit
`InvalidObjects`	Jumlah objek database tidak valid. Tidak berlaku untuk database kontainer. (Statistik: Maks, Interval: 24 jam)	Hitungan
`LogicalBlocksRead`	Jumlah rata-rata blok yang dibaca dari SGA/Memor y (buffer cache) per detik. (Statistik: Rata-rata, Interval: 1 menit)	Bacaan per detik
`MaxTablespaceSize`	Ukuran tablespace maksimum yang mungkin. Untuk database kontainer, metrik ini menyediakan data untuk ruang tabel kontainer root. (Statistik: Maks, Interval: 30 menit)	GB
`MemoryUsage`	Ukuran total kolam memori dalam MB. (Statistik: Rata-rata , Interval: 15 menit)	MB
`MonitoringStatus`	Status pemantauan sumber daya. Jika pengumpulan metrik gagal, informasi kesalahan ditangkap dalam metrik ini. (Statistik: Rata-rata, Interval: 5 menit)	Tidak berlaku
`NonReclaimableFRA`	Area pemulihan cepat yang tidak dapat direklamasi. Tidak berlaku untuk database pluggable. (Statistik: Rata-rata , Interval: 15 menit)	Persen

Metrik	Deskripsi	Unit
`OcpusAllocated`	Jumlah aktual yang OCPUs dialokasikan oleh layanan selama interval waktu yang dipilih. (Statistik: Hitung, Interval: 1 menit)	Bilangan Bulat
`ParseCount`	Jumlah parse keras dan lunak selama interval yang dipilih. (Statistik: Jumlah, Interval: 1 menit)	Hitungan
`ParsesByType`	Jumlah parse keras atau lunak per detik. (Statistik: Rata-rata, Interval: 1 menit)	Penguraian per detik
`ProblematicScheduledDBMSJobs`	Jumlah pekerjaan database terjadwal yang bermasalah. Tidak berlaku untuk database kontainer. (Statistik: Maks, Interval: 15 menit)	Hitungan
`ProcessLimitUtilization`	Proses membatasi pemanfaatan. Tidak berlaku untuk database yang dapat dicolokkan. (Statistik: Rata-rata, Interval: 1 menit)	Persen
`Processes`	Proses database dihitung. Tidak berlaku untuk database yang dapat dicolokkan. (Statistik: Maks, Interval: 1 menit)	Hitungan

Metrik	Deskripsi	Unit
ReclaimableFRA	Area pemulihan cepat yang dapat direklamasi. Tidak berlaku untuk database yang dapat dicolokkan. (Statistik: Rata-rata, Interval: 15 menit)	Persen
ReclaimableFRASpace	Area pemulihan flash ruang yang dapat direklamasi. Tidak berlaku untuk database yang dapat dicolokkan. (Statistik: Rata-rata, Interval: 15 menit)	GB
RedoSizeMB	Jumlah rata-rata redo yang dihasilkan, dalam MB per detik. (Statistik: Rata-rata, Interval: 1 menit)	MB per detik
SessionLimitUtilization	Pemanfaatan batas sesi. Tidak berlaku untuk database yang dapat dicolokkan. (Statistik: Rata-rata, Interval: 1 menit)	Persen
Sessions	Jumlah sesi dalam database. (Statistik: Rata-rata, Interval: 1 menit)	Hitungan
StorageAllocated	Jumlah maksimum ruang yang dialokasikan oleh tablespace selama interval. Untuk database kontainer, metrik ini menyediakan data untuk ruang tabel kontainer root. (Statistik: Maks, Interval: 30 menit)	GB

Metrik	Deskripsi	Unit
`StorageAllocatedByTablespace`	Jumlah maksimum ruang yang dialokasikan oleh tablespace selama interval. Untuk database kontainer, metrik ini menyediakan data untuk ruang tabel kontainer root. (Statistik: Maks, Interval: 30 menit)	GB
`StorageUsed`	Jumlah maksimum ruang yang digunakan selama interval. (Statistik: Maks, Interval: 30 menit)	GB
`StorageUsedByTablespace`	Jumlah maksimum ruang yang digunakan oleh tablespace selama interval. Untuk database kontainer, metrik ini menyediakan data untuk ruang tabel kontainer root. (Statistik: Maks, Interval: 30 menit)	GB
`StorageUtilization`	Persentase kapasitas penyimpanan yang disediakan saat ini digunakan. Merupakan total ruang yang dialokasikan untuk semua ruang tabel. (Statistik: Rata-rata, Interval: 30 menit)	Persen

Metrik	Deskripsi	Unit
`StorageUtilization ByTablespace`	Persentase ruang yang digunakan, oleh tablespace. Untuk database kontainer, metrik ini menyediakan data untuk ruang tabel kontainer root. (Statistik: Rata-rata, Interval: 30 menit)	Persen
`TransactionCount`	Jumlah gabungan komit pengguna dan rollback pengguna selama interval yang dipilih. (Statistik: Jumlah, Interval: 1 menit)	Hitungan
`TransactionsByStatus`	Jumlah transaksi yang dilakukan atau digulung kembali per detik. (Statistik: Rata-rata, Interval: 1 menit)	Transaksi per detik
`UnusableIndexes`	Indeks yang tidak dapat digunakan dihitung dalam skema database. Tidak berlaku untuk database kontainer. (Statistik: Maks, Interval: 24 jam)	Hitungan
`UsableFRA`	Area pemulihan cepat yang bisa digunakan. Tidak berlaku untuk database yang dapat dicolokkan. (Statistik: Rata-rata, Interval: 15 menit)	Persen

Metrik	Deskripsi	Unit
`UsedFRASpace`	Penggunaan ruang area pemulihan flash. Tidak berlaku untuk database yang dapat dicolokkan. (Statistik: Maks, Interval: 15 menit)	GB
`UserCalls`	Jumlah gabungan login, parses, dan mengeksekusi panggilan selama interval yang dipilih. (Statistik: Jumlah, Interval: 1 menit)	Hitungan
`WaitTimeSeconds`	Tingkat rata-rata akumulasi waktu tunggu non-idle oleh sesi latar depan dalam instance database selama interval waktu. Komponen waktu tunggu dari Sesi Aktif Rata-rata. (Statistik: Rata-rata, Interval: 5 menit)	Detik per detik

CloudWatch Dimensi Amazon untuk Oracle Database@AWS

Anda dapat memfilter data Oracle Database@AWS metrik dengan menggunakan dimensi apa pun dalam tabel berikut.

Dimensi	Memfilter data yang diminta terhadap . . .
`cloudVmClusterId`	Pengidentifikasi cluster VM.
`cloudExadataInfrastructureId`	Pengidentifikasi infrastruktur Exadata.
`collectionName`	Sebuah nama koleksi.

Dimensi	Memfilter data yang diminta terhadap . . .
deploymentType	Jenis infrastruktur.
diskgroupName	Nama grup disk
errorCode	Kode kesalahan.
errorSeverity	Tingkat keparahan kesalahan.
filesystemName	Nama sistem file.
hostName	Nama mesin host.
instanceName	Nama instance database.
instanceNumber	Nomor instance dari instance database.
ioType	Jenis I/O operasi.
jobId	Pengidentifikasi unik untuk suatu pekerjaan.
managedDatabaseGroupId	Pengidentifikasi a. Managed Database Group
managedDatabaseId	Pengidentifikasi a. Managed Database
memoryPool	Jenis kolam memori.
memoryType	Jenis memori.
ociCloudVmClusterId	Pengidentifikasi OCI dari cluster VM.
ociCloudExadataInfrastructureId	Pengidentifikasi OCI dari infrastruktur Exadata.
parseType	Jenis parse.
resourceId	Pengidentifikasi sumber daya.
resourceId_Database	Pengidentifikasi database.

Dimensi	Memfilter data yang diminta terhadap . . .
resourceId_DbNode	Identifier dari node database.
resourceName	Nama sumber daya.
resourceName_Database	Nama database.
resourceName_DbNode	Nama node database.
resourceType	Jenis database.
schemaName	Nama skema.
status	Status database.
tablespaceContents	Isi dari tablespace.
tablespaceName	Nama tablespace.
tablespaceType	Jenis tablespace.
transactionStatus	Status transaksi.
waitClass	Sebuah kelas acara menunggu.

Memantau Oracle Database@AWS peristiwa di Amazon EventBridge

Anda dapat memantau Oracle Database@AWS peristiwa di EventBridge, yang memberikan aliran data real-time dari aplikasi dan AWS layanan. EventBridge merutekan data ini ke target seperti AWS Lambda dan Amazon Simple Notification Service.

> **Note**
>
> EventBridge Sebelumnya bernama Amazon CloudWatch Events. Untuk informasi selengkapnya, lihat EventBridge evolusi CloudWatch Acara Amazon di Panduan EventBridge Pengguna Amazon.

Ikhtisar Oracle Database@AWS acara

Oracle Database@AWS peristiwa adalah pesan terstruktur yang menunjukkan perubahan dalam siklus hidup sumber daya. Bus acara adalah router yang menerima acara dan mengirimkannya ke nol atau lebih tujuan, atau target. Oracle Database@AWS peristiwa dapat dihasilkan dari sumber-sumber berikut:

Acara dari AWS

Peristiwa ini dihasilkan dari Oracle Database@AWS APIs AWS samping dan dikirim ke bus acara default di Anda Akun AWS.

Acara dari OCI

Peristiwa ini dihasilkan langsung dari OCI, seperti peristiwa yang terkait dengan infrastruktur Oracle Exadata atau cluster VM. Saat Anda berlangganan Oracle Database@AWS, bus acara dengan awalan `aws.partner/odb/` dibuat di Anda Akun AWS untuk menerima acara dari OCI.

Oracle Database@AWS peristiwa dari AWS

Oracle Database@AWS peristiwa dari AWS menyertakan perubahan siklus hidup yang terkait dengan jaringan ODB selama pembuatan dan penghapusan. Acara ini dikirim ke bus acara default di Anda Akun AWS. Jenis pengiriman adalah upaya terbaik.

Acara jaringan ODB

Peristiwa	ID peristiwa	Pesan
Pembuatan	ODB-ACARA-0001	Berhasil membuat jaringan ODB ODBNET_ID
Pembuatan gagal	ODB-ACARA-0011	Gagal membuat jaringan ODB ODBNET_ID
Penghapusan	ODB-ACARA-0002	Berhasil dihapus jaringan ODB ODBNET_ID

Peristiwa	ID peristiwa	Pesan
Penghapusan gagal	ODB-ACARA-0012	Gagal menghapus jaringan ODB ODBNET_ID

Contoh: acara pembuatan jaringan ODB

Contoh berikut menunjukkan acara untuk pembuatan jaringan ODB yang sukses.

```
{
  "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 acara dari OCI

Sebagian besar peristiwa dihasilkan langsung dari OCI. Oracle Database@AWS membuat bus acara dengan awalan `aws.partner/odb/` di Anda Akun AWS untuk menerima acara dari OCI. Kami menyarankan Anda untuk tidak menghapus bus acara ini.

OCI menyediakan jenis acara yang komprehensif, termasuk yang berikut:

- Infrastruktur Oracle Exadata
- Acara cluster VM
- Acara CDB
- Acara PDB

Untuk informasi selengkapnya tentang jenis dan detail peristiwa tertentu yang didukung OCI, lihat Layanan Database Oracle Exadata tentang Acara dan Acara Infrastruktur Khusus untuk Database Otonom pada Infrastruktur Exadata Khusus.

Acara penyaringan Oracle Database@AWS

Anda dapat mengikuti praktik terbaik yang EventBridge disarankan pada pengaturan bus acara di bus Acara di Amazon EventBridge. Bergantung pada kasus penggunaan, Anda dapat mengatur EventBridge aturan untuk memfilter peristiwa dan target untuk menerima dan menggunakan peristiwa.

Memfilter acara jaringan ODB dari AWS

Untuk acara jaringan ODB dari AWS, Anda dapat memfilter menggunakan pola peristiwa berikut:

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

Anda dapat menerapkan pola ini menggunakan EventBridge `put-rule` API dengan bus acara default. Untuk informasi selengkapnya, lihat PutRuledi Referensi Amazon EventBridge API.

Memfilter Oracle Database@AWS acara dari OCI

Untuk Oracle Database@AWS peristiwa dari OCI, Anda dapat mengatur aturan menggunakan perintah yang mirip dengan contoh PutRuledi Referensi Amazon EventBridge API. Perhatikan pedoman berikut:

- Gunakan pola acara khusus tergantung pada jenis acara yang ingin Anda filter.
- Setel EventBusNameke nama bus yang Oracle Database@AWS dibuat.

Untuk informasi selengkapnya tentang cara memfilter peristiwa dan mengatur EventBridge target di seluruh akun, lihat Mengirim dan menerima peristiwa antara Akun AWS di Amazon EventBridge.

Acara pemecahan masalah Oracle Database@AWS

Jika Anda mengalami masalah dengan pengiriman acara atau konten acara, lakukan hal berikut:

- Untuk acara jaringan ODB, hubungi AWS Dukungan.

- Untuk Oracle Database@AWS acara selain peristiwa jaringan ODB, hubungi Oracle Cloud Support.

Untuk informasi selengkapnya, lihat Mendapatkan dukungan untuk Oracle Database @AWS.

Pencatatan panggilan Oracle Database@AWS API menggunakan AWS CloudTrail

Oracle Database@AWS terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS. CloudTrail menangkap semua panggilan API untuk Oracle Database@AWS sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari Oracle Database@AWS konsol dan panggilan kode ke operasi Oracle Database@AWS API. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat Oracle Database@AWS, alamat IP dari mana permintaan dibuat, kapan dibuat, dan detail tambahan.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut hal ini:

- Baik permintaan tersebut dibuat dengan kredensial pengguna root atau pengguna.
- Apakah permintaan dibuat atas nama pengguna IAM Identity Center.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan tersebut dibuat oleh Layanan AWS lain.

> **Note**
>
> Oracle Database@AWS merekam panggilan `GetCallerIdentity` API dari AWS Security Token Service (STS) di CloudTrail log Anda. Panggilan STS API ini memverifikasi identitas Oracle Database@AWS saat berinteraksi dengan OCI atas nama Anda. Mereka adalah bagian AWS operasi yang normal dan aman dan tidak mengekspos informasi sensitif.

CloudTrail aktif di Anda Akun AWS ketika Anda membuat akun dan Anda secara otomatis memiliki akses ke riwayat CloudTrail Acara. Riwayat CloudTrail Acara menyediakan catatan yang dapat

dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir dari peristiwa manajemen yang direkam dalam file. AWS Region Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail Acara di Panduan AWS CloudTrail Pengguna. Tidak ada CloudTrail biaya untuk melihat riwayat Acara.

Untuk catatan acara yang sedang berlangsung dalam 90 hari Akun AWS terakhir Anda, buat jejak atau penyimpanan data acara CloudTrailDanau.

CloudTrail jalan setapak

Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Semua jalur yang dibuat menggunakan Konsol Manajemen AWS Multi-region. Anda dapat membuat jalur Single-region atau Multi-region dengan menggunakan. AWS CLI Membuat jejak Multi-wilayah disarankan karena Anda menangkap aktivitas Wilayah AWS di semua akun Anda. Jika Anda membuat jejak wilayah Tunggal, Anda hanya dapat melihat peristiwa yang dicatat di jejak. AWS Region Untuk informasi selengkapnya tentang jejak, lihat Membuat jejak untuk Anda Akun AWS dan Membuat jejak untuk organisasi di Panduan AWS CloudTrail Pengguna.

Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket Amazon S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga. Untuk informasi tentang harga Amazon S3, lihat Harga Amazon S3.

CloudTrail Penyimpanan data acara danau

CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL pada acara Anda. CloudTrail Lake mengubah peristiwa yang ada dalam format JSON berbasis baris ke format Apache ORC. ORC adalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara tingkat lanjut. Penyeleksi yang Anda terapkan ke penyimpanan data acara mengontrol peristiwa mana yang bertahan dan tersedia untuk Anda kueri. Untuk informasi lebih lanjut tentang CloudTrail Danau, lihat Bekerja dengan AWS CloudTrail Danau di Panduan AWS CloudTrail Pengguna.

CloudTrail Penyimpanan data acara danau dan kueri menimbulkan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Oracle Database@AWS acara manajemen di CloudTrail

Acara manajemen memberikan informasi tentang operasi manajemen yang dilakukan pada sumber daya di Anda Akun AWS. Ini juga dikenal sebagai operasi bidang kontrol. Secara default, CloudTrail mencatat peristiwa manajemen.

Oracle Database@AWS mencatat semua operasi pesawat Oracle Database@AWS kontrol sebagai peristiwa manajemen.

Oracle Database@AWS contoh acara

Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang operasi API yang diminta, tanggal dan waktu operasi, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga peristiwa tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan CloudTrail peristiwa yang menunjukkan `CreateOdbNetwork` operasi.


```
{
    "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"
    }
}
```


Untuk informasi tentang konten CloudTrail rekaman, lihat konten CloudTrail rekaman di Panduan AWS CloudTrail Pengguna.

Memecahkan Masalah Database Oracle@AWS

Gunakan bagian berikut untuk membantu memecahkan masalah jaringan yang mungkin Anda hadapi. Oracle Database@AWS

Topik

Pembuatan jaringan ODB gagal

Bila Anda tidak dapat membuat jaringan ODB, berikut ini adalah penyebab umum:

Rentang CIDR Terbatas

Jaringan ODB menggunakan rentang CIDR khusus untuk klien dan subnet cadangan. Pastikan rentang CIDR yang Anda pilih untuk subnet ini tidak tumpang tindih dengan rentang alamat IP yang dibatasi atau dicadangkan.

Rentang CIDR berikut dicadangkan dan tidak dapat digunakan untuk jaringan ODB:

- Rentang cadangan awan Oracle: 169.254.0.0/16
- Kelas D Cadangan: 224.0.0.0 - 239.255.255.255
- Kelas E Cadangan: 240.0.0.0 - 255.255.255.255
- Penggunaan OCI di masa depan: 100.105.0.0/16

Ikuti EC2 aturan untuk rentang CIDR seperti yang diuraikan dalam dokumentasi VPC. Untuk mempelajari lebih lanjut, lihat Pembatasan asosiasi blok CIDR.

Selain itu, hindari tumpang tindih antara rentang CIDR yang ditentukan dan yang digunakan untuk konektivitas VPC ke jaringan ODB.

Tumpang tindih VPC CIDR

Rentang CIDR yang Anda tentukan untuk jaringan ODB tidak boleh tumpang tindih dengan rentang CIDR yang digunakan oleh salah satu yang ada. VPCs Rentang CIDR yang tumpang

tindih dapat menyebabkan konflik perutean dan mencegah keberhasilan pembuatan jaringan ODB. Periksa rentang CIDR dari ODB peering VPCs dan pastikan CIDR jaringan ODB unik dan tidak tumpang tindih.

Kepemilikan VPCs

Jaringan ODB dan VPC yang Anda sambungkan harus dimiliki oleh akun yang sama. AWS Jika Anda mencoba mengintip jaringan ODB ke VPC yang dimiliki oleh akun lain, pembuatannya akan gagal. Verifikasi bahwa jaringan ODB dan VPC keduanya dimiliki oleh akun yang sama. AWS

Kurangnya gerbang transit

Jika Anda menambahkan rentang CIDR ke daftar CIDR peered jaringan ODB tanpa melampirkan gateway transit ke VPC, operasi buat atau perbarui gagal. Tidak ada persyaratan tentang rentang CIDR yang digunakan lampiran.

Masalah konektivitas antara VPC dan jaringan ODB atau kluster VM Anda

Bila Anda tidak dapat terhubung dari VPC ke jaringan ODB atau kluster VM di dalamnya, berikut ini adalah penyebab umum:

- Memverifikasi konfigurasi VPC — Di Oracle Database@AWS konsol, cari VPC yang diintip dengan jaringan ODB. Konfirmasikan ID VPC cocok dengan yang ditunjukkan dalam detail jaringan ODB.
- Memeriksa tabel rute - Di konsol VPC Amazon, temukan tabel rute yang dilampirkan ke subnet tempat aplikasi Anda berjalan. Periksa rute dengan CIDR tujuan yang cocok dengan CIDR subnet klien dari jaringan ODB. Konfirmasikan bahwa rute ini menunjuk ke ARN jaringan ODB yang benar. Jika rute hilang, tambahkan yang baru ke CIDR subnet klien jaringan ODB.
- Memvalidasi peered CIDRs - Tinjau `Peered CIDRs` bagian dalam detail jaringan ODB. Konfirmasikan semua blok CIDR yang relevan dari VPC Anda terdaftar. Jika CIDR yang diperlukan tidak ada, perbarui CIDRs peered.
- Memeriksa aturan grup keamanan — Di EC2 konsol Amazon, cari grup keamanan untuk sumber daya di VPC Anda. Tinjau aturan masuk dan keluar, perbarui sesuai kebutuhan untuk memungkinkan lalu lintas yang diperlukan.
- Mengonfirmasi Availability Zones — Di konsol VPC Amazon, identifikasi Availability Zone (AZ) subnet Anda. Verifikasi bahwa jaringan ODB juga digunakan di AZ yang sama dengan subnet Anda.

- Menghindari beberapa koneksi peering jaringan ODB — Periksa koneksi peering VPC Anda di Konsol. Oracle Database@AWS Pastikan Anda hanya memiliki satu koneksi aktif ke jaringan ODB. Jika Anda melihat lebih dari satu jaringan ODB mengintip, hapus yang ekstra.

Nama host atau pemindaian klaster VM yang tidak dapat diselesaikan dari VPC

Jika nama host atau nama pemindaian klaster VM tidak dapat diselesaikan dari VPC Anda, konfigurasikan penerusan DNS di VPC dan sumber daya berikut untuk menyelesaikan catatan DNS yang dihosting di jaringan ODB:

- Titik akhir keluar untuk mengirim kueri DNS ke jaringan ODB. Untuk informasi selengkapnya, lihat Mengkonfigurasi titik akhir keluar dalam jaringan ODB di Oracle Database@AWS.
- Aturan resolver untuk menentukan nama domain dari kueri DNS yang diteruskan oleh resolver ke DNS untuk jaringan ODB. Untuk informasi selengkapnya, lihat Mengkonfigurasi aturan resolver di Oracle Database@AWS.

Mendapatkan dukungan untuk Oracle Database @AWS

Pelajari cara mendapatkan informasi dan dukungan untuk Oracle AWS Database@.

Ruang lingkup dukungan Oracle dan informasi kontak

Oracle Cloud Support adalah baris pertama dukungan untuk semua pertanyaan Oracle Database AWS @. Untuk menghubungi dukungan, masuk ke Oracle Cloud Infrastructure (OCI) Console, lalu pilih ikon life raft. Jika Anda tidak memiliki akun Dukungan Cloud Oracle Saya, lihatAkun dan akses Oracle Cloud Support saya.

Contoh masalah yang Oracle Support dapat membantu Anda dengan termasuk yang berikut:

- Masalah koneksi database (Oracle TNS)
- Masalah kinerja Oracle Database
- Resolusi kesalahan Oracle Database
- Masalah jaringan yang terkait dengan komunikasi dengan penyewaan OCI yang terkait dengan layanan

- Kuota (limit) meningkat untuk menerima lebih banyak kapasitas (untuk informasi selengkapnya, lihat Meminta Peningkatan Batas untuk Sumber Daya Database)
- Penskalaan untuk menambahkan lebih banyak kapasitas komputasi dan penyimpanan ke infrastruktur Oracle Database Anda
- Peningkatan perangkat keras generasi baru
- Masalah penagihan yang terkait dengan tagihan Anda AWS Marketplace

Jika Anda perlu menghubungi Oracle Support di luar Konsol OCI, beri tahu agen Dukungan Oracle Anda bahwa masalah Anda terkait dengan Oracle Database@.AWS Ini karena permintaan untuk layanan ini ditangani oleh tim dukungan OCI yang mengkhususkan diri dengan penerapan ini.

Menghubungi dukungan Oracle melalui telepon

1. Hubungi 1-800-223-1711. Jika Anda berada di luar Amerika Serikat, kunjungi Oracle Support Contacts Global Directory untuk menemukan informasi kontak untuk negara atau wilayah Anda.
2. Pilih opsi “2" untuk membuka Permintaan Layanan (SR) baru.
3. Pilih opsi “4" untuk “tidak yakin”.
4. Biarkan agen tahu bahwa Anda memiliki masalah dengan sistem multicloud Anda, dan nama produk. Permintaan Layanan internal akan dibuka atas nama Anda dan insinyur dukungan OCI akan menghubungi Anda secara langsung.

Anda juga dapat mengajukan pertanyaan ke forum Multicloud di komunitas Cloud Customer Connect Oracle. Opsi ini tersedia untuk semua pelanggan.

Akun dan akses Oracle Cloud Support saya

Untuk membuat tiket permintaan layanan My Oracle Cloud Support, administrator AWS layanan Oracle Database@ organisasi Anda harus menyetujui permintaan Anda. Jika Anda AWS administrator Oracle Database@, lengkapi instruksi orientasi Dukungan Cloud Oracle Saya yang disertakan dalam email aktivasi layanan AWS Oracle Database@.

Anda dapat menemukan petunjuk untuk onboarding dengan My Oracle Cloud Support dalam topik berikut:

- Mengonfigurasi Akun Dukungan Oracle Anda
- Membuat Permintaan Support

Untuk petunjuk tentang menyetujui pengguna untuk membuka permintaan dukungan Dukungan Cloud Oracle Saya, lihat Tugas Administrator untuk Dukungan.

AWS Dukungan ruang lingkup dan informasi kontak

AWS Dukungan adalah baris dukungan pertama Anda untuk semua masalah dan pertanyaan AWS terkait. Buat AWS Dukungan kasus untuk masalah Anda, seperti yang Anda lakukan dengan AWS layanan lain. AWS Dukungan Tim bekerja sama dengan OCI Support sesuai kebutuhan.

Contoh AWS masalah Oracle Database@ yang AWS Dukungan dapat membantu Anda termasuk yang berikut:

- Masalah jaringan virtual termasuk yang melibatkan terjemahan alamat jaringan (NAT), firewall, DNS dan manajemen lalu lintas, dan subnet AWS
- Masalah bastion dan mesin virtual (VM) termasuk koneksi host database, instalasi perangkat lunak, latensi, dan kinerja host
- Pelaporan metrik klaster Exadata VM di Amazon CloudWatch
- Masalah penagihan yang terkait dengan layanan AWS

Untuk informasi tentang AWS Dukungan, lihat Memulai dengan AWS Dukungan.

Perjanjian tingkat layanan Oracle

Jika Anda memiliki pertanyaan tentang Oracle Database@AWS Service Level Agreements (SLAs), atau ingin meminta kredit layanan untuk pelanggaran SLA, hubungi manajer akun Oracle Anda. Lihat Perjanjian Tingkat Layanan untuk informasi selengkapnya.

Kuota untuk Oracle Database @AWS

Oracle Database@AWS adalah penawaran multicloud. AWS tidak menetapkan atau memberlakukan kuota untuk Oracle Database@AWS sumber daya. Kuota diberlakukan oleh Oracle Cloud Infrastructure (OCI). Untuk informasi selengkapnya tentang kuota OCI, lihat Kuota dan Batas Layanan dalam dokumentasi Oracle Cloud Infrastructure.

Riwayat dokumen untuk Panduan Oracle Database@AWS Pengguna

Tabel berikut menjelaskan rilis dokumentasi untuk Oracle Database@AWS.

Perubahan	Deskripsi	Tanggal
Oracle Database@AWS mendukung Wilayah Asia Pasifik (Sydney) dan Wilayah Kanada (Tengah)	Anda dapat membuat Oracle Database@AWS sumber daya Anda di wilayah ini. Untuk informasi selengkapnya, lihat Wilayah yang Didukung untuk Oracle Database@AWS.	Februari 2, 2026
Oracle Database@AWS mendukung Wilayah Asia Pasifik (Tokyo), Wilayah Timur AS (Ohio), Wilayah Eropa (Frankfurt)	Anda dapat membuat Oracle Database@AWS sumber daya Anda di wilayah ini. Untuk informasi selengkapnya, lihat Wilayah yang Didukung untuk Oracle Database@AWS.	Desember 22, 2025
Oracle Database@AWS mendukung pembagian hak di seluruh Akun AWS	Sekarang Anda dapat membagikan hak AWS Marketplace untuk Oracle Database@AWS Akun AWS di organisasi yang sama menggunakan AWS License Manager. AWS Untuk informasi selengkapnya, lihat Berbagi hak di Oracle Database@.AWS	Desember 19, 2025
Oracle Database@AWS mendukung modifikasi filter data integrasi nol-ETL	Oracle Database@AWS mendukung modifikasi filter data untuk integrasi nol-ETL yang ada dengan	Oktober 15, 2025

	Amazon Redshift. Anda dapat memperbarui pola filter data untuk menyertakan atau mengecualikan skema dan tabel tertentu dari replikasi data. Untuk informasi selengkapnya, lihat Mengelola integrasi nol-ETL.	
Oracle Database@AWS mendukung manajemen CIDR jaringan sejawat untuk koneksi peering	Anda dapat menentukan jaringan rekan CIDRs saat membuat atau memperbarui koneksi peering ODB. Anda mengontrol subnet mana di VPC rekan yang memiliki akses ke jaringan ODB Anda. Akun VPC dapat memperbarui rentang CIDR tanpa juga memiliki jaringan ODB. Untuk informasi selengkapnya, lihat Mengonfigurasi ODB mengintip ke VPC Amazon di. Oracle Database@AWS	Oktober 10, 2025
Oracle Database@AWS mendukung integrasi nol-ETL dengan Amazon Redshift	Oracle Database@AWS sekarang terintegrasi dengan VPC Lattice untuk mengaktifkan integrasi nol-ETL dengan Amazon Redshift. Untuk informasi selengkapnya, lihat Integrasi layanan untuk Oracle Database@.AWS	Juli 2, 2025

Pembaruan terhadap izin peran yang ditautkan layanan IAM	`AmazonODBServiceRolePolicy` Kebijakan ini sekarang memberikan izin tambahan untuk menjelaskan lampiran gateway transit VPC, menjelaskan subnet Amazon, dan EC2 mengaktifkan sumber Amazon. EventBridge Untuk informasi selengkapnya, lihat Oracle Database@AWS pembaruan kebijakan AWS terkelola.	Juni 30, 2025
Pembaruan terhadap izin peran yang ditautkan layanan IAM	`AmazonODBServiceRolePolicy` Kebijakan ini sekarang memberikan izin tambahan untuk mendeskripsikan peristiwa di Amazon EventBridge Scheduler dan membuat atau mendeskripsikan bus acara. Untuk informasi selengkapnya, lihat Oracle Database@AWS pembaruan kebijakan AWS terkelola.	Juni 26, 2025
Oracle Database@AWS mendukung Wilayah Barat AS (Oregon)	Anda dapat membuat Oracle Database@AWS sumber daya Anda di Wilayah AS Barat (Oregon). AZ fisik yang didukung IDs adalah `usw2-az3` dan`usw2-az4`. Untuk informasi selengkapnya, lihat Wilayah yang Didukung untuk Oracle Database@AWS.	Juni 26, 2025

Oracle Database@AWS mendukung berbagi sumber daya di seluruh Akun AWS	Sekarang Anda dapat berbagi infrastruktur Exadata dan kluster VM dengan yang lain Akun AWS di dalam organisasi Anda menggunakan (). AWS Resource Access Manager AWS RAM Anda dapat menyediakan infrastruktur sekali dan membagikannya di beberapa akun, mengurangi biaya sambil mempertahankan pemisahan tanggung jawab. Untuk informasi selengkapnya, lihat Berbagi sumber daya di Oracle AWS Database@.	Juni 26, 2025
Oracle Database@AWS mendukung acara di Amazon EventBridge	Oracle Database@AWS mengirimkan peristiwa ke Amazon EventBridge untuk memantau perubahan siklus hidup sumber daya. Acara dihasilkan dari keduanya AWS dan sumber OCI, memungkinkan Anda untuk melacak perubahan pada jaringan ODB, infrastruktur Exadata, cluster VM, dan database. Untuk informasi selengkapnya, lihat Memantau Oracle Database@AWS peristiwa di Amazon EventBridge.	Juni 26, 2025

Oracle Database@AWS mendukung Langganan lintas wilayah	Oracle Database@AWS mendukung langganan lintas wilayah, memungkinkan Anda untuk berlangganan sekali dan menggunakan layanan di semua yang tersedia Wilayah AWS. Untuk informasi selengkapnya, lihat Berlangganan Oracle Database@AWS di beberapa Wilayah.	Juni 26, 2025
Oracle Database@AWS mendukung koneksi peering ODB sebagai sumber daya terpisah	Koneksi peering ODB sekarang menjadi sumber daya terpisah dengan didedikasikan APIs untuk membuat, melihat, dan menghapus koneksi peering. Anda dapat membuat koneksi peering antara jaringan ODB dan VPC Amazon di akun yang sama atau di akun yang berbeda. Untuk informasi selengkapnya, lihat Bekerja dengan Koneksi Peering ODB.	Juni 26, 2025
Oracle Database@AWS mengintegrasikan jaringan ODB dengan Amazon S3	Oracle Database@AWS sekarang terintegrasi dengan VPC Lattice untuk mengaktifkan cadangan terkelola Oracle ke Amazon S3 dan akses jaringan ODB langsung ke Amazon S3. Untuk informasi selengkapnya, lihat Integrasi layanan untuk Oracle Database@.AWS	Juni 26, 2025

Oracle Database@AWS mendukung cluster VM otonom	Anda sekarang dapat membuat cluster VM Otonom di infrastruktur Exadata Anda. Cluster VM otonom adalah database yang dikelola sepenuhnya yang mengotomatiskan tugas manajemen utama menggunakan pembelajaran mesin dan AI. Untuk informasi selengkapnya, lihat Langkah 3: Membuat klaster Exadata VM atau cluster VM Otonom di. Oracle Database@AWS	28 Mei 2025
Oracle Database@AWS mendukung jendela pemeliharaan yang dapat disesuaikan	Anda sekarang dapat mengonfigurasi jendela pemeliharaan untuk infrastruktur Exadata Anda dengan opsi untuk jadwal yang dikelola Oracle atau yang dikelola Pelanggan. Anda juga dapat memilih mode patching (Rolling atau Non-rolling) dan menentukan preferensi waktu pemeliharaan. Untuk informasi selengkapnya, lihat Membuat infrastruktur Oracle Exadata di. Oracle Database@AWS	1 Mei 2025
Oracle Database@AWS mendukung Availability Zone (AZ) baru	Anda sekarang dapat membuat jaringan ODB di AZ dengan ID fisik `use1-az4` atau`use1-az6`. Untuk informasi selengkapnya, lihat Infrastruktur Oracle Exadata.	26 Maret 2025

Oracle Database@AWS mendukung Amazon VPC Transit Gateway	Jika Anda menghubungkan gateway transit ke VPC yang diintip ke jaringan ODB, Anda dapat menghubun gkan beberapa VPCs ke gateway ini. Aplikasi yang berjalan di dalamnya VPCs dapat mengakses cluster Exadata VM yang berjalan di jaringan ODB Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi Gateway Transit VPC Amazon untuk. Oracle Database@AWS	26 Maret 2025
Oracle Database@AWS mendukung database dan tipe server penyimpanan untuk Exadata X11M	Anda dapat menentukan jenis server database dan jenis server penyimpanan saat Anda membuat infrastruktur menggunakan Exadata X11M. Untuk informasi selengkap nya, lihat Membuat infrastru ktur Oracle Exadata di. Oracle Database@AWS	Februari 4, 2025
Kebijakan peran terkait layanan baru	Oracle Database@AWS menambahkan kebijakan baru `AmazonODBServiceRo lePolicy` untuk peran `AWSServiceRoleForO DB` terkait layanan. Untuk informasi selengkapnya, lihat Oracle Database@AWS pembaruan kebijakan AWS terkelola.	Desember 2, 2024

Rilis awal	Rilis awal Panduan Oracle Database@AWS Pengguna	Desember 2, 2024

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.