Oracle Database@AWS Guia do usuário

Oracle Database@AWS

Oracle Database@AWS: Oracle Database@AWS Guia do usuário

Table of Contents

O que é Oracle Database@AWS?

Oracle Database@AWS é uma oferta que permite acessar a infraestrutura Oracle Exadata gerenciada pela Oracle Cloud Infrastructure (OCI) dentro AWS dos data centers. Você pode migrar suas cargas de trabalho do Oracle Exadata, estabelecer conectividade de baixa latência com aplicativos em AWS execução e integrar-se aos serviços. AWS Você recebe uma única fatura AWS Marketplace, que conta para AWS compromissos e recompensas do Oracle Support.

O diagrama a seguir mostra uma visão geral de alto nível de uma região OCI vinculada a um AWS data center que hospeda a infraestrutura Oracle Exadata. Dentro de uma zona de AWS disponibilidade (AZ), você pode conectar uma Amazon VPC a uma rede privada vinculada ao data center. Ao emparelhar essas redes, os servidores de aplicativos na VPC podem acessar bancos de dados Oracle em execução na infraestrutura Oracle Exadata.

Características do Oracle Database@AWS

Com Oracle Database@AWS, você se beneficia dos seguintes recursos:

Migração das cargas de trabalho do banco de dados Oracle Exadata para AWS

> Com Oracle Database@AWS, você pode migrar facilmente suas cargas de trabalho do Oracle Exadata para o Oracle Exadata Database Service na infraestrutura dedicada ou o Oracle Autonomous Database na infraestrutura dedicada do Exadata. AWS A migração oferece mudanças mínimas, disponibilidade total de recursos, compatibilidade arquitetônica e o mesmo desempenho das implantações locais do Exadata. Você pode usar ferramentas padrão de migração de banco de dados Oracle, como Recovery Manager (RMAN), Oracle Data Guard, espaços de tabela transportáveis, Oracle Data Pump, Oracle, Database Migration GoldenGate Service e Oracle AWS Zero Downtime Migration.

Latência reduzida do aplicativo

> Você pode estabelecer conectividade de baixa latência entre o Oracle Exadata e os aplicativos executados nele. AWS A proximidade de aplicativos hospedados em AWS garante atrasos mínimos na rede e melhor desempenho.

Inovação por meio da unificação de dados

> Você pode gerar insights mais profundos e desenvolver novas inovações usando integrações sem ETL para unificar seus dados na Oracle e AWS para análises, aprendizado de máquina e IA

generativa. Com a integração Zero-ETL usando o Amazon Redshift, você pode habilitar análises e aprendizado de máquina (ML) quase em tempo real em dados transacionais armazenados em. Oracle Database@AWS

Gerenciamento e operações simplificados

Você pode se beneficiar de uma experiência unificada entre a Oracle e AWS com suporte, compras, gerenciamento e operações colaborativos. Seu uso dos serviços do Oracle Database se qualifica para seus AWS compromissos existentes e benefícios de licença da Oracle, como o Oracle Support Rewards. Você pode usar AWS ferramentas e interfaces familiares para comprar, provisionar e gerenciar seus Oracle Database@AWS recursos. Você pode provisionar e gerenciar seus recursos usando AWS APIs CLI ou. SDKs Em seguida, AWS APIs chame a OCI correspondente APIs necessária para provisionar e gerenciar os recursos.

Integração perfeita com serviços AWS

Você pode se integrar com outros AWS serviços e aplicativos executados no mesmo ambiente. Por exemplo, Oracle Database@AWS integra-se à Amazon EC2, Amazon VPC e IAM. Você também pode se integrar Oracle Database@AWS a AWS serviços como Amazon CloudWatch para monitoramento e Amazon EventBridge para gerenciamento de eventos. Para backups de banco de dados, você pode usar o Amazon S3, que foi projetado para exceder 11 9s de durabilidade.

Relacionado Serviços da AWS

Oracle Database@AWS trabalha com os seguintes serviços para melhorar a disponibilidade e a escalabilidade de seus aplicativos de banco de dados Oracle:

- Amazon EC2 — Fornece servidores virtuais que funcionam como servidores de aplicativos Oracle. Você pode configurar seu balanceador de carga para rotear o tráfego para seus servidores de EC2 aplicativos. Para obter mais informações, consulte o Guia EC2 do usuário da Amazon.
- Amazon Virtual Private Cloud (VPC) — Permite que você inicie AWS recursos em uma rede virtual logicamente isolada que você definiu. A infraestrutura do Oracle Exadata reside em uma rede especial chamada rede ODB, que você pode conectar a uma VPC. Em seguida, você pode executar servidores de aplicativos em sua VPC e acessar seus bancos de dados Exadata. Para saber mais, consulte o Manual do usuário da Amazon VPC.
- Amazon VPC Lattice — fornece acesso nativo a AWS serviços como Amazon S3 e backups gerenciados pela Oracle a partir da rede ODB. Para obter mais informações, consulte o artigo O que é o Amazon VPC Lattice? .

- Amazon CloudWatch — Fornece um serviço de monitoramento para Oracle Database@AWS. A OCI reúne dados métricos sobre seu sistema Oracle Exadata e os envia para o. CloudWatch Para obter mais informações, consulte Monitoramento Oracle Database@AWS com a Amazon CloudWatch.
- AWS Identity and Access Management (IAM) — Ajuda você a controlar com segurança o acesso aos Oracle Database@AWS recursos para seus usuários. Use o IAM para controlar quem pode usar seus AWS recursos (autenticação) e quais recursos os usuários podem usar de quais formas (autorização). Para obter mais informações, consulte Gerenciamento de identidade e acesso para Oracle Database@AWS.
- AWS serviços de análise — forneça um conjunto amplo e econômico de serviços de análise para ajudá-lo a obter insights mais rapidamente do seu banco de dados Exadata. Cada serviço é desenvolvido especificamente para uma ampla variedade de casos de uso de análise, como análise interativa, processamento de big data, armazenamento de dados, análise em tempo real, análise operacional, painéis e visualizações. Para obter mais informações, consulte Analytics on AWS.

Acessando Oracle Database@AWS

Você pode criar, acessar e gerenciar Oracle Database@AWS usando Console de gerenciamento da AWS o. Ele fornece uma interface da web que você pode usar para acessar Oracle Database@AWS.

Preços para Oracle Database@AWS

Você pode comprar Oracle Database@AWS ofertas em. AWS Marketplace Primeiro, entre em contato com um representante de vendas da Oracle. A Oracle então disponibiliza a oferta para você AWS Marketplace com base no contrato de preços privado. Sua AWS fatura mostra cobranças com base no seu uso.

Não há cobranças de transferência de dados quando o aplicativo Oracle e o banco de dados Oracle estão hospedados na mesma Zona de Disponibilidade (AZ). Taxas padrão de transferência de dados se aplicam à comunicação entre AZs.

Ao usar integrações Oracle Database@AWS gerenciadas, como Zero-ETL, backups gerenciados pela Oracle e Amazon S3, são aplicadas taxas padrão de processamento de dados para compartilhar e acessar recursos por meio do VPC Lattice. Não há cobrança horária para integrações

Oracle Database@AWS gerenciadas. Para obter mais informações, consulte os preços do Amazon VPC Lattice.

Próximas etapas

Agora você está pronto para começar a criar seus Oracle Database@AWS recursos.

1. Saiba mais sobre como Oracle Database@AWS funciona. Para obter mais informações, consulte Como Oracle Database@AWS funciona.

   > **Note**
   >
   > Se você estiver familiarizado com AWS o Oracle Exadata e quiser começar imediatamente, pule esta etapa.

2. Solicite uma oferta privada por Oracle Database@AWS meio do e Console de gerenciamento da AWS, em seguida, aceite a oferta. Para obter mais informações, consulte Solicite uma oferta privada para o Oracle Database@AWS.

   > **Note**
   >
   > Para solicitar uma oferta privada nesta prévia, você deve entrar em contato AWS para Conta da AWS adicioná-la a uma lista de permissões.

3. Crie sua rede ODB, infraestrutura Oracle Exadata e clusters de VM do Exadata usando o console. AWS Crie seus bancos de dados Exadata usando as ferramentas OCI. Para obter mais informações, consulte Introdução ao Oracle Database@AWS.
4. Compartilhe seus recursos entre contas com AWS Resource Access Manager (AWS RAM). Para obter mais informações, consulte Trabalhando com Oracle Database@AWS recursos compartilhados em uma conta confiável.

Como Oracle Database@AWS funciona

Oracle Database@AWS integra o Oracle Cloud Infrastructure (OCI) com o. Nuvem AWS Nas seções a seguir, você pode aprender sobre os principais componentes dessa arquitetura multicloud.

O Oracle Exadata Database Service on Dedicated Infrastructure é um serviço OCI que fornece o Exadata Database Machine. O Oracle Exadata Database Machine é uma plataforma full-stack integrada, pré-configurada e pré-testada para uso em data centers corporativos. Você pode criar a infraestrutura do Oracle Exadata e os clusters de VM em uma zona de AWS disponibilidade (AZ) usando o console AWS , a CLI ou. APIs

Depois de criar seus recursos no AWS, você usa o OCI APIs para criar e gerenciar bancos de dados Oracle Exadata. Uma rede ODB, que você conecta a uma Amazon VPC, permite que os servidores de EC2 aplicativos da Amazon acessem seus bancos de dados do Exadata. Dessa forma, os bancos de dados Oracle Exadata são integrados ao AWS ambiente.

O diagrama a seguir mostra a Oracle Database@AWS arquitetura.

Sites secundários da OCI

O Oracle Cloud Infrastructure é hospedado em regiões e domínios de disponibilidade da OCI. Uma região OCI consiste em domínios de disponibilidade OCI (ADs), que são clusters de data center isolados dentro de uma região OCI. Um site secundário do OCI é um data center que estende um domínio de disponibilidade do OCI para uma zona de disponibilidade (AZ) em uma AWS região. A infraestrutura do Exadata reside logicamente em uma região da OCI e reside fisicamente em uma região. AWS

O site secundário da OCI reside Oracle Database@AWS fisicamente em um AWS data center. AWS hospeda a infraestrutura do Exadata, e a OCI provisiona e mantém o hardware da infraestrutura do Exadata dentro do data center. Você pode configurar a infraestrutura, a rede privada e os clusters de VM do Exadata usando o console AWS , a CLI ou o. APIs Você pode usar AWS serviços como Amazon EC2 e Amazon VPC para permitir o acesso de aplicativos aos bancos de dados Oracle Exadata em execução na infraestrutura.

Infraestrutura Oracle Exadata

A infraestrutura do Oracle Exadata é a arquitetura subjacente dos servidores de banco de dados e servidores de armazenamento que executa os bancos de dados Oracle Exadata. A infraestrutura reside em uma zona de AWS disponibilidade (AZ). Para criar clusters de VM na infraestrutura do Exadata, você usa o console AWS , a CLI ou. APIs

A infraestrutura do Oracle Exadata é distribuída em máquinas físicas chamadas servidores de banco de dados. Esses servidores fornecem os recursos computacionais, semelhantes aos servidores EC2 dedicados da Amazon. Cada servidor de banco de dados hospeda uma ou mais máquinas virtuais (VMs) em execução em um hipervisor. Para diagramas de arquitetura que ilustram essas relações, consulte Exadata Database Service on Dedicated Infrastructure Technical Architecture.

Ao criar a infraestrutura do Exadata no Oracle Database@AWS, você especifica informações como as seguintes:

- O número total de servidores de banco de dados
- O número total de servidores de armazenamento
- O modelo do sistema Exadata (X11M)
- A AZ que hospeda a infraestrutura (consulteRegiões suportadas para Oracle Database@AWS)

Para saber como criar a infraestrutura Oracle Exadata, consulte. Etapa 2: Criar uma infraestrutura Oracle Exadata no Oracle Database@AWS

Rede ODB

Uma rede ODB é uma rede privada isolada que hospeda a infraestrutura OCI em uma Zona de AWS Disponibilidade (AZ). A rede ODB consiste em um intervalo CIDR de endereços IP. A rede ODB mapeia diretamente para a rede que existe dentro do site secundário da OCI, servindo assim como meio de comunicação entre AWS e a OCI. Você deve especificar uma rede ODB ao criar seus clusters de VM do Exadata (consulte). Etapa 3: criar um cluster de VM Exadata ou um cluster de VM autônoma no Oracle Database@AWS

Você provisiona recursos em uma rede ODB usando o Oracle AWS APIs Database@. A rede ODB é gerenciada por AWS, mas você pode configurar uma conexão de emparelhamento ODB para

conectar uma Amazon VPC à rede ODB. Para obter mais informações, consulte enEmparelhamento ODB.

Ao criar uma rede ODB, você especifica informações como as seguintes:

- Zona de disponibilidade — A rede ODB é específica para uma AZ.

  Você pode usar Oracle Database@AWS o seguinte Regiões da AWS:

  Leste dos EUA (Norte da Virgínia)

  Você pode usar o AZs com o físico IDs `use1-az4` `use1-az6` e.

  Oeste dos EUA (Oregon)

  Você pode usar o AZs com o físico IDs `usw2-az3` `usw2-az4` e.

  Ásia-Pacífico (Tóquio)

  Você pode usar o AZs com o físico IDs `apne1-az1` `apne1-az4` e.

  Leste dos EUA (Ohio)

  Você pode usar o AZs com o físico IDs `use2-az1` `use2-az2` e.

  Europa (Frankfurt)

  Você pode usar o AZs com o físico IDs `euc1-az1` `euc1-az2` e.

  Canadá (Central)

  Você pode usar o AZ com o ID físico`cac1-az4`.

  Ásia-Pacífico (Sydney)

  Você pode usar o AZ com o ID físico`apse2-az4`.

  Para encontrar os nomes lógicos de AZ em sua conta que são mapeados para a AZ física anterior IDs, execute o comando a seguir.

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

- Endereços CIDR do cliente — A rede ODB requer um CIDR de sub-rede cliente para clusters de VM do Exadata e clusters de VM autônomos.

- Backup de endereços CIDR — A rede ODB requer um CIDR de sub-rede de backup para backups gerenciados de bancos de dados de clusters de VM. A sub-rede de backup é opcional para clusters de VM do Exadata.
- AWS integrações de serviços — Você pode configurar um caminho de rede para integrações de AWS serviços como Amazon S3 e Zero-ETL com o Amazon Redshift. Para obter mais informações, consulte AWS integrações de serviços.

Para obter mais informações, consulte Etapa 1: Criar uma rede ODB no Oracle Database@AWS.

Nuvem privada virtual (VPC)

Uma Virtual Private Cloud (VPC) é uma rede virtual que você cria na nuvem. AWS Ele é logicamente isolado de outras redes virtuais na AWS nuvem, fornecendo controle total sobre o ambiente de rede virtual, incluindo a seleção do seu próprio intervalo de endereços IP, a criação de sub-redes e a configuração de tabelas de rotas e gateways de rede. Para obter mais informações, consulte O que é Amazon VPC?

Você pode iniciar EC2 instâncias da Amazon em sua Amazon VPC. As EC2 instâncias podem hospedar servidores de aplicativos que se comunicam com bancos de dados Oracle Exadata. Você pode gerenciar e iniciar os servidores de aplicativos da mesma forma que qualquer outra EC2 instância na sua VPC. Para obter mais informações, consulte O que é a Amazon EC2?

Por padrão, a rede ODB não tem conectividade com o. VPCs Para conectar a rede ODB à sua AWS infraestrutura existente, crie uma conexão de peering entre a rede ODB e uma VPC. Você pode especificar a VPC ao criar a rede ODB. Para obter mais informações, consulte Etapa 1: Criar uma rede ODB no Oracle Database@AWS.

Emparelhamento ODB

O emparelhamento ODB é uma conexão de rede criada pelo usuário que permite que o tráfego seja roteado de forma privada entre uma Amazon VPC e uma rede ODB. Há uma relação 1:1 entre uma VPC e uma rede ODB. Depois do peering, uma EC2 instância da Amazon dentro da VPC pode se comunicar com um banco de dados Oracle Exadata na rede ODB como se estivesse na mesma rede.

> **Note**
>
> O emparelhamento ODB é diferente do emparelhamento de VPC, que é uma conexão de emparelhamento entre dois VPCs que roteia o tráfego entre eles.

Você pode emparelhar uma rede ODB em uma conta e uma VPC em outra conta usando. AWS RAM Se você compartilha uma rede ODB com outra conta, a conta confiável pode iniciar diretamente o peering. A conta que inicia a conexão de emparelhamento ODB possui e gerencia a conexão.

Você pode especificar a rede ponto a ponto CIDRs ao criar ou atualizar conexões de emparelhamento ODB. Dessa forma, você controla quais sub-redes na VPC de mesmo nível têm acesso à sua rede ODB. Uma conta VPC pode atualizar os intervalos CIDR sem também possuir a rede ODB. Para obter mais informações, consulte Configurando o emparelhamento de ODB para uma Amazon VPC em. Oracle Database@AWS

Os recursos em uma VPC podem abranger zonas de disponibilidade ()AZs. Em uma rede ODB, os recursos são vinculados a uma única AZ. Você define essa AZ ao criar a rede ODB.

Criação de uma conexão de emparelhamento ODB

Uma conexão de emparelhamento ODB não é uma característica de uma rede ODB, mas é um recurso independente com seu próprio ID (prefixado com`odbpcx-`) e ciclo de vida. Você gerencia uma conexão de emparelhamento com um conjunto dedicado APIs. Por exemplo, você cria uma conexão de emparelhamento ODB com uma rede ODB existente usando o console Oracle Database@AWS ou a API. `CreateOdbPeeringConnection` Para obter mais informações, consulte Criando uma conexão de emparelhamento ODB no Oracle Database@AWS.

Quando você cria uma conexão de emparelhamento ODB, o Oracle Database@AWS executa as seguintes ações automaticamente:

1. Valida as configurações de rede, incluindo a verificação da sobreposição de blocos CIDR com o Oracle VCN CIDR
2. Configura a infraestrutura de emparelhamento de rede subjacente
3. Configura as tabelas de rotas da rede ODB (não a VPC) com os endereços CIDR da VPC

Depois de criar sua conexão de emparelhamento ODB, atualize suas tabelas de rotas de VPC manualmente usando o comando Amazon. EC2 `create-route` Para obter mais informações, consulte Configurando tabelas de rotas VPC para emparelhamento de ODB.

AWS integrações de serviços

Para fornecer funcionalidade aprimorada e opções de conectividade para seus bancos de dados Oracle, o Oracle Database@AWS se integra ao uso do Serviços da AWS Amazon VPC Lattice. Você pode configurar caminhos de rede Serviços da AWS diretamente da sua rede ODB sem precisar de configurações de rede adicionais VPCs ou complexas.

O Oracle Database@AWS oferece suporte às seguintes integrações de serviços AWS gerenciados:

Amazon S3

Você pode integrar o Amazon S3 com o Oracle Database@ das seguintes formas AWS :

- Backups automáticos gerenciados pela Oracle no Amazon S3 — o Oracle Database@ habilita AWS automaticamente o acesso à rede para backups automáticos. Essa integração não pode ser desativada. Se você definir o Amazon S3 como seu destino de backup gerenciado no console do OCI, o OCI carregará backups automáticos em um bucket do S3.
- Acesso direto ao Amazon S3 a partir da sua rede ODB — Você pode habilitar o acesso direto da rede ODB ao S3 e, em seguida, armazenar scripts, importar e exportar arquivos e arquivos relacionados em um bucket do S3. Você pode desativar esse acesso. Essa configuração é independente do acesso automático à rede para backups automáticos gerenciados pela Oracle.

Integração ETL zero com o Amazon Redshift

Você pode habilitar a integração sem ETL da sua rede ODB com o Amazon Redshift. Essa integração permite que você replique dados para o Amazon Redshift a partir de seus bancos de dados Oracle em execução no Oracle AWS Database@ sem o processo tradicional de extração, transformação e carregamento (ETL). Essa integração permite análises em tempo real e cargas de trabalho de IA ao sincronizar automaticamente seus dados Oracle com o Amazon Redshift.

Além das integrações gerenciadas para AWS serviços, você também pode usar o VPC Lattice para acessar serviços e recursos hospedados em VPCs outros, ou acessar instâncias de rede ODB a partir da sua VPC. Você pode gerenciar o acesso e os recursos usando o console VPC Lattice, a CLI e. APIs Para saber mais, consulte os seguintes recursos:

- Fazendo backup no Oracle Database@AWS
- Integração do Oracle Database@AWS Zero-ETL com o Amazon Redshift
- O que é o Amazon VPC Lattice? e VPC Lattice para Oracle Database@AWS

Roteamento de tráfego de vários VPCs

Para permitir que vários VPCs acessem Oracle Database@AWS recursos em uma rede ODB, você pode usar o AWS Transit Gateway AWS Cloud WAN.

AWS Transit Gateway

Um gateway de trânsito da Amazon VPC é um hub de trânsito de rede usado para interconectar VPCs redes locais. Uma rede ODB oferece suporte somente ao peering one-to-one direto entre a rede ODB e uma única VPC. Você pode emparelhar sua rede ODB para uma VPC e, em seguida, anexar essa VPC a um gateway de trânsito. O gateway pode se conectar a vários VPCs. Com essa configuração de gateway de trânsito, você pode rotear o tráfego entre várias sub-redes VPC para uma única rede ODB.

Para obter mais informações, consulte Configurando os Amazon VPC Transit Gateways para Oracle Database@AWS.

AWS WAN em nuvem

AWS O Cloud WAN é um serviço gerenciado de rede de área ampla (WAN) que permite criar, gerenciar e monitorar uma rede global unificada conectando recursos em seus ambientes locais e na nuvem. Usando o painel central, você pode conectar filiais locais, data centers e VPCs toda a rede AWS global.

Você pode emparelhar sua rede ODB para uma VPC e, em seguida, anexar essa VPC à rede principal do Cloud WAN. Com essa configuração, você pode usar o Cloud WAN para rotear o tráfego entre redes múltiplas VPCs ou locais e sua rede ODB. Para obter mais informações, consulte Configurando o AWS Cloud WAN para Oracle Database@AWS.

Clusters de VM do Exadata

Um cluster de VM do Exadata é um conjunto de Exadata fortemente acoplados. VMs Cada VM tem uma instalação completa do banco de dados Oracle que inclui todos os recursos do Oracle

Enterprise Edition, incluindo o Oracle Real Application Clusters (Oracle RAC) e o Oracle Grid Infrastructure. Você pode criar um ou mais bancos de dados Oracle Exadata em um cluster de VM. Para diagramas que mostram a arquitetura VMs e os clusters de VM, consulte Exadata Database Service on Dedicated Infrastructure Technical Architecture.

Ao criar um cluster de VM, você especifica informações que incluem o seguinte:

- Uma rede ODB
- Uma infraestrutura Oracle Exadata
- Os servidores de banco de dados nos quais colocar o VMs no cluster
- A quantidade total de armazenamento utilizável do Exadata

Você pode configurar os núcleos da CPU, a memória e o armazenamento local para cada VM em um cluster de VM. Para obter mais informações, consulte Etapa 3: criar um cluster de VM Exadata ou um cluster de VM autônoma no Oracle Database@AWS.

Clusters de VM autônomos

Os clusters de VM autônomos são bancos de dados totalmente gerenciados que automatizam as principais tarefas de gerenciamento usando aprendizado de máquina e IA. Diferentemente dos bancos de dados tradicionais, os bancos de dados autônomos provisionam, protegem, atualizam, fazem backup e ajustam automaticamente o banco de dados sem a necessidade de intervenção humana.

Você pode configurar a contagem de núcleos da ECPU por VM, a memória do banco de dados por CPU, o armazenamento do banco de dados e o número máximo de bancos de dados de contêineres autônomos. Para obter mais informações, consulte Etapa 3: criar um cluster de VM Exadata ou um cluster de VM autônoma no Oracle Database@AWS.

Bancos de dados Oracle Exadata

O Oracle Exadata é um sistema projetado que fornece uma plataforma de alto desempenho para executar bancos de dados Oracle. Com Oracle Database@AWS, você usa o AWS console para criar a infraestrutura do Oracle Exadata e os clusters de VM que hospedam os bancos de dados Exadata. Em seguida, você usa o OCI APIs para criar e gerenciar os bancos de dados Oracle. Para obter mais informações, consulte Etapa 4: Crie bancos de dados Oracle Exadata no Oracle Cloud Infrastructure.

Integração ao Oracle Database@AWS

Antes de começar a usar Oracle Database@AWS, certifique-se de estar inscrito AWS e criar os usuários necessários. Em seguida, você pode comprar o Oracle Database@AWS AWS Marketplace aceitando uma oferta privada da Oracle.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS Centro de Identidade do AWS IAM, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login Console de gerenciamento da AWScomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS .

2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

   Para obter instruções, consulte Habilitar o Centro de Identidade do AWS IAM no Guia do usuário do Centro de Identidade do AWS IAM .

2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia Centro de Identidade do AWS IAM do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de logon único ao grupo.

Para obter instruções, consulte Adicionar grupos no Guia do usuário do Centro de Identidade do AWS IAM .

Solicite uma oferta privada para o Oracle Database@AWS

O recurso de oferta privada do AWS Marketplace vendedor permite que você solicite e receba os AWS preços e os termos do EULA do Oracle Database@ da Oracle. Você negocia preços e condições com a Oracle e, em seguida, a Oracle cria uma oferta privada para a Conta da AWS que você designar. Você aceita a oferta privada e recebe o preço negociado e os termos de uso. Neste momento, você pode usar o Oracle Database@AWS painel. Quando o contrato de oferta privada atinge a data de expiração, você passa automaticamente para o preço público do produto ou cancela a assinatura do Oracle Database@.AWS Para obter mais informações sobre ofertas privadas, consulte Ofertas privadas em AWS Marketplace.

Para solicitar e aceitar uma oferta privada para Oracle Database@AWS

1. Faça login no Console de gerenciamento da AWS.
2. Pesquise e escolha Oracle Database@AWS.
3. Escolha Solicitar oferta privada.

> **Note**
>
> O Oracle Database@AWS painel não estará disponível até que você aceite uma oferta privada.

4. No site do Oracle Cloud Infrastructure (OCI), especifique detalhes como a região e suas informações de contato.
5. Aguarde até que um representante da OCI entre em contato com você e disponibilize uma oferta privada.
6. Em Console de gerenciamento da AWS, escolha Exibir oferta privada.
7. Escolha a oferta e, em seguida, escolha Exibir oferta.
8. Escolha Criar contrato e responda às solicitações subsequentes para aceitar a oferta privada.
9. Depois de aceitar a oferta privada, você precisará ativar sua conta OCI. Você pode acessar os links de ativação da Oracle diretamente de Console de gerenciamento da AWS.

    1. No console, navegue até a seção Introdução.

2. Clique no link de ativação da Oracle fornecido no console. Como alternativa, você também pode usar o link de ativação enviado por e-mail.
3. Na página de ativação da Oracle, escolha se deseja criar uma nova conta Oracle Cloud ou adicioná-la a uma conta existente.
4. Conclua o processo de ativação seguindo as instruções na tela.
5. Depois de enviar sua solicitação de ativação, você verá o status de Ativação em andamento no Console de gerenciamento da AWS, e o painel será temporariamente desativado com um motivo exibido.
6. Após a conclusão da ativação, o AWS painel do Oracle Database@ fica disponível, permitindo que você gerencie seus recursos.

10. No Console de gerenciamento da AWS, escolha Painel.

Assine o Oracle Database@AWS em várias regiões

Quando você se inscreve AWS Marketplace e conclui a Oracle Database@AWS integração, você Conta da AWS está vinculado à sua locação da OCI. Esse link, junto com os recursos relacionados, é replicado automaticamente para todas as AWS regiões onde Oracle Database@AWS está disponível. Você se inscreve e se inscreve uma vez, em vez de repetir o processo para cada região.

Para usar Oracle Database@AWS em várias regiões, execute as seguintes etapas:

1. Inscreva-se AWS Marketplace e Oracle Database@AWS conclua o processo de integração.

   Quando você assina o Oracle Database@ pela primeira vez AWS, sua conta é ativada em uma região de origem. Você especifica a região inicial no Oracle Cloud Infrastructure (OCI).
2. Ative suas regiões preferidas por meio do console OCI.

   Se você não habilitar uma região no OCI e depois alternar para essa região no Oracle Database@AWS console, receberá um erro informando que você não se inscreveu. Nesse caso, você deve habilitar essa região no OCI antes de poder usar o Oracle Database@AWS painel nessa região.
3. Acesse Oracle Database@AWS em qualquer AWS região compatível sem repetir o processo de assinatura.

Introdução ao Oracle Database@AWS

Para começar a usar Oracle Database@AWS, você pode criar os seguintes recursos usando o Oracle Database@AWS console, a CLI ou: APIs

1. Rede ODB
2. Infraestrutura Oracle Exadata
3. Cluster de VM Exadata ou cluster de VM autônoma
4. Conexão de emparelhamento ODB

Para criar bancos de dados Oracle Exadata em sua infraestrutura, você deve usar o console do Oracle Cloud Infrastructure (OCI) ou APIs não o painel. Oracle Database@AWS Assim, você implanta recursos em dois ambientes de nuvem: os recursos de rede e infraestrutura estão dentro AWS, enquanto o plano de controle de administração do banco de dados está na OCI. Para obter mais informações, consulte Oracle Database@AWSa documentação do Oracle Cloud Infrastructure.

Pré-requisitos para configuração Oracle Database@AWS

Antes de configurar sua infraestrutura Oracle Exadata, certifique-se de fazer o seguinte:

- Siga as etapas em Integração ao Oracle Database@AWS. Você deve ter aceitado uma oferta privada para usar Oracle Database@AWS.
- Conceda ao diretor do IAM as permissões de política listadas emPermita que os usuários provisionem Oracle Database@AWS recursos. Essas permissões são necessárias para uso Oracle Database@AWS.

Serviços OCI suportados em Oracle Database@AWS

Oracle Database@AWS suporta os seguintes serviços do Oracle Cloud Infrastructure (OCI):

- Oracle Exadata Database Service em infraestrutura dedicada — fornece um ambiente Exadata totalmente gerenciado e dedicado, acessível internamente. AWS Para obter mais informações, consulte Oracle Cloud Exadata Database Service on Dedicated Infrastructure na documentação da OCI.

- Banco de dados autônomo em infraestrutura dedicada do Exadata — fornece um ambiente de banco de dados altamente automatizado e totalmente gerenciado executado no OCI com recursos de hardware e software comprometidos. Para obter mais informações, consulte Sobre o banco de dados autônomo na infraestrutura dedicada do Exadata na documentação da OCI.

Regiões suportadas para Oracle Database@AWS

Você pode usar Oracle Database@AWS o seguinte Regiões da AWS:

Leste dos EUA (Norte da Virgínia)

Você pode usar o AZs com o físico IDs `use1-az4` `use1-az6` e.

Oeste dos EUA (Oregon)

Você pode usar o AZs com o físico IDs `usw2-az3` `usw2-az4` e.

Ásia-Pacífico (Tóquio)

Você pode usar o AZs com o físico IDs `apne1-az1` `apne1-az4` e.

Leste dos EUA (Ohio)

Você pode usar o AZs com o físico IDs `use2-az1` `use2-az2` e.

Europa (Frankfurt)

Você pode usar o AZs com o físico IDs `euc1-az1` `euc1-az2` e.

Canadá (Central)

Você pode usar o AZ com o ID físico`cac1-az4`.

Ásia-Pacífico (Sydney)

Você pode usar o AZ com o ID físico`apse2-az4`.

Para encontrar os nomes lógicos de AZ em sua conta que são mapeados para a AZ física anterior IDs, execute o comando a seguir.

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

Planejando o espaço de endereço IP em Oracle Database@AWS

Planeje cuidadosamente a entrada de espaço de endereço IP Oracle Database@AWS. Considere o consumo de endereços IP com base no número de clusters de VM, incluindo o número VMs por cluster que você pode provisionar na rede ODB. Para obter mais informações, consulte ODB Network Design na documentação do Oracle Cloud Infrastructure.

Tópicos

Restrições para endereços IP na rede ODB

Observe as seguintes restrições em relação aos intervalos de CIDR na rede ODB:

- Você não pode modificar o intervalo CIDR da sub-rede do cliente ou da sub-rede de backup para a rede ODB depois de criá-la.
- Você não pode usar os intervalos de CIDR da VPC na coluna Associações restritas na tabela em Restrições de associação de blocos IPv4 CIDR.
- Para o Exadata X9M, os endereços IP 100.106.0.0/16 e 100.107.0.0/16 são reservados para a interconexão do cluster pela automação OCI, portanto, você não pode fazer o seguinte:
  - Atribua esses intervalos ao intervalo CIDR do cliente ou de backup da rede ODB.
  - Use esses intervalos para um CIDR VPC usado para se conectar à rede ODB.
- Os seguintes intervalos CIDR são reservados para o Oracle Cloud Infrastructure e não podem ser usados para a rede ODB:
  - Intervalo reservado CIDR 169.254.0.0/16 do Oracle Cloud
  - Classe reservada D 224.0.0.0 — 239.255.255.255
  - Classe reservada E 240.0.0.0 — 255.255.255.255
- Você não pode sobrepor os intervalos de CIDR de endereços IP para as sub-redes cliente e de backup.
- Você não pode sobrepor os intervalos CIDR de endereços IP alocados para as sub-redes cliente e de backup com os intervalos CIDR da VPC usados para se conectar à rede ODB.

- Você não pode provisionar VMs em um cluster de VM em diferentes redes ODB. A rede é uma propriedade do cluster da VM, o que significa que você só pode provisionar o do VMs cluster da VM na mesma rede ODB.

Requisitos CIDR da sub-rede do cliente para a rede ODB

Na tabela a seguir, você pode encontrar o número de endereços IP consumidos pelo serviço e pela infraestrutura para o CIDR da sub-rede do cliente. O tamanho mínimo do CIDR para a sub-rede do cliente é /27 e o tamanho máximo é /16.

Número de endereços IP	Consumido por	Observações
6	Oracle Database@AWS	Esses endereços IP são reservados independentemente de quantos clusters de VM você provisiona na rede ODB. Oracle Database@AWS consome o seguinte: • 3 endereços IP reservados para os recursos de rede ODB em AWS • 3 endereços IP reservados para o serviço de rede OCI
3	Cada cluster de VM	Esses endereços IP são reservados para nomes de acesso de cliente único (SCANs), independentemente de quantos VMs estejam presentes em cada cluster de VM.
4	Cada VM	Esses endereços IP dependem unicamente do número de VMs na infraestrutura.

Requisitos de CIDR de sub-rede de backup para a rede ODB

Na tabela a seguir, você pode encontrar o número de endereços IP consumidos pelo serviço e pela infraestrutura para o CIDR da sub-rede de backup. O tamanho mínimo do CIDR para a sub-rede de backup é /28 e o tamanho máximo é /16.

Número de endereços IP	Consumido por	Observações
3	Oracle Database@AWS	Esses endereços IP são reservados independentemente de quantos clusters de VM você provisiona na rede ODB. Oracle Database@AWS consome o seguinte: • 2 endereços IP no início do intervalo CIDR • 1 endereço IP no final do intervalo CIDR
3	Cada VM	Esses endereços IP dependem unicamente do número de VMs na infraestrutura.

Cenários de consumo de IP para a rede ODB

Na tabela a seguir, você pode ver os endereços IP consumidos na rede ODB para diferentes configurações de clusters de VM. Considerando que /28 é o intervalo CIDR técnico mínimo para o CIDR da sub-rede do cliente implantar 1 cluster de VM com 2 VMs, recomendamos que você use pelo menos um intervalo CIDR /27. Nesse caso, o intervalo de IP não é totalmente consumido pelos clusters de VM e permite a alocação de endereços IP adicionais.

Configuração	Cliente IPs consumido	IPs Mínimo de clientes	Backup IPs consumido	Backup IPs mínimo
1 cluster de VM com 2 VMs	17 (6 serviços + 3 clusters + 4*2)	32 (intervalo CIDR /27)	9 (3 serviços + 3*2)	16 (intervalo CIDR /28)
1 cluster de VM com 3 VMs	21 (6 serviços + 3 clusters + 4*3)	32 (intervalo CIDR /27)	12 (3 serviços + 3*3)	16 (intervalo CIDR /28)
1 cluster de VM com 4 VMs	25 (6 serviços + 3 clusters + 4*4)	32 (intervalo CIDR /27)	15 (3 serviços + 3*4)	16 (intervalo CIDR /28)
1 cluster de VM com 8 VMs	41 (6 serviços + 3 clusters + 4*8)	64 (intervalo CIDR /26)	27 (3 serviços + 3*8)	32 (intervalo CIDR /27)

A tabela a seguir mostra quantas instâncias de cada configuração são possíveis, considerando um intervalo CIDR específico do cliente. Por exemplo, 1 cluster de VM com 4 VMs consome 24 endereços IP na sub-rede do cliente. Se o intervalo CIDR for /25, 128 endereços IP estarão disponíveis. Assim, você pode provisionar 5 clusters de VM na sub-rede.

Configuração do cluster de VM	Número com /27 (32 IPs)	Número com /26 (64 IPs)	Número com /25 (128 IPs)	Número com /24 (256 IPs)	Número quando /23 (IPs512)	Número quando /22 (IPs1024)
1 cluster de VM com 2 VMs (16 IPs)	1	3	7	15	30	60
1 cluster de VM com 3 VMs (20 IPs)	1	3	6	12	24	48
1 cluster de VM com 4 VMs (24 IPs)	1	2	5	10	20	40
2 clusters de VM com 2 VMs cada (27 IPs)	1	2	4	9	18	36
2 clusters de VM com 3 VMs cada (35 IPs)	0	1	3	7	14	28
2 clusters de VM com 4 VMs cada (43 IPs)	0	1	2	5	11	23

Etapa 1: Criar uma rede ODB no Oracle Database@AWS

Uma rede ODB é uma rede privada isolada que hospeda a infraestrutura OCI em uma Zona de Disponibilidade (AZ). Uma rede ODB e uma infraestrutura Oracle Exadata são pré-condições para provisionar clusters de VM e criar bancos de dados Exadata. Você pode criar a rede ODB e a infraestrutura do Oracle Exadata em qualquer ordem. Para obter mais informações, consulte Rede ODB e Emparelhamento ODB.

Essa tarefa pressupõe que você tenha lidoPlanejando o espaço de endereço IP em Oracle Database@AWS. Para modificar ou excluir a rede ODB posteriormente, consulteGerenciando o Oracle Database@AWS.

Para criar uma rede ODB

1. Faça login no Console de gerenciamento da AWS e abra o Oracle Database@AWS console em https://console.aws.amazon.com/odb/.
2. Escolha sua AWS região no canto superior direito. Para obter mais informações, consulte Regiões suportadas para Oracle Database@AWS.
3. No painel esquerdo, escolha Redes ODB.
4. Escolha Criar rede ODB.
5. Em Nome da rede ODB, insira um nome de rede. O nome deve ter de 1 a 255 caracteres e começar com um caractere alfabético ou sublinhado. Ele não pode conter hífens consecutivos.
6. Em Zona de disponibilidade, escolha um nome de AZ. Para obter suporte AZs, consulteRegiões suportadas para Oracle Database@AWS.
7. Para CIDR da sub-rede do cliente, especifique um intervalo de CIDR para as conexões do cliente. Para obter mais informações, consulte Requisitos CIDR da sub-rede do cliente para a rede ODB.
8. Para o CIDR da sub-rede de backup, especifique um intervalo de CIDR para as conexões de backup. Para isolar o tráfego de backup e melhorar a resiliência, recomendamos que você não sobreponha o CIDR de backup e o CIDR do cliente. Para obter mais informações, consulte Requisitos de CIDR de sub-rede de backup para a rede ODB.
9. Para configuração de DNS, escolha uma das seguintes opções:

   Padrão

   Em Prefixo do nome de domínio, insira um nome para usar como prefixo do seu domínio. O nome do domínio é fixado como oraclevcn.com. Por exemplo, se você inserir**`myhost`**, o nome de domínio totalmente qualificado será myhost.oraclevcn.com.

   Nome de domínio personalizado

   Em Nome do domínio, insira um nome de domínio completo. Por exemplo, você pode inserir myhost.myodb.com.
10. (Opcional) Para integrações de serviços, selecione um serviço para integrar à sua rede usando o VPC Lattice. O Oracle Database@AWS se integra a vários Serviços da AWS para fornecer opções aprimoradas de funcionalidade e conectividade para seus bancos de dados Oracle. Selecione uma das seguintes integrações:

Amazon S3

Habilite o acesso direto à rede ODB ao Amazon S3. Seus bancos de dados podem acessar o S3 para importação/exportação de dados ou backups personalizados. Você pode inserir uma política JSON. Para obter mais informações, consulte Backups gerenciados pelo usuário no Amazon S3 no Oracle Database@AWS.

Zero-ETL

Habilite análises em tempo real e aprendizado de máquina em dados transacionais usando o Amazon Redshift. Para obter mais informações, consulte Integração do Oracle Database@AWS Zero-ETL com o Amazon Redshift.

> **Note**
>
> Quando você cria sua rede ODB, o Oracle Database@ pré-configura AWS automaticamente o acesso à rede para backups gerenciados pela Oracle no Amazon S3. Você não pode ativar ou desativar essa integração. Para obter mais informações, consulte AWS integrações de serviços.

11. (Opcional) Em Tags, insira até 50 tags para a rede. Uma tag é um par de valores-chave que você pode usar para organizar e monitorar seus recursos.
12. Escolha Criar rede ODB.

Depois de criar uma rede ODB, você pode emparelhá-la para uma VPC. O emparelhamento ODB é uma conexão de rede criada pelo usuário que permite que o tráfego seja roteado de forma privada entre uma Amazon VPC e uma rede ODB. Depois do peering, uma EC2 instância da Amazon dentro da VPC pode se comunicar com recursos na rede ODB como se estivessem na mesma rede. Para obter mais informações, consulte Configurando o emparelhamento de ODB para uma Amazon VPC no Oracle Database@AWS.

Etapa 2: Criar uma infraestrutura Oracle Exadata no Oracle Database@AWS

A infraestrutura do Oracle Exadata é a arquitetura subjacente de servidores de banco de dados, servidores de armazenamento e redes que executam bancos de dados Oracle Exadata. Escolha o

Exadata X9M ou o X11M como modelo do sistema. Em seguida, você pode criar clusters de VM na infraestrutura do Exadata usando o console. AWS

Você pode criar a infraestrutura do Oracle Exadata e a rede ODB em qualquer ordem. Você não precisa especificar informações de rede ao criar a infraestrutura.

Você não pode modificar uma infraestrutura Oracle Exadata depois de criá-la. Para excluir uma infraestrutura do Exadata, consulte. Excluindo uma infraestrutura Oracle Exadata no Oracle Database@AWS

Para criar uma infraestrutura do Exadata

1. Faça login no Console de gerenciamento da AWS e abra o Oracle Database@AWS console em https://console.aws.amazon.com/odb/.
2. No painel esquerdo, escolha Infraestruturas do Exadata.
3. Escolha Criar infraestrutura do Exadata.
4. Para o nome da infraestrutura do Exadata, insira um nome. O nome deve ter de 1 a 255 caracteres e começar com um caractere alfabético ou sublinhado. Ele não pode conter hífens consecutivos.
5. Para Zona de disponibilidade, escolha uma das suportadas AZs. Escolha Próximo.
6. Para o modelo do sistema Exadata, escolha Exadata.X9M ou Exadata.X11M. Para o Exadata.X11M, escolha também os seguintes tipos de servidor:

   - Para Tipo de servidor de banco de dados, escolha o tipo de modelo de servidor de banco de dados da sua infraestrutura do Exadata. Atualmente, a única opção é o X11M.
   - Em Tipo de servidor de armazenamento, escolha o tipo de modelo de servidor de armazenamento da sua infraestrutura do Exadata. Atualmente, a única opção é o X11M-HC.
7. Para servidores de banco de dados, deixe o padrão de 2 ou mova o controle deslizante para escolher até 32 servidores. Para especificar mais de 2, solicite um aumento de limite da OCI.

   Cada servidor de banco de dados Exadata X9M suporta 126. OCPUs Cada servidor de banco de dados Exadata X11M suporta 760. ECPUs A contagem total de computação muda à medida que você altera o número de servidores. Para obter mais informações sobre OCPUs e ECPUs, consulte Modelos de computação no banco de dados autônomo na documentação da Oracle.
8. Para servidores de armazenamento, deixe o padrão de 3 ou mova o controle deslizante para escolher até 64 servidores. Para especificar mais de 3, solicite um aumento de limite da OCI. Cada servidor de armazenamento X9M fornece 64 TB. Cada servidor de armazenamento X11m

fornece 80 TB. O total de TB de armazenamento muda à medida que você altera o número de servidores. Escolha Próximo.

9. Para a janela Manutenção, configure quando a manutenção do sistema pode ocorrer:

   a. Para Preferência de agendamento, selecione uma das seguintes opções:

      - Cronograma gerenciado pela Oracle - a Oracle determina o horário ideal para as atividades de manutenção.
      - Cronograma gerenciado pelo cliente - você especifica quando as atividades de manutenção podem ocorrer.

   b. Para o modo Patching, selecione uma das seguintes opções:

      - Continuação - As atualizações são aplicadas a um nó por vez, permitindo que o banco de dados permaneça disponível durante a aplicação de patches.
      - Não contínua - as atualizações são aplicadas a todos os nós simultaneamente, o que pode exigir tempo de inatividade.

   c. Se você selecionou Agenda gerenciada pelo cliente, defina as seguintes configurações adicionais:

      - Em Meses de manutenção, selecione os meses em que a manutenção pode ser realizada.
      - Em Semana do mês, selecione qual semana do mês a manutenção pode ser realizada (Primeira, Segunda, Terceira, Quarta ou Última).
      - Em Dia da semana, selecione o dia em que a manutenção pode ser realizada (de segunda a domingo).
      - Em Hora de início, selecione a hora em que a janela de manutenção começa. A hora está em UTC.
      - Em Prazo de entrega da notificação, selecione com quantos dias de antecedência você deseja ser notificado sobre a manutenção futura.

   > **Note**
   >
   > O Oracle Cloud Infrastructure realiza a manutenção do sistema durante essa janela. Durante a manutenção, sua infraestrutura do Exadata permanece disponível, mas você pode passar por breves períodos de maior latência.

10. (Opcional) Para contatos de notificação de manutenção da OCI, insira até 10 endereços de e-mail. AWS encaminha esses endereços de e-mail para a OCI. Quando ocorrem atualizações, a OCI envia notificações para os endereços listados.
11. (Opcional) Em Tags, insira até 50 tags para a infraestrutura. Uma tag é um par de valores-chave que você pode usar para organizar e monitorar seus recursos.
12. Escolha Avançar e revise suas configurações de infraestrutura.
13. Escolha Criar infraestrutura do Exadata.

Etapa 3: criar um cluster de VM Exadata ou um cluster de VM autônoma no Oracle Database@AWS

Um cluster de VM do Exadata é um conjunto VMs no qual você pode criar bancos de dados Oracle Exadata. Você cria os clusters de VM na infraestrutura do Exadata. Você pode implantar vários clusters de VM com diferentes infraestruturas Oracle Exadata na mesma rede ODB. Você tem controle administrativo total sobre os bancos de dados que você cria nos clusters de VM do Exadata.

Um cluster de VM autônomo é um pool pré-alocado de recursos de computação e armazenamento do Oracle Exadata, virtualizados no nível da VM, que executa bancos de dados autônomos (ADB). Ao contrário dos bancos de dados gerenciados pelo usuário que você cria em um cluster de VM do Exadata, um banco de dados autônomo é autoajustável, autocorrigido e gerenciado pela Oracle, e não por um administrador de banco de dados.

Considere as seguintes limitações ao criar clusters de VM:

- Você pode implantar um cluster de VM somente na AZ onde criou sua rede ODB e a infraestrutura do Oracle Exadata.
- Se você não compartilha um cluster de VM entre contas, ele deve estar na Conta da AWS mesma infraestrutura do Oracle Exadata. Se você costuma AWS RAM compartilhar uma rede ODB e uma infraestrutura Oracle Exadata de uma AWS conta com uma conta confiável, a conta confiável pode criar clusters de VM em sua própria conta.
- Você pode implantar somente clusters de VM na sua rede ODB. Nenhum outro recurso é permitido.
- Você não pode alterar a alocação de armazenamento depois de criar um cluster de VM.

> **Important**
>
> O processo de criação pode levar mais de 6 horas, dependendo do tamanho do cluster da VM.

Exadata VM cluster

Para criar um cluster de VM do Exadata

1. Faça login no Console de gerenciamento da AWS e abra o Oracle Database@AWS console em https://console.aws.amazon.com/odb/.
2. No painel esquerdo, escolha Clusters de VM do Exadata.
3. Escolha Criar cluster de VM.
4. Em Nome do cluster da VM, insira um nome. O nome deve ter de 1 a 255 caracteres e começar com um caractere alfabético ou sublinhado. Ele não pode conter hífens consecutivos.
5. (Opcional) Para o nome do cluster de infraestrutura de grade, insira uma versão da infraestrutura de grade para seu cluster de VM que corresponda à versão do banco de dados Oracle que você está usando. O nome deve ter de 1 a 11 caracteres e não pode conter hífens.
6. Em Fuso horário, insira um fuso horário.
7. Para opções de licença, escolha Traga sua própria licença (BYOL) ou Licença incluída e, em seguida, escolha Avançar. Essa licença é a licença OCI fornecida pela Oracle, não uma licença fornecida pela AWS.
8. Defina as configurações de infraestrutura do Exadata da seguinte forma:

   a. Para Infraestrutura, escolha o seguinte:

      - Para o nome da infraestrutura do Exadata, escolha a infraestrutura a ser usada para esse cluster de VM.
      - Para a versão Grid Infrastructure, escolha a versão a ser usada para esse cluster de VM.
      - Para a versão de imagem do Exadata, escolha a versão a ser usada para esse cluster de VM. Recomendamos que você escolha a versão exibida, que é a versão mais alta disponível.

b. Para servidores de banco de dados, selecione um ou mais servidores de banco de dados para hospedar seu cluster de VM.

c. Para Configuração, faça o seguinte:

- Escolha a contagem de núcleos da CPU, a memória e o armazenamento local para cada VM ou aceite os padrões.
- Escolha a quantidade total de armazenamento do Exadata para o cluster da VM ou aceite o padrão.

d. (Opcional) Para alocação de armazenamento, selecione qualquer uma das seguintes opções:

- Habilite a alocação de armazenamento para instantâneos esparsos do Exadata
- Habilite a alocação de armazenamento para backups locais

A alocação de armazenamento utilizável muda conforme você seleciona as opções. Você não pode alterar essa alocação de armazenamento posteriormente. Revise sua seleção e escolha Avançar.

9. Configure a conectividade da seguinte forma:

a. Para rede ODB, escolha uma rede ODB existente.

b. Em Prefixo do nome do host, insira um prefixo para o cluster da VM. Certifique-se de não incluir o nome do domínio. O prefixo forma a primeira parte do nome do host do cluster Oracle Exadata VM.

> **Note**
>
> O nome do domínio Host é fixado como oraclevcn.com.

c. Para porta de ouvinte SCAN (TCP/IP), insira um número de porta para acesso TCP ao ouvinte com nome de acesso de cliente único (SCAN). A porta padrão é 1521. Ou você pode inserir uma porta SCAN personalizada no intervalo de 1024 a 8999, excluindo os seguintes números de porta: 2484, 6100, 6200, 7060, 7070, 7085 e 7879. Escolha Próximo.

d. Para pares de chaves SSH, insira a parte da chave pública de um ou mais pares de chaves usados para acesso SSH ao cluster da VM. Escolha Próximo.

10. (Opcional) Escolha diagnósticos e tags da seguinte forma:

a. Escolha se deseja ativar a coleta de diagnósticos para eventos de diagnóstico, Health monitor e registros de incidentes e coleções de rastreamento. A Oracle pode usar essas informações de diagnóstico para identificar, rastrear e resolver problemas.

b. Em Tags, insira até 50 tags para o cluster da VM. Uma tag é um par de valores-chave que você pode usar para organizar e monitorar seus recursos. Escolha Próximo.

11. Examine suas configurações. Em seguida, escolha Criar cluster de VM.

Autonomous VM cluster

Para criar um cluster de VM autônomo

1. Faça login no Console de gerenciamento da AWS e abra o Oracle Database@AWS console em https://console.aws.amazon.com/odb/.
2. No painel esquerdo, escolha Clusters de VM autônomos.
3. Escolha Criar cluster de VM autônomo.
4. Em Nome do cluster da VM, insira um nome. O nome deve ter de 1 a 255 caracteres e começar com um caractere alfabético ou sublinhado. Ele não pode conter hífens consecutivos.
5. Em Fuso horário, insira um fuso horário.
6. Para opções de licença, escolha Traga sua própria licença (BYOL) ou Licença incluída e, em seguida, escolha Avançar. Essa licença é a licença OCI fornecida pela Oracle, não uma licença fornecida pela AWS.
7. Defina as configurações de infraestrutura do Exadata da seguinte forma:

   a. Para o nome da infraestrutura do Exadata, escolha a infraestrutura a ser usada para esse cluster de VM autônoma.

   b. Para servidores de banco de dados, selecione um ou mais servidores de banco de dados para hospedar seu cluster de VM autônoma.

   c. Para Configuração, faça o seguinte:

      - Escolha a contagem de núcleos da ECPU por VM, a memória do banco de dados por CPU, o armazenamento do banco de dados e o número máximo de bancos de dados de contêineres autônomos ou aceite os padrões.
      - Escolha a quantidade total de armazenamento do Exadata para o cluster de VM autônoma ou aceite o padrão.

8. Configure a conectividade da seguinte forma:

    a. Para rede ODB, escolha uma rede ODB existente.

    b. Em Porta do ouvinte SCAN (TCP/IP), insira um número de porta para Porta (não TLS). A porta padrão é 1521. Ou você pode inserir uma porta (TLS) no intervalo de 1024 a 8999, excluindo os seguintes números de porta: 2484, 6100, 6200, 7060, 7070, 7085 e 7879. Escolha Próximo.

    Selecione Habilitar autenticação TLS mútua (mTLS) para permitir a autenticação TLS mútua.

9. (Opcional) Escolha diagnósticos e tags da seguinte forma:

    a. Escolha se deseja programar a configuração de modificação para o cronograma gerenciado pela Oracle ou para o cronograma gerenciado pelo Cliente. Se você escolher o cronograma gerenciado pelo cliente, defina os meses de manutenção, as semanas do mês, o dia da semana e a hora de início (UTC).

    b. Em Tags, insira até 50 tags para o cluster de VM autônoma. Uma tag é um par de valores-chave que você pode usar para organizar e monitorar seus recursos. Escolha Próximo.

10. Examine suas configurações. Em seguida, escolha Criar cluster de VM autônomo.

Etapa 4: Crie bancos de dados Oracle Exadata no Oracle Cloud Infrastructure

Em Oracle Database@AWS, você pode criar e gerenciar os seguintes recursos usando o AWS console, a CLI ou: APIs

- Redes ODB
- Infraestrutura Oracle Exadata
- Clusters de VM Exadata e clusters de VMs autônomas
- Conexões de emparelhamento ODB

Para criar e gerenciar bancos de dados Oracle Exadata na infraestrutura que você criou, você deve usar o console do Oracle Cloud Infrastructure em vez do Oracle Database@AWS painel. Você pode criar um banco de dados Exadata gerenciado pelo usuário em um cluster de VM Exadata e um

banco de dados autônomo em um cluster de VM Exadata autônomo. Para obter informações sobre a criação de bancos de dados Oracle no OCI, consulte Exadata Database na documentação do Oracle Cloud Infrastructure.

Para criar bancos de dados Oracle Exadata

1. Faça login no Console de gerenciamento da AWS e abra o Oracle Database@AWS console em https://console.aws.amazon.com/odb/.
2. No painel esquerdo, escolha clusters de VM do Exadata ou clusters de VM autônomos.
3. Escolha um cluster de VM para ver a página de detalhes.
4. Escolha Gerenciar no OCI para ser redirecionado para o console do Oracle Cloud Infrastructure.
5. Crie seu banco de dados Exadata gerenciado pelo usuário ou banco de dados autônomo no OCI.

Configurando o emparelhamento de ODB para uma Amazon VPC no Oracle Database@AWS

O emparelhamento ODB é uma conexão de rede criada pelo usuário que permite que o tráfego seja roteado de forma privada entre uma Amazon VPC e uma rede ODB. Há uma one-to-one relação entre uma VPC e uma rede ODB. Depois de criar uma conexão de emparelhamento usando o console, a CLI ou a API, certifique-se de atualizar suas tabelas de rotas de VPC e configurar a resolução de DNS. Para obter uma visão geral conceitual do emparelhamento de ODB, consulte. Emparelhamento ODB

Criando uma conexão de emparelhamento ODB no Oracle Database@AWS

Com conexões de emparelhamento ODB, você pode estabelecer conectividade de rede privada entre sua infraestrutura Oracle Exadata e os aplicativos executados em sua Amazon. VPCs Cada conexão de emparelhamento ODB é um recurso separado que você pode criar, visualizar e excluir independentemente da rede ODB.

Ao criar uma conexão de emparelhamento ODB, você pode especificar intervalos de CIDR de rede de mesmo nível. Essa técnica limita o acesso à rede às sub-redes necessárias, reduz os alvos potenciais de ataques e permite uma segmentação de rede mais granular para os requisitos de conformidade.

Você pode criar os seguintes tipos de conexões de emparelhamento ODB:

Emparelhamento de ODB na mesma conta

- Você pode criar uma conexão de emparelhamento ODB entre uma rede ODB e uma Amazon VPC na mesma conta. AWS

Emparelhamento ODB entre contas

- Você pode criar uma conexão de emparelhamento ODB entre uma rede ODB em uma conta e uma Amazon VPC em uma conta diferente, após a rede ODB ter sido compartilhada usando. AWS RAM As contas de proprietários de VPC podem gerenciar intervalos CIDR especificados na conexão de peering sem também serem proprietárias da rede ODB.

Há uma relação 1:1 entre uma VPC e uma rede ODB. Você não pode criar uma conexão de emparelhamento ODB entre uma VPC e várias redes ODB ou entre uma rede ODB e várias. VPCs

Console

1. Faça login no Console de gerenciamento da AWS e abra o Oracle Database@AWS console em https://console.aws.amazon.com/odb/.
2. No painel de navegação, escolha Conexões de emparelhamento ODB.
3. Escolha Criar conexão de emparelhamento ODB.
4. (Opcional) Para nome de emparelhamento ODB, insira um nome exclusivo para sua conexão.
5. Para rede ODB, escolha a rede ODB a ser emparelhada.
6. Para rede ponto a ponto, escolha a Amazon VPC para fazer peer com sua rede ODB.
7. (Opcional) Para rede ponto a ponto CIDRs, especifique blocos CIDR adicionais da VPC de mesmo nível que possam acessar a rede ODB. Se você não especificar CIDRs, todos CIDRs da VPC de mesmo nível terão acesso permitido.
8. (Opcional) Em Tags, adicione um par de chave e valor.
9. Escolha Criar conexão de emparelhamento ODB.

Depois de criar uma conexão de emparelhamento ODB, configure suas tabelas de rotas da Amazon VPC para rotear o tráfego para a rede ODB emparelhada. Para obter mais informações, consulte Configurando tabelas de rotas VPC para emparelhamento de ODB. Observe que o Oracle Database@ configura AWS automaticamente as tabelas de rotas de rede ODB.

AWS CLI

Para criar uma conexão de emparelhamento ODB, use o `create-odb-peering-connection` comando.

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

Para limitar o acesso à rede ODB a intervalos CIDR específicos, use o `--peer-network-cidrs-to-be-added` parâmetro. Se você não especificar intervalos de CIDR, todos os intervalos terão acesso.

```
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"
```

Para listar suas conexões de emparelhamento ODB, use o `list-odb-peering-connections` comando.

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

Para obter detalhes sobre uma conexão de emparelhamento ODB específica, use o `get-odb-peering-connection` comando.

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

Atualizando uma conexão de emparelhamento ODB

Você pode atualizar uma conexão de emparelhamento ODB existente para adicionar ou remover uma rede de mesmo nível. CIDRs Você controla quais sub-redes na VPC de mesmo nível têm acesso à sua rede ODB.

Console

1. Faça login no Console de gerenciamento da AWS e abra o Oracle Database@AWS console em https://console.aws.amazon.com/odb/.
2. No painel de navegação, escolha Conexões de emparelhamento ODB.
3. Selecione a conexão de emparelhamento ODB que você deseja atualizar.
4. Escolha Ações e, em seguida, escolha Atualizar conexão de peering.
5. Na CIDRs seção Rede de mesmo nível, adicione ou remova blocos CIDR conforme necessário:
   - Para adicionar CIDRs, escolha Adicionar CIDR e insira o bloco CIDR.
   - Para remover CIDRs, escolha o X ao lado do bloco CIDR que você deseja remover.
6. Escolha Atualizar conexão de peering.

AWS CLI

Para adicionar uma rede de pares CIDRs a uma conexão de emparelhamento ODB, especifique o parâmetro `--peer-network-cidrs-to-be-added` no comando. `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"
```

Para remover a rede ponto a ponto CIDRs de uma conexão de emparelhamento ODB, especifique o parâmetro `--peer-network-cidrs-to-be-removed` no comando. `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"
```

Configurando tabelas de rotas VPC para emparelhamento de ODB

Uma tabela de rotas contém um conjunto de regras, chamado de rotas, que determinam para onde o tráfego de rede de sua sub-rede ou gateway é direcionado. O CIDR de destino em uma tabela de rotas é um intervalo de endereços IP para onde você deseja que o tráfego vá. Se você especificou uma VPC para emparelhamento ODB para sua rede ODB, atualize sua tabela de rotas VPC com o intervalo de IP de destino em sua rede ODB. Para obter mais informações sobre emparelhamento de ODB, consulte. Emparelhamento ODB

Para atualizar uma tabela de rotas, use o AWS CLI `ec2 create-route` comando. Os exemplos a seguir atualizam as tabelas de rotas da Amazon VPC. Para obter mais informações, consulte Configurando tabelas de rotas VPC para emparelhamento de 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
```

As tabelas de rotas de rede ODB são atualizadas automaticamente com a VPC CIDRs. Para permitir o acesso à rede ODB somente para uma sub-rede específica e CIDRs não para toda CIDRs a VPC,

você pode especificar a rede de mesmo nível CIDRs ao criar uma conexão de emparelhamento de ODB ou atualizar uma conexão de emparelhamento de ODB existente para adicionar ou remover intervalos de CIDR emparelhados. Para obter mais informações, consulte Criando uma conexão de emparelhamento ODB no Oracle Database@AWS e Atualizando uma conexão de emparelhamento ODB.

Para obter mais informações sobre tabelas de rotas de VPC, consulte Tabelas de rotas de sub-rede no Guia do usuário da Amazon Virtual Private Cloud e ec2 create-route na Referência de comandos.AWS CLI

Configurando o DNS para Oracle Database@AWS

O Amazon Route 53 é um serviço web de Sistema de Nomes de Domínio (DNS) altamente disponível e escalável que você pode usar para roteamento de DNS. Ao criar uma conexão de emparelhamento ODB entre sua rede ODB e uma VPC, você precisa de um mecanismo para resolver consultas de DNS para recursos de rede ODB de dentro da VPC. Você pode usar o Amazon Route 53 para configurar os seguintes recursos:

- Um endpoint de saída

  O endpoint é necessário para enviar consultas de DNS para a rede ODB.
- Uma regra de resolução

  Essa regra especifica o nome de domínio das consultas DNS que o Resolvedor do Route 53 encaminha para o DNS da rede ODB.

Como o DNS funciona em Oracle Database@AWS

Oracle Database@AWS gerencia automaticamente a configuração do Sistema de Nomes de Domínio (DNS) para a rede ODB. Para o nome de domínio, você pode especificar um prefixo personalizado para o nome de domínio padrão `oraclevcn.com` ou um nome de domínio totalmente personalizado. Para obter mais informações, consulte Etapa 1: Criar uma rede ODB no Oracle Database@AWS.

Ao Oracle Database@AWS provisionar uma rede ODB, ela cria os seguintes recursos:

- Uma rede de nuvem virtual (VCN) da Oracle Cloud Infrastructure (OCI) com os mesmos blocos CIDR da rede ODB

Essa VCN reside na locação OCI vinculada do cliente. Há um mapeamento 1:1 entre uma rede ODB e uma OCI VCN. Cada rede ODB está associada a um OCI VCN.

- Um resolvedor de DNS privado dentro do OCI VCN

  Esse resolvedor de DNS lida com consultas de DNS dentro do OCI VCN. A automação OCI cria registros para o cluster de VM. As digitalizações usam o nome de domínio `*.oraclevcn.com` totalmente qualificado (FQDN).
- Um endpoint de escuta de DNS dentro do OCI VCN para o resolvedor de DNS privado

  Você pode encontrar o endpoint de escuta do DNS na página de detalhes da rede ODB no console. Oracle Database@AWS

Configurando um endpoint de saída em uma rede ODB no Oracle Database@AWS

Um endpoint de saída permite que as consultas de DNS sejam enviadas da sua VPC para uma rede ou endereço IP. O endpoint especifica os endereços IP dos quais as consultas são originadas. Para encaminhar consultas de DNS da sua VPC para sua rede ODB, crie um endpoint de saída usando o console do Route 53. Para obter mais informações, consulte Encaminhando consultas DNS de saída para sua rede.

Para configurar um endpoint de saída em uma rede ODB

1. Faça login no Console de gerenciamento da AWS e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel esquerdo, escolha Pontos de extremidade de saída.
3. Na barra de navegação, escolha a região da VPC em que você deseja criar o endpoint de saída.
4. Escolha Create outbound endpoint (Criar endpoint de saída).
5. Preencha a seção Configurações gerais para endpoint de saída da seguinte forma:

   a. Escolha um grupo de segurança que permita conectividade TCP e UDP de saída com o seguinte:

      - Endereços IP que os resolvedores usam para consultas de DNS na sua rede ODB
      - Portas que os resolvedores usam para consultas de DNS na sua rede ODB

   b. Em Endpoint Type (Tipo de endpoint), selecione IPv4.

c. Em Protocolos para esse endpoint, escolha Do53.

6. Em endereços IP, forneça as seguintes informações:

   - Especifique endereços IP ou deixe o Route 53 Resolver escolher endereços IP para você a partir dos endereços disponíveis na sub-rede. Escolha um mínimo de 2 até um máximo de 6 endereços IP para consultas de DNS. Recomendamos que você escolha endereços IP em pelo menos duas zonas de disponibilidade diferentes.
   - Para Sub-rede, escolha sub-redes que tenham o seguinte:
     - Tabelas de rotas que incluem rotas para os endereços IP do ouvinte DNS na rede ODB
     - Listas de controle de acesso à rede (ACLs) que permitem tráfego UDP e TCP para os endereços IP e as portas que os resolvedores usam para consultas de DNS na rede ODB
     - Rede ACLs que permite tráfego de resolvedores no intervalo de portas de destino 1024-65535

7. (Opcional) Para Tags, especifique tags para o endpoint.
8. Selecione Enviar.

Configurando uma regra de resolução em Oracle Database@AWS

Uma regra de resolução é um conjunto de critérios que determina como rotear consultas de DNS. Reutilize ou crie uma regra que especifique o nome de domínio das consultas DNS que o resolvedor encaminha para o DNS da rede ODB.

Usando uma regra de resolução existente

Para usar uma regra de resolução existente, sua ação depende do tipo de regra:

Uma regra para o mesmo domínio na mesma AWS região que a VPC em seu Conta da AWS

Associe a regra à sua VPC em vez de criar uma nova regra. Escolha a regra no painel de controle de regras e associe-a à aplicável VPCs na AWS região.

Uma regra para o mesmo domínio na mesma região da sua VPC, mas em uma conta diferente

Use AWS Resource Access Manager para compartilhar a regra da conta remota com sua conta. Ao compartilhar uma regra, você também compartilha o endpoint de saída correspondente. Depois de compartilhar a regra com sua conta, escolha a regra no painel de regras e associe-a à VPCs da sua conta. Para obter mais informações, consulte Gerenciando regras de encaminhamento.

Criando uma nova regra de resolução

Se você não puder reutilizar uma regra de resolução existente, crie uma nova regra usando o console do Amazon Route 53.

Para criar uma nova regra de resolução

1. Faça login no Console de gerenciamento da AWS e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel esquerdo, escolha Regras.
3. Na barra de navegação, escolha a região da VPC em que o endpoint de saída existe.
4. Escolha Criar regra.
5. Complete a regra para seções de tráfego de saída da seguinte forma:
   a. Em Tipo de regra, escolha Regra de encaminhamento.
   b. Em Nome do domínio, especifique o nome completo do domínio da rede ODB.
   c. Para VPCs isso, use essa regra, associe-a à VPC de onde as consultas DNS são encaminhadas para sua rede ODB.
   d. Para Endpoint de saída, escolha o endpoint de saída que você criou em. Configurando um endpoint de saída em uma rede ODB no Oracle Database@AWS

   > **Note**
   >
   > A VPC associada a essa regra não precisa ser a mesma VPC em que você criou o endpoint de saída.

6. Preencha a seção Endereços IP de destino da seguinte forma:
   a. Para endereço IP, especifique o endereço IP do ouvinte DNS na sua rede ODB.
   b. Em Porta, especifique 53. Essa é a porta que o resolvedor usa para consultas de DNS.

   > **Note**
   >
   > O Route 53 Resolver encaminha consultas de DNS que correspondem a essa regra e se originam de uma VPC associada a essa regra para o endpoint de saída referenciado. Essas consultas são encaminhadas para os endereços IP de destino que você especifica nos endereços IP de destino.

c. Para Protocolo de transmissão, escolha Do53.

7. (Opcional) Para Tags, especifique tags para a regra.
8. Selecione Enviar.

Testando sua configuração de DNS em Oracle Database@AWS

Depois de criar o endpoint de saída e a regra do resolvedor, teste para garantir que o DNS seja resolvido corretamente. Usando uma EC2 instância da Amazon em seu aplicativo VPC, execute uma resolução de DNS da seguinte forma:

Para Linux ou macOS

Use um comando do formulário`dig` *`record-name record-type`*.

No Windows

Use um comando do formulário`nslookup -type=`*`record-name record-type`*.

Configurando os Amazon VPC Transit Gateways para Oracle Database@AWS

O Amazon VPC Transit Gateways é um hub de trânsito de rede que interconecta nuvens privadas virtuais (VPCs) e redes locais. Cada VPC na hub-and-spoke arquitetura pode se conectar ao gateway de trânsito para obter acesso a outras conectadas. VPCs AWS Transit Gateway suporta tráfego para ambos IPv4 IPv6 e.

Em Oracle Database@AWS, uma rede ODB oferece suporte a uma conexão emparelhada com apenas uma VPC. Se você conectar um gateway de trânsito a uma VPC emparelhada a uma rede ODB, poderá conectar vários VPCs a esse gateway. Aplicativos executados nesses diferentes tipos VPCs podem acessar um cluster de VM do Exadata em execução na sua rede ODB.

O diagrama a seguir mostra um gateway de trânsito conectado a duas redes locais VPCs e uma.

No diagrama anterior, uma VPC é emparelhada para uma rede ODB. Nessa configuração, a rede ODB pode rotear o tráfego para todos os VPCs conectados ao gateway de trânsito. A tabela de rotas de cada VPC inclui a rota local e as rotas que enviam tráfego destinado à rede ODB para o gateway de trânsito.

Em AWS Transit Gateway, você é cobrado pelo número de conexões que você faz com o gateway de trânsito por hora e pela quantidade de tráfego que flui AWS Transit Gateway. Para obter informações sobre custos, consulte AWS Transit Gateway preços.

Requisitos

Certifique-se de que seu Oracle Database@AWS ambiente atenda aos seguintes requisitos:

- A VPC que está emparelhada para sua rede ODB deve estar na mesma. Conta da AWS Se a VPC emparelhada estiver em uma conta diferente da rede ODB, os anexos do gateway de trânsito falharão independentemente das configurações de compartilhamento.
- A VPC que está emparelhada para sua rede ODB deve ter um anexo de gateway de trânsito.

> **Note**
>
> Se o gateway de trânsito estiver configurado para compartilhamento, ele poderá residir em qualquer conta. Assim, o gateway em si não precisa estar na mesma conta da rede VPC e ODB.

- O anexo do gateway de trânsito deve estar na mesma Zona de Disponibilidade (AZ) da rede ODB.

Limitações

Observe as seguintes limitações dos Amazon VPC Transit Gateways para: Oracle Database@AWS

- O Amazon VPC Transit Gateways não oferece integração nativa para usar uma rede ODB como anexo. Portanto, recursos de VPC como os seguintes não estão disponíveis:
  - Resolução de nomes de host DNS públicos para endereços IP privados
  - Notificação de eventos para alterações na topologia da rede ODB, no roteamento e no status da conexão
- O tráfego multicast para a rede ODB não é suportado.

Configurando e configurando um gateway de trânsito

Você cria e configura um gateway de trânsito usando o console ou `aws ec2` os comandos da Amazon VPC. O procedimento a seguir pressupõe que você não tenha uma rede ODB emparelhada

para uma VPC em seu. Conta da AWS Se uma rede ODB e uma VPC já estiverem emparelhadas em sua conta, pule as etapas de 1 a 3.

> **Note**
>
> Se você anexar ou reconectar os anexos em sua VPC, certifique-se de inserir novamente os intervalos de CIDR na rede ODB ODB.

Para instalar e configurar um gateway de trânsito para Oracle Database@AWS

1. Crie uma rede ODB. Para obter mais informações, consulte Etapa 1: Criar uma rede ODB no Oracle Database@AWS.
2. Crie uma VPC usando a mesma conta que contém a rede ODB. Para obter mais informações, consulte Criar uma VPC no Guia do usuário da Amazon VPC.
3. Crie uma conexão de emparelhamento ODB entre sua rede ODB e sua VPC. Para obter mais informações, consulte Configurando o emparelhamento de ODB para uma Amazon VPC no Oracle Database@AWS.
4. Configure um gateway de trânsito seguindo as etapas em Comece a usar os Amazon VPC Transit Gateways. O gateway deve estar na Conta da AWS mesma rede ODB e na VPC ou compartilhado por outra conta.

   > **Important**
   >
   > Crie o anexo do gateway de trânsito na mesma AZ da rede ODB.

5. Adicione intervalos CIDR à sua rede ODB para VPCs as redes locais que você planeja conectar à sua rede principal. Para obter mais informações, consulte Atualizando uma rede ODB no Oracle Database@AWS.

   Se você estiver usando a CLI, execute o comando `update-odb-network` com e. `--peered-cidrs-to-be-added` `--peered-cidrs-to-be-removed` Para obter mais informações, consulte Referência de comandos da AWS CLI.

Configurando o AWS Cloud WAN para Oracle Database@AWS

AWS O Cloud WAN é um serviço gerenciado de rede de área ampla (WAN). Você pode usar o AWS Cloud WAN para criar, gerenciar e monitorar uma rede global unificada que conecta recursos em execução em seus ambientes locais e na nuvem.

Na AWS Cloud WAN, uma rede global é uma rede única e privada que atua como o contêiner de alto nível para seus objetos de rede. Uma rede central é a parte da sua rede global gerenciada pela AWS.

AWS A WAN em nuvem oferece os seguintes benefícios principais:

- Gerenciamento de rede centralizado que simplifica as operações enquanto mantém a segurança em várias regiões
- Redes principais com segmentação integrada para isolar o tráfego por meio de vários domínios de roteamento
- Support para políticas para automatizar o gerenciamento da rede e definir configurações consistentes em toda a sua rede global

No Oracle Database@AWS, uma rede ODB oferece suporte ao peering para somente uma VPC. Se você conectar uma rede principal do AWS Cloud WAN a uma VPC emparelhada, isso permitirá o roteamento global do tráfego. Aplicativos conectados em várias VPCs regiões podem acessar clusters de VM do Exadata em sua rede ODB. Você pode isolar o tráfego de rede ODB em seu próprio segmento ou permitir o acesso a outros segmentos.

O diagrama a seguir mostra uma rede principal do AWS Cloud WAN conectada a três VPCs e uma rede local.

AWS O Cloud WAN não oferece integração nativa para usar uma rede ODB como anexo. Portanto, recursos de VPC como os seguintes não estão disponíveis:

- Resolução de nomes de host DNS públicos para endereços IP privados
- Notificação de eventos para alterações na topologia da rede ODB, no roteamento e no status da conexão

Na AWS Cloud WAN, você é cobrado por hora pelo seguinte:

- Número de regiões (bordas da rede principal)
- Número de conexões de rede principais
- A quantidade de tráfego que flui pela sua rede principal por meio dos anexos

Para obter informações detalhadas sobre preços, consulte Preços AWS da Cloud WAN.

Para configurar uma rede principal para Oracle Database@AWS

1. Adicione intervalos CIDR à sua rede ODB para VPCs as redes locais que você planeja conectar à sua rede principal. Para obter mais informações, consulte Atualizando uma rede ODB no Oracle Database@AWS.

   > **Note**
   >
   > Se você anexar ou reconectar os anexos em sua VPC, certifique-se de inserir novamente os intervalos de CIDR na rede ODB ODB.

2. Siga as etapas em Criar uma rede global e uma rede principal de WAN em AWS nuvem.

Compartilhamento de direitos no Oracle Database@AWS

Com o Oracle Database@AWS, você pode compartilhar direitos do AWS Marketplace para o Oracle Database@AWS na mesma organização. Contas da AWS AWS Isso permite que outras contas provisionem sua própria infraestrutura Oracle Exadata e recursos de rede ODB usando sua assinatura.

Métodos de compartilhamento

O Oracle Database@AWS oferece suporte a dois métodos de compartilhamento:

Compartilhamento de direitos com AWS o License Manager

- Conceda a outras contas a capacidade de provisionar sua própria infraestrutura Oracle Exadata e recursos de rede ODB
- Cada conta opera de forma independente com controle total do ciclo de vida dos recursos
- Ideal para permitir o provisionamento de autoatendimento entre equipes ou unidades de negócios

Compartilhamento de recursos com AWS Resource Access Manager (AWS RAM)

- Compartilhe a infraestrutura Oracle Exadata já provisionada e os recursos de rede ODB
- Centralize o gerenciamento da infraestrutura e, ao mesmo tempo, permita que as contas de destinatários criem clusters de VM
- Otimize os custos fazendo com que várias contas usem a mesma infraestrutura

Você pode usar os dois métodos de compartilhamento simultaneamente com base nas necessidades da sua organização.

Limitações do compartilhamento de direitos do Oracle Database@AWS

Ao compartilhar AWS direitos do Oracle Database@, tenha em mente as seguintes limitações:

- Você só pode compartilhar com Contas da AWS dentro da sua AWS organização

- Você não pode compartilhar com uma unidade organizacional (OU) inteira ou com toda a organização
- Uma conta pode receber direitos de apenas uma conta de comprador (de uma oferta privada)
- Uma conta de comprador não pode compartilhar direitos com outra conta de comprador
- As contas de destinatário devem inicializar o AWS serviço Oracle Database@ antes de poderem usar o direito compartilhado
- As operações de concessão de direitos só podem ser realizadas na região Leste dos EUA (Norte da Virgínia)

Compartilhamento de AWS direitos do Oracle Database@ entre contas

Para permitir a colaboração e, ao mesmo tempo, otimizar os custos, compartilhe os AWS direitos do Oracle Database@ com outras Contas da AWS pessoas da mesma organização. AWS Este tópico explica como compartilhar direitos usando o AWS License Manager.

Pré-requisitos para compartilhar direitos

Antes de compartilhar os AWS direitos do Oracle Database@, verifique se você tem o seguinte:

- Uma AWS assinatura ativa do Oracle Database@ (você deve ser a conta do comprador que aceitou a oferta privada por meio de) AWS Marketplace
- A IDs das AWS contas em sua organização com as quais você deseja compartilhar direitos
- Permissões necessárias para que o concedente e o beneficiário usem os recursos e operações do AWS License Manager (para obter mais informações, consulte Gerenciamento de identidade e acesso do License Manager no Guia do Usuário do License Manager AWS)
- Permissões listadas abaixo para você (concedente) e beneficiário do direito (beneficiário)

Permissões necessárias para compartilhamento de direitos

Além das permissões do AWS License Manager, o Oracle Database@AWS exige as seguintes permissões:

Permissões do concedente

- `odb:CreateGrantShare`

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

Permissões concedidas

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

Compartilhando AWS direitos do Oracle Database@ com outra conta usando o License Manager AWS

Para compartilhar direitos com outra AWS conta, você cria uma concessão usando o AWS License Manager. Para obter mais informações, consulte Distribute os direitos do License Manager no Guia do usuário do AWS License Manager.

Depois de criar a concessão, o destinatário (beneficiário) deve:

- Aceite e ative a concessão. Para obter mais informações, consulte Aceitação e ativação de concessões no License Manager no Guia do Usuário do AWS License Manager.
- Siga as instruções de inicialização do Oracle AWS Database@.

Após a conclusão da inicialização, o beneficiário pode provisionar recursos do Oracle Database@AWS usando o direito compartilhado.

Compartilhamento de recursos no Oracle Database@AWS

Com o Oracle Database@AWS, você pode compartilhar a infraestrutura do Exadata e sua rede ODB entre várias Contas da AWS na mesma organização. AWS Isso permite provisionar a infraestrutura uma vez e reutilizá-la em contas confiáveis, reduzindo custos e separando responsabilidades.

Quando você compartilha recursos:

- A conta proprietária do recurso (conta do proprietário) mantém o controle sobre o ciclo de vida do recurso.
- As contas que recebem acesso a recursos compartilhados (contas confiáveis) podem visualizar e usar esses recursos com base nas permissões concedidas.
- As contas confiáveis podem criar seus próprios recursos na infraestrutura compartilhada, mas não podem excluir os recursos compartilhados subjacentes.

Integração do Oracle Database@AWS com AWS RAM

O Oracle Database@AWS usa AWS Resource Access Manager (AWS RAM) para permitir o compartilhamento seguro e controlado de recursos entre contas. Com AWS RAM, você pode compartilhar com segurança seus AWS recursos do Oracle Database@ em várias AWS contas na mesma organização. AWS AWS RAM simplifica o compartilhamento de recursos, reduz a sobrecarga operacional e fornece segurança e visibilidade aos recursos compartilhados do Oracle AWS Database@.

Com AWS RAM, você compartilha recursos de sua propriedade criando um compartilhamento de recursos. Um compartilhamento de recursos especifica os recursos a serem compartilhados e Contas da AWS com quem compartilhá-los.

Benefícios do compartilhamento de recursos no Oracle Database@AWS

Compartilhar AWS recursos do Oracle Database@ entre contas oferece os seguintes benefícios:

- Otimização de custos — provisione uma infraestrutura cara do Exadata uma vez por meio de uma conta administrativa e compartilhe-a com várias contas, reduzindo os custos gerais.

- Separação de responsabilidades — mantenha limites claros entre os administradores da infraestrutura e os usuários do banco de dados e, ao mesmo tempo, permita a colaboração.
- Gerenciamento simplificado — centralize o provisionamento e o gerenciamento da infraestrutura e, ao mesmo tempo, habilite operações de banco de dados distribuídas.
- Governança consistente — aplique políticas e controles consistentes em todos os recursos compartilhados.

Por exemplo, um administrador pode provisionar a infraestrutura do Oracle Exadata e a rede ODB em suas contas Conta da AWS e compartilhá-las com contas de desenvolvedores. Os desenvolvedores podem então criar clusters de VM nessa infraestrutura compartilhada sem precisar provisionar seu próprio hardware caro. Essa abordagem reduz significativamente os custos, mantendo a separação adequada das responsabilidades entre as contas.

Como o compartilhamento de recursos funciona no Oracle Database@AWS

Você pode compartilhar os seguintes recursos do Oracle Database@:AWS

- Infraestrutura Oracle Exadata
- Rede ODB

O Oracle Database@AWS compartilha os recursos anteriores por meio do seguinte processo:

1. A conta do comprador (a conta que aceita a oferta AWS privada do Oracle Database@ via AWS Marketplace) provisiona AWS recursos do Oracle Database@, como a infraestrutura do Exadata e uma rede ODB.
2. A conta do comprador cria um compartilhamento de recursos usando AWS RAM, especificando os recursos a serem compartilhados e as contas confiáveis com as quais compartilhá-los.
3. Os compartilhamentos de recursos das contas confiáveis dentro da mesma organização são aceitos automaticamente.
4. Antes de usar recursos compartilhados, as contas confiáveis devem inicializar o AWS serviço Oracle Database@ em sua conta usando o `aws odb initialize-service` comando ou escolhendo Ativar conta no console Oracle Database@.AWS
5. Após a inicialização, as contas confiáveis podem criar seus próprios recursos na infraestrutura compartilhada, como clusters de VM na infraestrutura compartilhada do Exadata e na rede ODB.

Permissões em recursos compartilhados para contas confiáveis

Quando você compartilha recursos, o Oracle Database@ seleciona AWS automaticamente ações específicas (permissões gerenciadas) para cada tipo de recurso:

Para a infraestrutura Exadata

O Oracle Database@AWS concede as seguintes permissões às contas confiáveis:

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

Para rede ODB

As seguintes permissões são concedidas a contas confiáveis:

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

O compartilhamento de recursos respeita a natureza hierárquica dos recursos do Oracle Database@.AWS Por exemplo, se você compartilha a infraestrutura do Exadata, contas confiáveis podem criar clusters de VM nessa infraestrutura, mas não podem modificar ou excluir a própria infraestrutura do Exadata.

Quando um recurso não é compartilhado, as contas confiáveis perdem a capacidade de criar novos recursos na infraestrutura compartilhada. No entanto, todos os recursos que eles já criaram permanecem acessíveis e funcionais.

Limitações do compartilhamento de recursos do Oracle Database@AWS

Antes de compartilhar recursos, tenha em mente as seguintes limitações.

Limitações para compartilhar recursos

Ao compartilhar os AWS recursos do Oracle Database@, tenha em mente as seguintes limitações:

- Você só pode compartilhar recursos com Conta da AWS IDs o.
- Você só pode compartilhar recursos Contas da AWS dentro da mesma AWS organização.
- Você compartilha recursos em uma AWS região específica. Para compartilhar recursos entre regiões, você deve criar compartilhamentos de recursos separados em cada região.
- Quando você cria um compartilhamento de recursos, as ações (permissões gerenciadas) para cada tipo de recurso são selecionadas automaticamente e não podem ser modificadas.
- Você não pode usar o Oracle Database@AWS como um recurso e compartilhar com outros. Contas da AWS
- Uma conta confiável pode usar recursos compartilhados de apenas uma conta de comprador (de uma oferta privada). Assim, duas contas de comprador não podem compartilhar recursos com a mesma conta confiável.
- Uma conta de comprador não pode compartilhar recursos com outra conta de comprador.
- Os recursos compartilhados com uma conta confiável devem ser compartilhados primeiro pela conta do comprador na região de origem do comprador.
- Ao cancelar o compartilhamento de um recurso, recomendamos que você espere aproximadamente 15 minutos antes de compartilhar novamente o mesmo recurso com a mesma conta confiável.

Limitações para criar e usar recursos compartilhados

Ao criar ou usar os AWS recursos do Oracle Database@, tenha em mente as seguintes limitações:

- Somente a conta do comprador pode criar a infraestrutura do Exadata e os recursos de rede ODB. A conta do comprador é aquela que aceita a oferta AWS privada do Oracle Database@.
- Contas confiáveis podem criar recursos somente na infraestrutura do Exadata compartilhada pela conta do comprador.

- As contas confiáveis devem inicializar o AWS serviço Oracle Database@ em suas contas antes de poderem usar recursos compartilhados.

Limitações para excluir recursos compartilhados

- Você não pode excluir a infraestrutura do Exadata que tem clusters de VM criados por contas confiáveis até que esses clusters de VM sejam removidos.
- Você não pode excluir uma rede ODB que tenha uma conexão de emparelhamento de ODB criada por uma conta confiável até que a conexão de emparelhamento de ODB seja removida.
- A conta do comprador não pode excluir AWS recursos do Oracle Database@ criados por contas confiáveis.
- Contas confiáveis podem visualizar recursos compartilhados, mas não podem modificar ou excluir AWS recursos do Oracle Database@ de propriedade da conta do comprador.

Compartilhamento de Oracle Database@AWS recursos entre contas

Para permitir a colaboração e, ao mesmo tempo, otimizar os custos, compartilhe os AWS recursos do Oracle Database@ com outras pessoas da Contas da AWS mesma organização. AWS Este tópico explica como compartilhar recursos usando AWS Resource Access Manager (AWS RAM).

Tópicos

Pré-requisitos para compartilhar recursos

Antes de compartilhar os AWS recursos do Oracle Database@, verifique se você tem o seguinte:

- Uma AWS assinatura ativa do Oracle Database@ (você deve ser a conta do comprador que aceitou a oferta privada por meio de) AWS Marketplace

- Os nomes IDs ou dos recursos que você deseja compartilhar, como infraestrutura do Exadata ou redes ODB
- A IDs das AWS contas em sua organização com as quais você deseja compartilhar recursos
- Permissões necessárias para criar compartilhamentos de recursos no AWS RAM
- A capacidade de compartilhar recursos com AWS Organizations o uso AWS RAM (para obter mais informações, consulte Habilitar o compartilhamento de recursos AWS Organizations no Guia AWS Resource Access Manager do usuário)

Compartilhando AWS recursos do Oracle Database@ com outra conta usando AWS RAM

Para compartilhar uma infraestrutura do Exadata ou rede ODB com outra AWS conta, você cria um compartilhamento de recursos usando. AWS RAM Isso permite que a conta confiável crie clusters de VM em sua infraestrutura do Exadata.

Console

1. Abra o AWS RAM console em https://console.aws.amazon.com/ram/.
2. Escolha Criar compartilhamento de recursos.
3. Em Nome, insira um nome descritivo para seu compartilhamento de recursos.
4. Em Selecionar tipo de recurso, um dos seguintes recursos:
   - Rede Oracle Database@ ODB AWS
   - Infraestrutura Oracle Database@ Exadata AWS
5. Selecione os recursos de infraestrutura do Exadata que você deseja compartilhar. Escolha Avançar até conseguir conceder acesso aos diretores.
6. Em Diretores, escolha e Contas da AWS, em seguida, insira a AWS conta com a qual IDs você deseja compartilhar.
7. Em Permissões gerenciadas, selecione as seguintes permissões para permitir que a conta confiável crie clusters de VM na infraestrutura compartilhada do Exadata:
   - AWSRAMDefaultPermissãoODBNetwork
   - AWSRAMDefaultPermissãoODBCloudExadataInfrastructure
8. Escolha Criar compartilhamento de recursos.

AWS CLI

Para compartilhar recursos usando o AWS CLI, use o `aws ram create-resource-share` comando. O exemplo a seguir cria um compartilhamento de recursos chamado `ExadataInfraShare` que compartilha a infraestrutura do Exadata especificada com a conta 222222222222, permitindo que essa conta crie clusters de VM na infraestrutura compartilhada.

```
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
```

Visualizando seus compartilhamentos de recursos

Para ver os recursos que você compartilhou e as contas com as quais você os compartilhou:

Console

1. Abra o AWS RAM console em https://console.aws.amazon.com/ram/.
2. Escolha Recursos compartilhados para ver os recursos que você compartilhou com outras contas.
3. Selecione um compartilhamento de recursos para ver seus detalhes, incluindo os recursos compartilhados e os principais com os quais eles são compartilhados.

AWS CLI

Para visualizar seus compartilhamentos de recursos usando o AWS CLI, use o `get-resource-shares` comando:

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

Para visualizar os recursos em um compartilhamento de recursos específico, use o `list-resources` comando:

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

Para ver os principais (contas) com os quais um compartilhamento de recursos é compartilhado, use o `list-principals` comando:

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

Atualizando ou excluindo compartilhamentos de recursos usando AWS RAM

Para parar de compartilhar um recurso com uma conta confiável usando AWS RAM, execute qualquer uma das seguintes ações:

- Remova o recurso do compartilhamento de recursos.
- Remova a conta confiável do compartilhamento de recursos.
- Exclua o compartilhamento de recursos.

Antes de revogar o acesso ou excluir um recurso compartilhado, considere as seguintes implicações:

- Contas confiáveis não podem mais criar novos recursos na infraestrutura não compartilhada.
- Os recursos existentes criados por contas confiáveis na infraestrutura compartilhada do Exadata continuam funcionando e permanecem acessíveis a elas. Contas da AWS
- Você não pode excluir a infraestrutura do Exadata que tem clusters de VM criados por contas confiáveis até que esses clusters de VM sejam removidos.

Antes de deixar de compartilhar recursos, recomendamos que você se coordene com as contas confiáveis para garantir uma transição tranquila.

Para obter mais informações, consulte Atualizar um compartilhamento de recursos AWS RAM e Excluir um compartilhamento de recursos AWS RAM no Guia do AWS Resource Access Manager usuário.

Inicializando Oracle Database@AWS em uma conta confiável

Uma conta confiável é Conta da AWS aquela que você designa como qualificada para receber compartilhamentos de recursos. Deve ser outra pessoa Conta da AWS em sua AWS organização.

Antes de usar AWS recursos compartilhados do Oracle Database@ em uma conta confiável, você deve inicializar o serviço. A inicialização cria os metadados necessários e estabelece a conexão entre você Conta da AWS e o Oracle Cloud Infrastructure.

Tópicos

O que é a inicialização do Oracle Database@AWS ?

Depois que um recurso for compartilhado com sua conta, você deverá inicializar o AWS serviço Oracle Database@ antes de poder acessar ou usar o recurso compartilhado. Se você tentar usar o Oracle Database@AWS APIs sem inicializar o serviço primeiro, receberá um erro.

A inicialização é um processo único. Ele cria os metadados necessários e estabelece uma conexão entre você Conta da AWS e o Oracle Cloud Infrastructure.

Você pode inicializar o serviço usando o AWS Management Console ou o. AWS CLI

Console

1. Abra o AWS console do Oracle Database@ em. https://console.aws.amazon.com/odb/
2. Se esta for a primeira vez que você acessa o AWS console Oracle Database@ nessa conta, você verá uma página de boas-vindas.
3. Escolha Ativar conta.
4. O processo de inicialização do serviço começa. Esse processo pode levar alguns minutos para ser concluído.
5. Atualize a página de boas-vindas periodicamente até que o botão Ativar conta mude para o botão Painel.
6. Escolha Dashboard para começar a usar o Oracle Database@AWS.

AWS CLI

Para inicializar o Oracle Database@AWS em sua conta confiável usando o AWS CLI, use o comando. `initialize-service`

```
aws odb initialize-service
```

Para verificar o status de inicialização, use o `get-oci-onboarding-status` comando.

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

Quando a inicialização estiver concluída, a saída mostrará um status de`ACTIVE_LIMITED`, indicando que sua conta pode acessar recursos compartilhados, mas não pode criar uma nova infraestrutura do Exadata ou rede ODB.

Próximas etapas

Depois de inicializar o Oracle Database@AWS em sua conta confiável, você pode fazer o seguinte:

- Visualize recursos compartilhados usando os `get` comandos `list` e ou no AWS console.
- Crie clusters de VM e clusters de VM autônomos em uma infraestrutura compartilhada do Exadata e rede ODB.
- Crie uma conexão de emparelhamento ODB em uma rede ODB compartilhada.

Para obter mais informações sobre como trabalhar com recursos compartilhados, consulteTrabalhando com Oracle Database@AWS recursos compartilhados em uma conta confiável.

Trabalhando com Oracle Database@AWS recursos compartilhados em uma conta confiável

Depois que um recurso for compartilhado com sua conta confiável e você tiver inicializado o AWS serviço Oracle Database@, você poderá visualizar e usar o recurso compartilhado. Este tópico explica como trabalhar com recursos compartilhados em uma conta confiável.

Tópicos

Limitações para recursos compartilhados em uma conta confiável

Ao trabalhar com AWS recursos compartilhados do Oracle Database@, esteja ciente das seguintes limitações:

- O compartilhamento de recursos é suportado somente dentro da mesma AWS organização.
- Somente a conta do comprador (a conta que aceita a oferta AWS privada do Oracle Database@) pode criar a infraestrutura do Exadata e os recursos de rede ODB.
- Você pode criar recursos somente na infraestrutura compartilhada e somente se tiver as permissões necessárias.
- As ações específicas (permissões gerenciadas) para cada tipo de recurso são selecionadas automaticamente durante a criação do compartilhamento de recursos e não podem ser modificadas.
- Você não pode modificar ou excluir recursos pertencentes a outra conta.
- Os recursos que você cria na infraestrutura compartilhada pertencem à sua conta e contam para suas cotas de OCI. O mesmo se aplica aos recursos dos pais.
- Se a conta do proprietário não compartilhar um recurso, você não poderá mais criar novos recursos nessa infraestrutura compartilhada. No entanto, seus recursos existentes continuam funcionando.
- O compartilhamento de recursos entre regiões não é suportado. Você só pode compartilhar recursos dentro da mesma AWS região.
- Os recursos da conta confiável são cobrados do comprador da assinatura Oracle Database@AWS .
- Ao usar um recurso compartilhado, você deve fornecer o Amazon Resource Name (ARN).

Criação de clusters de VM na infraestrutura compartilhada do Exadata

Se sua conta confiável tiver acesso a uma infraestrutura compartilhada do Exadata e a uma rede ODB, você poderá criar clusters de VM do Exadata, clusters de VM autônomos ou pares de ODB nessa infraestrutura.

> **Note**
>
> Ao usar um recurso compartilhado com você, em vez de especificar apenas o ID do recurso, você deve especificar o Amazon Resource Name (ARN).

Console

1. Abra o AWS console do Oracle Database@ em. https://console.aws.amazon.com/odb/
2. No painel de navegação, escolha Clusters de VM do Exadata ou clusters de VM autônomos.
3. Escolha Criar cluster de VM ou Criar cluster de VM autônomo.
4. Para a infraestrutura do Exadata, selecione a infraestrutura compartilhada do Exadata na qual você deseja criar o cluster da VM.
5. Preencha os campos restantes conforme necessário para a configuração do seu cluster de VM.
6. Escolha Criar cluster de VM ou Criar cluster de VM autônomo.

AWS CLI

Para criar um cluster de VM na infraestrutura compartilhada do Exadata usando o AWS CLI, use o comando: `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..." \
```

Para criar um cluster de VM autônoma na infraestrutura compartilhada do Exadata usando o AWS CLI, use o comando: `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
```

O cluster de VM é criado na infraestrutura compartilhada especificada do Exadata e pertence à sua conta confiável.

Visualizando recursos compartilhados em uma conta confiável

Você pode visualizar os recursos que foram compartilhados com sua conta usando o AWS Management Console ou AWS CLI o.

Console

1. Abra o AWS console do Oracle Database@ em. https://console.aws.amazon.com/odb/
2. No painel de navegação, escolha o tipo de recurso que você deseja visualizar: infraestrutura do Exadata ou rede ODB.
3. O console exibe os recursos compartilhados com você.
4. Selecione um recurso compartilhado para ver seus detalhes.

AWS CLI

Para visualizar recursos compartilhados usando o AWS CLI, use o `list` comando apropriado para o tipo de recurso. Por exemplo, para listar a infraestrutura do Exadata:

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

A resposta mostra os recursos compartilhados com você.

Para obter informações detalhadas sobre um recurso compartilhado específico, use o `get` comando apropriado com o ID do recurso:

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

Configurando o emparelhamento ODB com redes ODB compartilhadas

Para permitir a comunicação entre seus aplicativos e bancos de dados em redes ODB compartilhadas, você pode configurar o emparelhamento de ODB entre sua VPC e a rede ODB compartilhada. Para obter mais informações sobre emparelhamento de ODB, consulte. Criando uma conexão de emparelhamento ODB no Oracle Database@AWS

Console

1. Abra o AWS console do Oracle Database@ em. https://console.aws.amazon.com/odb/
2. No painel de navegação, escolha ODB peering.

3. Escolha Criar peering de rede ODB.
4. Para rede ODB, selecione a rede ODB compartilhada com a qual você deseja fazer peering.
5. Em Rede ponto a ponto, selecione sua VPC.
6. Escolha Criar peering de rede ODB.

AWS CLI

Para criar uma conexão de emparelhamento de rede entre sua VPC e uma rede ODB compartilhada usando AWS CLI o, use o comando. `create-odb-peering-connection`

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

Depois de criar a conexão de peering, atualize suas tabelas de rotas para ativar o tráfego entre as redes com peering.

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

Gerenciando o Oracle Database@AWS

Você pode modificar e excluir alguns Oracle Database@AWS recursos depois de criá-los.

Atualizando uma rede ODB no Oracle Database@AWS

Você pode atualizar os seguintes recursos de rede ODB:

- O nome da rede ODB
- A Amazon VPC a ser usada para estabelecer uma conexão de emparelhamento ODB com a rede ODB
- Os intervalos de CIDR do VPC que podem acessar os recursos do Exadata na rede ODB

> **Note**
>
> Ao especificar intervalos de CIDR, você limita a conectividade às sub-redes VPC necessárias em vez de disponibilizar a VPC inteira para a rede ODB.

Esta seção pressupõe que você já tenha criado uma rede ODB em. Etapa 1: Criar uma rede ODB no Oracle Database@AWS

Para atualizar uma rede ODB

1. Faça login no Console de gerenciamento da AWS e abra o Oracle Database@AWS console em https://console.aws.amazon.com/odb/.
2. No painel esquerdo, escolha Redes ODB.
3. Selecione a rede que você deseja modificar.
4. Escolha Modificar.
5. (Opcional) Em Nome da rede ODB, insira um novo nome de rede. O nome deve ter de 1 a 255 caracteres e começar com um caractere alfabético ou sublinhado. Ele não pode conter hífens consecutivos.
6. (Opcional) Para emparelhado CIDRs, especifique os intervalos de CIDR da VPC emparelhada que precisam de conectividade com a rede ODB. Para limitar o acesso, recomendamos que você especifique os intervalos mínimos de CIDR necessários.

7. (Opcional) Para configurar integrações de serviços, selecione ou desmarque Amazon S3 ou Zero-ETL.
8. Escolha Continuar e, em seguida, escolha Modificar.

Excluindo uma rede ODB no Oracle Database@AWS

Você pode excluir uma rede ODB. Esta seção pressupõe que você já tenha criado uma rede ODB em. Etapa 1: Criar uma rede ODB no Oracle Database@AWS Você não pode excluir uma rede ODB que esteja sendo usada atualmente por um cluster de VM.

Para excluir uma rede ODB

1. Faça login no Console de gerenciamento da AWS e abra o Oracle Database@AWS console em https://console.aws.amazon.com/odb/.
2. No painel esquerdo, escolha Redes ODB.
3. Selecione a rede que você deseja excluir.
4. Escolha Excluir.
5. (Opcional) Escolha Excluir recursos OCI associados para excluir os recursos OCI que foram criados junto com a rede ODB.
6. Na caixa de texto, digite **`delete me`**.
7. Escolha Excluir.

Excluindo um cluster de VM no Oracle Database@AWS

Você pode excluir um cluster de VM Exadata ou um cluster de VM autônoma. Esta seção pressupõe que você já tenha criado um cluster de VM em. Etapa 3: criar um cluster de VM Exadata ou um cluster de VM autônoma no Oracle Database@AWS

Para excluir um cluster de VM

1. Faça login no Console de gerenciamento da AWS e abra o Oracle Database@AWS console em https://console.aws.amazon.com/odb/.
2. No painel esquerdo, escolha clusters de VM do Exadata ou clusters de VM autônomos.
3. Escolha um cluster de VM para excluir.
4. Escolha Excluir.

5. Quando solicitado, insira **`delete me`** e escolha Excluir.

Excluindo uma infraestrutura Oracle Exadata no Oracle Database@AWS

Você pode excluir uma infraestrutura do Oracle Exadata. Esta seção pressupõe que você já tenha criado uma infraestrutura Oracle Exadata em. Etapa 2: Criar uma infraestrutura Oracle Exadata no Oracle Database@AWS Você não pode excluir uma infraestrutura do Exadata que esteja sendo usada atualmente por um cluster de VM.

Para excluir uma infraestrutura Oracle Exadata

1. Faça login no Console de gerenciamento da AWS e abra o Oracle Database@AWS console em https://console.aws.amazon.com/odb/.
2. No painel esquerdo, escolha Infraestruturas do Exadata.
3. Escolha uma infraestrutura do Exadata para excluir.
4. Escolha Excluir.
5. Quando solicitado, insira **`delete me`** e escolha Excluir.

Excluindo uma conexão de emparelhamento ODB

Quando você não precisar mais de uma conexão de emparelhamento ODB, poderá excluí-la. Você deve excluir todas as conexões de emparelhamento de ODB antes de excluir uma rede ODB.

Console

1. Faça login no Console de gerenciamento da AWS e abra o Oracle Database@AWS console em https://console.aws.amazon.com/odb/.
2. No painel de navegação, escolha Conexões de emparelhamento ODB.
3. Selecione a conexão de emparelhamento ODB a ser excluída.
4. Escolha Excluir.
5. Para confirmar a exclusão, insira **`delete me`** e escolha Excluir.

AWS CLI

Para excluir uma conexão de emparelhamento ODB, use o `delete-odb-peering-connection` comando.

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

Fazendo backup no Oracle Database@AWS

O Oracle Database@AWS fornece várias opções de backup para proteger seus bancos de dados Oracle. Você pode usar backups gerenciados pela Oracle que se integram perfeitamente ao Amazon S3 ou criar seus próprios backups gerenciados pelo usuário usando o Oracle Recovery Manager (RMAN).

Backups gerenciados pela Oracle para o Amazon S3

Quando você cria uma rede ODB, o Oracle Database@ configura AWS automaticamente o acesso à rede para backups gerenciados pela Oracle no Amazon S3. O OCI configura as entradas de DNS e as listas de segurança necessárias. Essas configurações permitem o tráfego entre a OCI Virtual Cloud Network (VCN) e o Amazon S3. A rede ODB não habilita nem controla backups automáticos.

Os backups gerenciados pela Oracle são totalmente gerenciados pela OCI. Ao criar seu banco de dados Oracle Exadata, você pode ativar backups automáticos escolhendo Habilitar backups automáticos no console OCI. Escolha um dos seguintes destinos de backup:

- Amazon S3
- Armazenamento de objetos OCI
- Serviço de recuperação autônoma

Para obter mais informações, consulte Backup do banco de dados Exadata na documentação da OCI.

Backups gerenciados pelo usuário no Amazon S3 no Oracle Database@AWS

Com o Oracle Database@AWS, você pode criar backups gerenciados pelo usuário do seu banco de dados usando o Exadata Database Service on Dedicated Infrastructure. Você faz backup de seus dados com o Oracle Recovery Manager (RMAN) e os armazena em seus buckets do Amazon S3. Você tem controle total sobre o agendamento de backup, as políticas de retenção e os custos de armazenamento, mantendo os benefícios do serviço gerenciado do Oracle AWS Database@.

> **Note**
>
> O Oracle Database@AWS não oferece suporte a backups gerenciados pelo usuário para o Autonomous Database on Dedicated Infrastructure.

Os backups gerenciados pelo usuário complementam as soluções de backup AWS gerenciado fornecidas pelo Oracle AWS Database@. Você pode usar backups manuais para requisitos de conformidade, recuperação de desastres entre regiões ou integração com fluxos de trabalho de gerenciamento de backup existentes.

Você pode usar as seguintes técnicas de backup gerenciado pelo usuário:

Backup seguro da Oracle

Transmita backups diretamente para o Amazon S3 com desempenho ideal.

Storage Gateway

Use o Storage Gateway para backups baseados em arquivos que usam um compartilhamento NFS.

Ponto de montagem S3

Use um cliente de arquivos para montar um bucket do Amazon S3 como um sistema de arquivos local.

Pré-requisitos para backups gerenciados pelo usuário no Amazon S3 no Oracle Database@AWS

Antes de fazer backup de seus bancos de dados Oracle Exadata no Amazon S3, faça o seguinte:

1. Habilite o acesso direto ao Amazon S3 a partir da sua rede ODB.
2. Configure a conectividade e o roteamento de rede entre o Oracle Database@ e o Amazon AWS S3.

Habilitando o acesso da sua rede ODB ao Amazon S3

Para fazer backup manual do seu banco de dados no Amazon S3, habilite o acesso direto ao S3 a partir da sua rede ODB. Essa técnica permite que seus bancos de dados acessem o Amazon S3

para suas necessidades comerciais, como importação/exportação de dados ou backups gerenciados pelo usuário. Você tem controle total sobre o destino de destino do armazenamento de backup e pode usar políticas para restringir o acesso ao Amazon S3 usando o VPC Lattice.

O acesso direto ao Amazon S3 a partir da sua rede ODB não está habilitado por padrão. Você pode ativar o acesso ao S3 ao criar ou modificar sua rede ODB.

Console

Para habilitar o acesso direto ao Amazon S3 a partir da sua rede ODB

1. Abra o AWS console Oracle Database@ em. https://console.aws.amazon.com/odb/
2. No painel de navegação, escolha Redes ODB.
3. Selecione a rede ODB para a qual você deseja habilitar o acesso ao Amazon S3.
4. Escolha Modificar.
5. Selecione Amazon S3.
6. (Opcional) Configure um documento de política do Amazon S3 para controlar o acesso ao Amazon S3. Se você não especificar uma política, a política padrão concederá acesso total.
7. Escolha Continuar e, em seguida, Modificar.

AWS CLI

Para habilitar o acesso direto ao Amazon S3 a partir da sua rede ODB, use o `update-odb-network` comando com o parâmetro: `s3-access`

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

Para configurar um documento de política do Amazon S3, use o `--s3-policy-document` parâmetro:

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

Quando o acesso ao Amazon S3 está habilitado, você pode acessar o Amazon S3 a partir da sua rede ODB usando o DNS regional. `s3.region.amazonaws.com` O OCI configura esse nome DNS

por padrão. Para usar um nome DNS personalizado, modifique seu DNS VCN para garantir que o DNS personalizado seja resolvido para o endereço IP do endpoint da rede de serviços.

Configurando a conectividade de rede entre o Oracle Database@AWS e o Amazon S3

Para permitir backups gerenciados pelo usuário no Amazon S3, sua VM deve ser capaz de acessar o endpoint Amazon VPC do S3. No console OCI, você pode editar as regras de segurança em um grupo de segurança de rede (NSG) para controlar o tráfego de entrada e saída. Para backups gerenciados pelo usuário, o tráfego flui pela sub-rede do cliente em vez da sub-rede de backup. Nas etapas a seguir, você atualiza a sub-rede do cliente NSGs para adicionar a regra de saída para o endereço IP do VPC endpoint.

Para permitir o acesso da VM ao endpoint do Amazon S3

1. Abra o AWS console Oracle Database@ em. https://console.aws.amazon.com/odb/
2. Escolha redes ODB.
3. Escolha o nome da rede ODB.
4. Escolha os recursos do OCI.
5. Escolha a guia Integrações de serviços.
6. No Amazon S3, observe as seguintes informações:
   - O IPv4 endereço do endpoint Amazon VPC S3. Você precisará dessas informações mais tarde. Por exemplo, o endereço IP pode ser`192.168.12.223`.
   - O nome de domínio do endpoint Amazon VPC S3. Você precisará dessas informações mais tarde. Por exemplo, o nome do domínio pode ser`s3.us-east-1.amazonaws.com`.
7. No painel de navegação esquerdo, escolha Clusters de VM do Exadata e, em seguida, escolha o nome do seu cluster de VM.
8. Na parte superior da página, escolha a guia Resumo.
9. Escolha Máquinas virtuais e, em seguida, escolha o nome da sua VM.
10. Anote o valor em Nome DNS. Esse é o nome do host que você especifica ao se conectar à sua VM usando`ssh`.
11. No canto superior direito, escolha Gerenciar no OCI. Isso abre o console OCI.
12. Na página de listagem Virtual Cloud Networks, escolha o VCN que contém o grupo de segurança de rede (NSG) para a sub-rede do cliente de rede ODB (). `exa_static_nsg` Para obter mais informações, consulte Gerenciando regras de segurança para um NSG na documentação da OCI.

13. Na página de detalhes, execute uma das ações a seguir, dependendo da opção exibida:
    - Na guia Segurança, vá para Grupos de Segurança de Rede.
    - Em Recursos, escolha Grupos de segurança de rede.
14. Escolha o NSG para a sub-rede do cliente ()`exa_static_nsg`.
15. Adicione uma regra de saída para o endereço do VPC endpoint que você anotou anteriormente.

Para testar a conectividade com o S3 a partir da sua VM

1. Use `ssh` para se conectar `root` à VM cujo nome DNS você obteve anteriormente. Ao se conectar, especifique um `.pem` arquivo com suas chaves SSH.
2. Execute os comandos a seguir para garantir que a VM possa acessar o endpoint Amazon S3 Amazon VPC. Use o nome de domínio S3 que você anotou anteriormente.

```
# 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
```

Fazendo backup no Amazon S3 usando o Oracle Secure Backup

O Oracle Secure Backup atua como uma interface SBT para uso com o Recovery Manager (RMAN). Você pode usar o RMAN com o Oracle Secure Backup para fazer backup de seus AWS bancos de dados Oracle Database@ diretamente no Amazon S3. O Oracle Secure Backup oferece os seguintes benefícios:

- O Oracle Secure Backup otimiza a transferência de dados entre o RMAN e o S3.
- Nenhum armazenamento intermediário de backup é necessário.
- O Oracle Secure Backup gerencia o ciclo de vida de sua mídia de backup.

Para fazer backup no Amazon S3 usando o Oracle Secure Backup

1. Instale o módulo Oracle Secure Backup em seu servidor Exadata VM. Substitua os valores do espaço reservado por sua chave de AWS acesso e chave de acesso secreta. Para obter mais informações, consulte a documentação da Oracle em 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. Conecte-se ao RMAN e configure o canal de backup e o tipo de dispositivo padrão.

```
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. Verifique a configuração.

```
RMAN> SHOW ALL;
```

4. Faça backup do bancos de dados.

```
RMAN> BACKUP DATABASE;
```

5. Verifique se o backup foi concluído com êxito.

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

Fazendo backup no Amazon S3 AWS Storage Gateway usando na Amazon EC2

AWS Storage Gateway é um serviço híbrido que conecta seu ambiente local aos serviços Nuvem AWS de armazenamento. Para AWS backups do Oracle Database@, você pode usar o Storage Gateway para criar um fluxo de trabalho de backup baseado em arquivos que grava diretamente no Amazon S3. Diferentemente da técnica do Oracle Secure Backup, você gerencia o ciclo de vida dos backups.

Nessa solução, você cria uma EC2 instância separada da Amazon para configurar o Storage Gateway. Você também adiciona um volume do Amazon EBS para armazenar em cache as leituras e gravações no Amazon S3.

Essa técnica oferece os seguintes benefícios:

- Você não precisa de um gerenciador de mídia como o Oracle Secure Backup.
- Nenhum armazenamento intermediário de backup é necessário.

Para implantar seu Storage Gateway e criar um compartilhamento de arquivos

1. Abra o Console de gerenciamento da AWS at https://console.aws.amazon.com/storagegateway/home/ e escolha a AWS região onde você deseja criar seu gateway.
2. Implante e ative um gateway de arquivos Amazon S3, usando uma EC2 instância da Amazon como hub. Siga as instruções em Implantar um EC2 host Amazon personalizado para o S3 File Gateway no Guia do usuário do Storage Gateway.

   Ao configurar seu gateway de arquivos, certifique-se de fazer o seguinte:

   - Adicione pelo menos um volume do Amazon EBS para armazenamento em cache, com um tamanho de pelo menos 150 GiB.
   - Abra a TCP/UDP porta 2049 para acesso ao NFS em seu grupo de segurança. Isso permite que você crie compartilhamentos de arquivos NFS.
   - Abra a porta TCP 80 para tráfego de entrada para permitir acesso HTTP único durante a ativação do gateway. Após a ativação, será possível fechar essa porta.
3. Crie um endpoint Amazon VPC para conectividade privada entre sua rede ODB e o Storage Gateway. Para obter mais informações, consulte Acessar um AWS serviço usando uma interface VPC endpoint.
4. Crie um compartilhamento de arquivos para seu bucket do Amazon S3 por meio do console do Storage Gateway. Para obter mais informações, consulte Criação de um compartilhamento de arquivos.

Para fazer backup do seu banco de dados no Amazon S3 usando o Storage Gateway

1. Em um terminal, use `ssh` para se conectar ao nome DNS da VM do Exadata. Para encontrar o nome do DNS, consultePré-requisitos para backups gerenciados pelo usuário no Amazon S3 no Oracle Database@AWS.
2. Crie um diretório no servidor de cluster Exadata VM para a montagem do NFS. O exemplo a seguir cria o diretório `/home/oracle/sgw_mount/`.

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

3. Monte o compartilhamento NFS no diretório que você acabou de criar. O exemplo a seguir cria o compartilhamento no diretório`/home/oracle/sgw_mount/`. *SG-IP-address*Substitua pelo endereço IP do Storage Gateway e *your-bucket-name* pelo nome do bucket do S3.

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

4. Conecte-se ao RMAN e faça backup do banco de dados no diretório montado. O exemplo a seguir cria o canal `rman_local_bkp` e usa o caminho do ponto de montagem para formatar as peças de backup.

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

5. Verifique se os arquivos de backup foram criados no diretório de montagem. O exemplo a seguir mostra duas peças de backup.

```
$ 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
```

Fazendo backup no Amazon S3 usando um ponto de montagem S3

Você pode usar o ponto de montagem do Amazon S3 para criar backups localmente primeiro e depois copiá-los para o Amazon S3. Essa técnica cria backups no armazenamento local e depois os transfere para o Amazon S3 usando a interface de ponto de montagem. O tempo de backup é maior do que em outras técnicas porque você precisa fazer backup dos dados duas vezes.

> **Note**
>
> O backup direto para o Amazon S3 usando o ponto de montagem, sem preparação, não é suportado. O RMAN exige permissões específicas do sistema de arquivos que não são compatíveis com a interface de ponto de montagem do Amazon S3.

Essa técnica não exige que você licencie um gerenciador de mídia, como o Oracle Secure Backup. Você gerencia o ciclo de vida dos seus backups.

Para fazer backup no Amazon S3 usando um ponto de montagem S3

1. Em um terminal, use `ssh` para se conectar ao nome DNS da VM do Exadata. Para encontrar o nome do DNS, consultePré-requisitos para backups gerenciados pelo usuário no Amazon S3 no Oracle Database@AWS.
2. Instale o ponto de montagem do Amazon S3 no servidor de cluster Exadata VM. Para obter mais informações sobre instalação e configuração, consulte Mountpoint for Amazon S3 no Guia do usuário do Amazon S3.

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

3. Verifique a instalação executando o `mount-s3` comando.

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

4. Crie um diretório de backup intermediário no armazenamento local do servidor de cluster Exadata VM. Você fará backup do seu banco de dados nesse diretório local e, em seguida, copiará o backup para o bucket do S3. O exemplo a seguir cria um diretório`/u02/rman_bkp_local`.

   ```
   mkdir /u02/rman_bkp_local
   ```

5. Crie um diretório para o ponto de montagem do Amazon S3. O exemplo a seguir cria um diretório`/home/oracle/s3mount`.

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

6. Monte seu bucket Amazon S3 usando o ponto de montagem. O exemplo a seguir monta um bucket do S3 no diretório. `/home/oracle/s3mount` *`your-s3-bucket-name`*Substitua pelo nome real do bucket do Amazon S3.

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

7. Verifique se você pode acessar o conteúdo do bucket do Amazon S3.

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

8. Conecte o RMAN ao seu banco de dados de destino e faça backup dele em seu diretório de preparação local. O exemplo a seguir cria o canal `rman_local_bkp` e usa o caminho `/u02/rman_bkp_local/` para formatar as peças de backup.

```
$ rman TARGET /

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

9. Verifique se os backups foram criados no diretório local:

```
$ 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. Copie os arquivos de backup do diretório de armazenamento local para o ponto de montagem do Amazon S3.

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

11. Verifique se você copiou os arquivos com sucesso para o 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
```

Desabilitando o acesso direto ao Amazon S3

Se você não precisar mais de acesso direto ao Amazon S3 a partir da sua rede ODB, você pode desativá-lo. Ativar ou desativar o acesso direto à rede ao S3 não afeta o acesso à rede aos backups gerenciados pela Oracle no Amazon S3.

Console

Para desativar o acesso direto ao Amazon S3

1. Abra o AWS console Oracle Database@ em. https://console.aws.amazon.com/odb/
2. No painel de navegação, escolha Redes ODB.
3. Selecione a rede ODB para a qual você deseja desativar o acesso ao Amazon S3.
4. Escolha Modificar.
5. Desmarque a caixa de seleção Ativar acesso ao S3.
6. Escolha Modificar rede ODB.

AWS CLI

Use o comando `update-odb-network` com o parâmetro `s3-access`.

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

Solução de problemas da integração com o Amazon S3

Se você encontrar problemas com os backups gerenciados pela Oracle no Amazon S3 ou com o acesso direto ao Amazon S3, considere as seguintes etapas de solução de problemas:

Não é possível acessar o Amazon S3 a partir do seu banco de dados

Verifique o seguinte:

- Verifique se o acesso ao Amazon S3 está habilitado para sua rede ODB. Use a `GetOdbNetwork` ação para verificar se o `s3Access` status é`Enabled`.
- Verifique se você está usando o nome DNS regional correto:`s3.region.amazonaws.com`.

- Verifique se seu banco de dados Oracle tem as permissões necessárias para acessar o Amazon S3.

Falha nos backups gerenciados pela Oracle

Verifique o seguinte:

- Os backups gerenciados pela Oracle para o Amazon S3 estão habilitados por padrão e não podem ser desativados. Se os backups estiverem falhando, verifique se há mensagens de erro específicas nos logs do banco de dados Oracle.
- Verifique se os recursos do Amazon VPC Lattice estão configurados corretamente visualizando os recursos de integração de serviços.
- Entre em contato com o Suporte da Oracle para obter ajuda com problemas de backup automático gerenciado pela Oracle. Para obter mais informações, consulte Obtendo suporte para o Oracle Database@AWS.

Integração do Oracle Database@AWS Zero-ETL com o Amazon Redshift

A integração Zero-ETL é uma solução totalmente gerenciada que disponibiliza dados transacionais e operacionais no Amazon Redshift a partir de várias fontes. Com essa solução, você pode replicar dados para o Amazon Redshift a partir de seus bancos de dados Oracle executados no Oracle Exadata ou no Autonomous Database na infraestrutura dedicada do Exadata. A sincronização automática evita o processo tradicional de extração, transformação e carregamento (ETL). Ele também permite análises em tempo real e cargas de trabalho de IA. Consulte mais informações em Integrações ETL zero no Guia de gerenciamento do Amazon Redshift.

A integração Zero-ETL oferece os seguintes benefícios:

- Replicação de dados em tempo real — sincronização contínua de dados dos bancos de dados Oracle para o Amazon Redshift com latência mínima
- Eliminação de pipelines ETL complexos — Não há necessidade de criar e manter soluções personalizadas de integração de dados
- Redução da sobrecarga operacional — Configuração e gerenciamento automatizados por meio de AWS APIs
- Arquitetura simplificada de integração de dados — integração perfeita entre o Oracle Database@AWS e os serviços de análise AWS
- Segurança aprimorada — criptografia integrada e controles de acesso AWS IAM

O Amazon Redshift não cobra uma taxa adicional pela integração Zero-ETL com o Oracle Database@.AWS Você paga pelos recursos existentes do Amazon Redshift usados para criar e processar os dados de alteração criados como parte de uma integração sem ETL. Para obter mais informações, consulte Preços do Amazon Redshift.

Versões de banco de dados suportadas para integração com Zero-ETL no Oracle Database@AWS

A integração Zero-ETL suporta as seguintes versões do banco de dados Oracle:

- Oracle Exadata — Banco de dados Oracle 19c
- Banco de dados autônomo em infraestrutura dedicada — Oracle Database 19c e 23ai

Como a integração Zero-ETL funciona no Oracle Database@AWS

A integração sem ETL permite que o Oracle Database@ replique dados AWS para o Amazon Redshift. A integração aproveita o Amazon VPC Lattice para criar conectividade de rede segura. A tecnologia Change Data Capture (CDC) garante a sincronização de dados em tempo real. Você gerencia a integração por meio de AWS Glue APIs.

A arquitetura de integração Zero-ETL inclui o seguinte:

- Conectividade segura — usa SSL/TLS criptografia pela porta TLS 2484 para transferência de dados
- AWS Secrets Manager — Armazena credenciais e certificados de banco de dados com segurança usando o Key Management Service AWS
- AWS Integração com Glue — fornece uma interface de gerenciamento unificada para integrações sem ETL

A replicação prossegue com as seguintes etapas:

1. Estabelecendo conexão segura com o banco de dados Oracle usando SSL na porta 2484
2. Executando um despejo inicial completo dos bancos de dados, esquemas e tabelas selecionados
3. Configurando a captura de dados de alteração (CDC) para replicação contínua em tempo real
4. Gravando os dados replicados no cluster de destino do Amazon Redshift

> **Important**
>
> A integração Zero-ETL não está habilitada por padrão. Você deve configurá-lo usando AWS Glue APIs. Você não pode configurar a integração Zero-ETL diretamente usando o Oracle Database@.AWS APIs

Pré-requisitos para integração com ETL zero no Oracle Database@AWS

Antes de configurar a integração Zero-ETL, certifique-se de atender aos seguintes pré-requisitos.

Pré-requisitos gerais

- AWS Configuração do Oracle Database@ — Certifique-se de ter pelo menos um cluster de VM provisionado e em execução.
- Integração com Zero-ETL ativado — Certifique-se de que seu cluster de VM ou cluster de VM autônoma esteja associado a uma rede ODB com Zero-ETL ativado.
- Versões do Oracle Database suportadas — Você deve usar o Oracle Database 19c (Oracle Exadata) ou o Oracle Database 19c/23ai (Banco de dados autônomo em infraestrutura dedicada).
- Mesma AWS região — O banco de dados Oracle de origem e o cluster do Amazon Redshift de destino devem estar na mesma AWS região.

Pré-requisitos do banco de dados Oracle

Você deve configurar seu banco de dados Oracle com as seguintes configurações.

Configuração do usuário de replicação

Crie um usuário de replicação dedicado em cada banco de dados conectável (PDB) que você deseja replicar:

- Para Oracle Exadata — Crie um usuário `ODBZEROETLADMIN` com uma senha segura.
- Para banco de dados autônomo em infraestrutura dedicada — Use o `GGADMIN` usuário existente.

Conceda as seguintes permissões ao usuário de replicação.

```
-- 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";
```

Registro em log complementar

Ative o registro suplementar em seu banco de dados Oracle para capturar dados de alteração.

```
-- 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;
```

Para configurar uma integração sem ETL entre o Oracle Database@ e o AWS Amazon Redshift, você deve configurar o SSL.

Para bancos de dados Oracle Exadata

Você deve configurar manualmente o SSL na porta 2484. Essa tarefa envolve o seguinte:

- Configurando em `(PROTOCOL=tcps)(PORT=2484)` `listener.ora`
- Configurando a carteira usando `sqlnet.ora`
- Geração e configuração de certificados SSL (consulte Como configurar SSL/TCPS o Exadata Cloud Database (ExAcc/EXACS) (ID do documento 2947301.1) na documentação do My Oracle Support)

Para bancos de dados autônomos

O SSL na porta 2484 está habilitado por padrão. Não é exigida nenhuma configuração adicional.

> **Important**
>
> A porta SSL é fixada como 2484.

AWS pré-requisitos de serviço

Antes de configurar a integração Zero-ETL, configure o AWS Secrets Manager e configure as permissões do IAM.

Configurar o AWS Secrets Manager

Armazene suas credenciais do banco de dados Oracle no AWS Secrets Manager da seguinte forma:

1. Crie uma chave gerenciada pelo cliente (CMK) no AWS Key Management Service.
2. Armazene as credenciais do banco de dados no AWS Secrets Manager usando a CMK.
3. Configure políticas de recursos para permitir o acesso ao Oracle Database@AWS .

Para obter o ID e a senha da chave do TDE, use a técnica descrita em Métodos de criptografia suportados para usar o Oracle como fonte para o AWS Database Migration Service. O comando a seguir gera a carteira base64.

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

O exemplo a seguir mostra um segredo para o Oracle Exadata. Pois*asm_service_name*, o *111.11.11.11* representa o IP virtual do nó da VM. Você também pode registrar o ouvinte ASM com o 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"
  }
```

```
}
```

O exemplo a seguir mostra um segredo para o Banco de Dados Autônomo em Infraestrutura Dedicada.

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

Configurar permissões do IAM

Crie políticas de IAM que permitam operações de integração sem ETL. O exemplo de política a seguir permite descrever, criar, atualizar e excluir operações para um cluster de VM do Exadata. Para um cluster de VM autônomo, use o valor `cloud-autonomous-vm-cluster` em vez do `cloud-vm-cluster` ARN do recurso.

Considerações sobre a integração sem ETL no Oracle Database@AWS

Ao configurar a integração sem ETL entre o Amazon Redshift e o Amazon Oracle Database@AWS Redshift, considere as seguintes diretrizes:

Tempo inicial de carregamento de dados

O tempo inicial de carregamento total depende do tamanho do seu banco de dados. Bancos de dados grandes podem levar várias horas ou dias para concluir a sincronização inicial.

Desempenho do banco de dados Oracle

A captura de dados de alterações pode afetar o desempenho do banco de dados Oracle, especialmente durante altos volumes de transações. Depois de habilitar a integração Zero-ETL, monitore o desempenho do seu banco de dados.

Alterações de esquema

Alterações na linguagem de definição de dados (DDL) no banco de dados Oracle de origem podem exigir que você intervenha manualmente para recriar a integração. Planeje as mudanças no esquema com cuidado.

Para considerações gerais, consulte Considerações ao usar integrações sem ETL com o Amazon Redshift.

Limitações da integração Zero-ETL no Oracle Database@AWS

Observe as seguintes limitações gerais:

PDB único por integração

Cada integração Zero-ETL só pode replicar dados de um banco de dados conectável (PDB). Filtros de dados como esses `include: pdb1.*.*, include: pdb2.*.*` não são suportados.

Integração única por banco de dados autônomo ou infraestrutura Exadata

Cada integração com zero ETL só pode replicar dados de um banco de dados autônomo em uma infraestrutura dedicada.

Porta SSL fixa

As conexões SSL devem usar a porta 2484.

Exigência da mesma região

O cluster de AWS VM Oracle Database@ de origem e o cluster Amazon Amazon Redshift de destino devem estar na mesma região. AWS A replicação entre regiões não é suportada.

Sem suporte para mTLS

O TLS mútuo (mTLS) não é suportado. Se seu banco de dados OCI tiver o mTLS ativado, você deverá desativá-lo para usar a integração Zero-ETL.

Configurações de integração imutáveis

Depois de criar o ARN secreto ou a chave KMS associada a uma integração, você não poderá modificá-la. Você deve excluir e recriar a integração para alterar essas configurações.

Criptografia em nível de coluna do TDE

A Criptografia de Dados Transparente (TDE) em nível de coluna não é compatível com bancos de dados Oracle Exadata. Somente o TDE em nível de tablespace é suportado.

Suporte ao tipo de dados

Alguns tipos de dados específicos da Oracle podem não ser totalmente suportados ou podem exigir transformação durante a replicação. Teste minuciosamente seus tipos de dados específicos antes de implantar seu banco de dados na produção.

Configurando AWS integrações do Oracle Database@ com o Amazon Redshift

Para configurar a integração sem ETL entre seu banco de dados Oracle e o Amazon Redshift, conclua as seguintes etapas:

1. Ative o Zero-ETL na sua rede ODB.
2. Configure os pré-requisitos do banco de dados Oracle.
3. Configure o AWS Secrets Manager e o AWS Key Management Service.
4. Configurar permissões do IAM
5. Configure as políticas de recursos do Amazon Redshift.
6. Crie a integração Zero-ETL.
7. Crie o banco de dados de destino no Amazon Redshift.

Etapa 1: Habilitar Zero-ETL para sua rede ODB

Você pode ativar a integração Zero-ETL para a rede ODB associada ao seu cluster de VM de origem. Por padrão, essa integração está desativada.

Console

Para habilitar a integração Zero-ETL

1. Abra o AWS console Oracle Database@ em. https://console.aws.amazon.com/odb/
2. No painel de navegação, escolha Redes ODB.
3. Selecione a rede ODB para a qual você deseja habilitar a integração Zero-ETL.

4. Escolha Modificar.
5. Selecione Zero-ETL.
6. Escolha Continuar e, em seguida, Modificar.

AWS CLI

Para habilitar a integração Zero-ETL, use o `update-odb-network` comando com o parâmetro: `--zero-etl-access`

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

Para habilitar a integração Zero-ETL para a rede ODB associada ao seu cluster de VM de origem, use o comando. `update-odb-network` Esse comando configura a infraestrutura de rede necessária para a integração Zero-ETL.

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

Etapa 2: Configurar seu banco de dados Oracle

Conclua a configuração do banco de dados Oracle conforme descrito nos Pré-requisitos:

- Crie usuários de replicação e conceda as permissões necessárias.
- Ative os redo logs arquivados.
- Configure o SSL (somente Oracle Exadata).
- Configure usuários do ASM, se aplicável (somente Oracle Exadata).

Etapa 3: Configurar o AWS Secrets Manager e o AWS Key Management Service

Crie uma Chave Gerenciada pelo Cliente (CMK) e armazene suas credenciais de banco de dados.

1. Crie uma CMK no AWS Key Management Service usando o `create-key` comando.

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

2. Armazene suas credenciais de banco de dados no 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. Anexe uma política de recursos ao segredo para permitir o acesso ao Oracle Database@AWS .

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

No comando anterior, `secret-resource-policy.json` contém o seguinte JSON.

JSON

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

4. Anexe uma política de recursos à CMK. A política de recursos da CMK deve incluir permissões para o responsável pelo serviço principal do Oracle Database@ e pelo responsável pelo AWS serviço principal do Amazon Redshift para oferecer suporte à integração criptografada de zero ETL.

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

O `cmk-resource-policy.json` arquivo deve incluir as seguintes declarações de política. A primeira instrução permite o acesso ao AWS serviço Oracle Database@ e a segunda permite que o Amazon Redshift crie concessões na chave KMS para operações de dados criptografados.

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"
          ]
        }
      }
    }
  ]
}
```

Etapa 4: configurar as permissões do IAM

Crie e anexe políticas do IAM que permitam operações de integração sem 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
```

A política a seguir concede as permissões necessárias.

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": "*"
    }
  ]
}
```

Etapa 5: Configurar as políticas de recursos do Amazon Redshift

Configure políticas de recursos em seu cluster do Amazon Redshift para autorizar integrações de entrada.

```
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**
>
> Como alternativa, você pode usar a opção Corrigir para mim no AWS console. Essa opção configura automaticamente as políticas necessárias do Amazon Redshift sem que você precise fazer isso manualmente.

Etapa 6: Crie a integração Zero-ETL usando AWS Glue

Crie a integração Zero-ETL usando o comando. AWS Glue `create-integration` Nesse comando, você especifica o cluster de VM de origem e o namespace Amazon Redshift de destino.

O exemplo a seguir cria uma integração com um PDB chamado em `pdb1` execução em um cluster de VM do Exadata. Você também pode criar um cluster de VM autônomo `cloud-vm-cluster` substituindo-o por `cloud-autonomous-vm-cluster` no ARN de origem. Especificar uma chave KMS é opcional. Se você especificar uma chave, ela poderá ser diferente daquela que você criou emEtapa 3: Configurar o AWS Secrets Manager e o 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"
```

O comando retorna um ARN de integração e define o status como. `creating` Você pode monitorar o status da integração usando o `describe-integrations` comando.

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

> **Important**
>
> Somente um PDB por integração é suportado. O filtro de dados deve especificar um único PDB, por exemplo,`include: pdb1.*.*`. A origem deve estar na mesma AWS região e conta em que a integração está sendo criada.

Etapa 7: Criar um banco de dados de destino no Amazon Redshift

Depois que a integração estiver ativa, crie um banco de dados de destino em seu cluster do Amazon Redshift.

```
-- 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";
```

Depois de criar o banco de dados de destino, você pode consultar os dados replicados.

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

-- Connect to the new database
\c target_database_name

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

Verifique a integração Zero-ETL

Verifique se a integração funciona consultando o status da integração AWS Glue e certificando-se de que suas alterações no Oracle estejam sendo replicadas para o Amazon Redshift.

Para verificar se sua integração com Zero-ETL está funcionando corretamente

1. Verifique o status da integração.

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

O status deve ser `ACTIVE` ou`REPLICATING`.

2. Verifique a replicação de dados fazendo alterações em seu banco de dados Oracle e verificando se elas aparecem no Amazon Redshift.
3. Monitore as métricas de replicação na Amazon CloudWatch (se disponível).

Filtragem de dados para integrações com zero ETL em Oracle Database@AWS

Oracle Database@AWS As integrações Zero-ETL oferecem suporte à filtragem de dados. Você pode usá-lo para controlar quais dados seu banco de dados Oracle Exadata de origem replica no data warehouse de destino. Em vez de replicar todo o banco de dados, você pode aplicar um ou mais filtros para incluir ou excluir seletivamente tabelas específicas. Isso ajuda a otimizar o desempenho do armazenamento e das consultas, garantindo que somente os dados relevantes sejam transferidos. A filtragem é limitada aos níveis do banco de dados e da tabela. A filtragem em nível de coluna e linha não é suportada.

O banco de dados Oracle e o Amazon Redshift lidam com maiúsculas e minúsculas de nomes de objetos de forma diferente, o que afeta tanto a configuração do filtro de dados quanto as consultas de destino. Observe o seguinte:

- O banco de dados Oracle armazena nomes de bancos de dados, esquemas e objetos em maiúsculas, a menos que seja explicitamente citado na instrução `CREATE`. Por exemplo, se você criar `mytable` (sem aspas), o dicionário de dados Oracle armazenará o nome da tabela como `MYTABLE`. Se você citar o nome do objeto em sua declaração de criação, o dicionário de dados Oracle preservará a maiúscula e minúscula.
- Os filtros de dados ETL zero diferenciam maiúsculas e minúsculas e devem corresponder exatamente às maiúsculas e minúsculas dos nomes dos objetos conforme eles aparecem no dicionário de dados Oracle. Por exemplo, se o dicionário Oracle armazenar o esquema e o nome da tabela`REINVENT.MYTABLE`, crie um filtro usando`include: ORCL.REINVENT.MYTABLE`.
- As consultas do Amazon Redshift usam como padrão nomes de objetos em minúsculas, a menos que sejam explicitamente citados. Por exemplo, uma consulta de `MYTABLE` (sem aspas) procura `mytable`.

Preste atenção às diferenças de tamanho da letra ao criar o filtro do Amazon Redshift e consultar os dados. As considerações de filtragem para Oracle Database@AWS são as mesmas do Amazon RDS for Oracle. Para obter exemplos de como o caso pode afetar os filtros de dados em um banco de dados Oracle, consulte exemplos do RDS for Oracle no Guia do Usuário do Amazon Relational Database Service.

Monitorando a integração Zero-ETL

O monitoramento regular de sua integração Zero-ETL garante um desempenho ideal e ajuda a identificar problemas precocemente.

Monitoramento do status de integração

Monitore o status de suas integrações com ETL zero usando o 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
```

Os status de integração incluem:

- criando — A integração está sendo configurada
- ativo — a integração está sendo executada e replicando dados
- modificando — A configuração de integração está sendo atualizada
- needs_attention — A integração requer intervenção manual
- falhou — A integração encontrou um erro
- excluindo — A integração está sendo removida

Monitoramento do desempenho

Monitore os seguintes aspectos do seu desempenho de integração com ETL zero:

- Atraso na replicação — A diferença de tempo entre quando uma alteração ocorre no Oracle e quando ela aparece no Amazon Redshift

- Taxa de transferência de dados — O volume de dados que estão sendo replicados por unidade de tempo
- Taxas de erro — a frequência de erros ou falhas de replicação
- Utilização de recursos — uso de CPU, memória e rede nos sistemas de origem e de destino

Use CloudWatch a Amazon para monitorar essas métricas e configurar alarmes para limites críticos.

Gerenciando integrações sem ETL no Oracle Database@AWS

Depois de criar uma integração sem ETL, você pode realizar várias operações de gerenciamento, incluindo modificar e excluir integrações. Esta seção aborda o gerenciamento contínuo de suas integrações com ETL zero.

Modificar integrações ETL zero

É possível modificar somente o nome, a descrição e as opções de filtragem de dados de uma Integração ETL zero em um data warehouse compatível. Você não pode modificar a AWS chave do Serviço de Gerenciamento de Chaves usada para criptografar a integração ou os bancos de dados de origem ou de destino.

Pré-requisitos para modificar integrações

Antes de modificar uma integração com ETL zero, verifique se você tem o seguinte:

- Permissões necessárias — Seu usuário ou função do IAM deve ter a `odb:UpdateOutboundIntegration` permissão além das AWS Glue permissões padrão.
- Integração no estado ativo — A integração deve estar em um `ACTIVE` estado, não em`CREATING`,`MODIFYING`,`DELETING`, ou`FAILED`.
- Sintaxe de filtro de dados válida — Os novos filtros de dados devem seguir a sintaxe include/exclude padrão compatível.

Modificando filtros de dados

Você pode alterar quais tabelas ou esquemas são replicados modificando o filtro de dados. Dessa forma, você pode adicionar ou remover objetos de banco de dados da replicação sem recriar toda a integração.

Para modificar o filtro de dados para uma integração, use o `modify-integration` comando.

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

Você também pode modificar o nome e a descrição da integração ao mesmo tempo. No exemplo a seguir, você modifica o nome, as descrições e os filtros da integração para dois esquemas em`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**
>
> Quando você modifica o filtro de dados, a integração entra em um `modifying` estado e executa uma ressincronização dos dados. A integração interrompe a replicação, aplica as novas configurações de filtro e retoma a replicação com uma operação de destino de recarga. Monitore o status da integração para garantir que a modificação seja concluída com êxito.

Considerações sobre modificações no filtro de dados em integrações com ETL zero

Considere o seguinte ao modificar os filtros de dados:

- Limitação de PDB único — Você só pode especificar um banco de dados conectável (PDB) por integração. Filtros de dados como `include: pdb1.*.*, include: pdb2.*.*` não são suportados
- Interrupção da replicação — a replicação de dados é interrompida durante o processo de modificação e é retomada após a aplicação do novo filtro.
- Recarga de dados — A integração executa uma recarga completa dos dados que correspondem aos novos critérios de filtro.
- Impacto no desempenho — Grandes alterações no filtro de dados podem levar um tempo significativo para serem concluídas e podem afetar o desempenho do banco de dados de origem durante a recarga.

Limitações para modificações nas configurações de integração Zero-ETL

Você não pode modificar as seguintes configurações depois de criar uma integração sem ETL:

- ARN secreto — O segredo do AWS Secrets Manager contendo credenciais do banco de dados
- Chave KMS — A chave gerenciada pelo cliente usada para criptografia
- ARN de origem — O cluster de VM do Oracle Database@AWS
- ARN de destino — O cluster ou namespace do Amazon Redshift

Para alterar essas configurações, exclua a integração Zero-ETL existente e crie uma nova.

Excluir integrações ETL zero

Quando você não precisar mais de uma integração com zero ETL, poderá excluí-la para interromper a replicação e limpar os recursos associados.

Exclusão usando AWS Glue

Exclua uma integração sem ETL usando a API AWS Glue.

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

Você pode excluir integrações nos seguintes estados:

- ativo
- precisa_atenção
- com falha
- sincronizando

Efeitos da exclusão

Ao excluir uma integração com zero ETL, considere os seguintes efeitos:

A replicação é interrompida.

O Oracle Database@AWS não replica novas alterações do Amazon Redshift.

Os dados existentes são preservados.

Os dados já replicados para o Amazon Redshift permanecem disponíveis.

O banco de dados de destino permanece.

O banco de dados do Amazon Redshift criado a partir da integração não é excluído automaticamente.

> **Important**
>
> A exclusão é irreversível. Se você precisar retomar a replicação após a exclusão, crie uma nova integração, que executa uma carga inicial completa.

Melhores práticas para gerenciamento de ETL zero

Siga essas melhores práticas para garantir o desempenho, a segurança e a economia ideais de suas integrações com ETL zero.

Melhores práticas operacionais

Essas práticas operacionais ajudam a manter integrações confiáveis e eficientes de zero ETL.

Monitoramento regular

Configure CloudWatch alarmes para monitorar as métricas de integridade e desempenho da integração.

Rotação de credenciais

Alterne regularmente as senhas do banco de dados e atualize-as no AWS Secrets Manager.

Verificação de backup

Verifique regularmente se os backups do banco de dados Oracle incluem os componentes necessários para a recuperação de desastres.

Testes de performance

Teste o impacto da integração com ETL zero no desempenho do seu banco de dados Oracle, especialmente durante os períodos de pico de uso.

Planejamento de mudança de esquema

Planeje e teste as alterações do esquema em um ambiente de desenvolvimento antes de aplicá-las à produção.

Práticas recomendadas de segurança

Implemente essas medidas de segurança para proteger sua integração e seus dados com zero ETL.

Acesso de privilégio mínimo

Conceda somente as permissões mínimas necessárias para usuários de replicação e funções AWS do IAM.

Segurança de rede

Use grupos de segurança e NACLs restrinja o acesso à rede somente às portas e fontes necessárias.

Criptografia em repouso

Garanta que os bancos de dados Oracle e os clusters do Amazon Redshift usem criptografia em repouso.

Registro em log de auditoria

Ative o registro de auditoria no Oracle e no Amazon Redshift para rastrear o acesso e as alterações aos dados.

Gerenciamento secreto

Use AWS os recursos de rotação automática do Secrets Manager sempre que possível.

Otimização de custos

Aplique essas estratégias para otimizar os custos e, ao mesmo tempo, manter um desempenho efetivo de integração sem ETL.

Filtragem de dados

Use filtros de dados precisos para replicar somente os dados de que você precisa, reduzindo os custos de armazenamento e computação.

Otimização do Amazon Redshift

Use os tipos de nós apropriados do Amazon Redshift e implemente a compactação de dados para otimizar os custos.

Monitoramento do uso

Analise regularmente o uso e os custos da integração Zero-ETL por meio do Cost Explorer AWS .

Limpe integrações não utilizadas

Exclua integrações que não são mais necessárias para evitar cobranças contínuas.

Solução de problemas de integração com Zero-ETL

Esta seção fornece orientação para resolver problemas comuns com a integração Zero-ETL.

Zero falhas na configuração da integração ETL

Falhas de autenticação

- Verifique se o usuário de replicação existe e tem a senha correta no AWS Secrets Manager.
- Certifique-se de que todas as permissões necessárias tenham sido concedidas ao usuário de replicação.
- Verifique se o ARN secreto está correto e acessível pelo Oracle Database@.AWS
- Verifique se a política de recursos da CMK permite o acesso pelo responsável pelo serviço Oracle Database@AWS .

Problemas de conectividade de rede

- Certifique-se de que sua rede ODB tenha a integração Zero-ETL ativada.
- Verifique se o SSL está configurado corretamente na porta 2484 (somente Exadata).
- Verifique se o ouvinte do banco de dados Oracle está em execução e aceitando conexões.
- Garanta que a rede se agrupe e NACLs permita o tráfego na porta 2484.
- Verifique se o nome do serviço em seu segredo corresponde ao nome real do serviço Oracle.

Erros de permissão

- Verifique se seu usuário ou função do IAM tem as permissões necessárias para operações de AWS Glue integração.
- Verifique se a política de recursos do Amazon Redshift permite integrações de entrada do seu cluster de VM.

- Certifique-se de que o Oracle Database@AWS tenha acesso aos seus segredos e à chave do AWS Key Management Service.

Problemas de replicação

Falhas de carga inicial

- Verifique se o banco de dados Oracle tem recursos suficientes para suportar a operação de carga total.
- Certifique-se de que o registro suplementar esteja ativado no banco de dados de origem.
- Verifique se há bloqueios ou restrições em nível de tabela que possam impedir a extração de dados.

Alterar problemas de captura de dados

- Verifique se o banco de dados Oracle tem espaço de redo log e retenção adequados.
- Verifique se o usuário de replicação tem acesso aos redo logs arquivados.
- Para sistemas habilitados para ASM, certifique-se de que o usuário ASM esteja configurado corretamente.
- Monitore o desempenho do banco de dados Oracle para garantir que o CDC não esteja causando contenção de recursos.

Alto atraso de replicação

- Monitore as métricas de atraso de replicação em. CloudWatch
- Verifique se há altos volumes de transações ou grandes transações no banco de dados de origem.
- Verifique se o cluster do Amazon Redshift tem capacidade adequada para lidar com dados recebidos.

Problemas de consistência de dados

Dados ausentes ou incompletos

- Verifique se o filtro de dados inclui todos os esquemas e tabelas necessários.
- Verifique se há tipos de dados não compatíveis que possam estar causando falhas na replicação.
- Certifique-se de que o usuário de replicação tenha permissões SELECT em todas as tabelas necessárias.

Erros de conversão do tipo de dados

- Analise os mapeamentos de tipos de dados compatíveis entre o Oracle e o Redshift.
- Verifique os tipos de dados específicos do Oracle que podem exigir tratamento personalizado.
- Considere modificar seu esquema Oracle para usar tipos de dados mais compatíveis.

Monitoramento e depuração

Use as seguintes abordagens para monitorar e depurar problemas de integração com ETL zero:

- Monitoramento do status da integração — Verifique regularmente o status da integração usando`aws glue describe-integrations`.
- CloudWatch métricas — monitore CloudWatch as métricas disponíveis para desempenho e erros de replicação.
- Monitoramento do banco de dados Oracle — monitore o desempenho e a utilização de recursos do banco de dados Oracle.
- Monitoramento do Redshift — Monitore o desempenho do cluster e a utilização do armazenamento do Amazon Redshift.

Para problemas complexos que não podem ser resolvidos usando este guia de solução de problemas, entre em contato AWS Support com as seguintes informações:

- ARN de integração e status atual.
- As mensagens de erro da integração descrevem as operações.
- Configurações de banco de dados Oracle e cluster do Amazon Redshift.
- Cronograma de quando o problema começou a ocorrer.

Segurança em Oracle Database@AWS

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre AWS a OCI e você. O modelo de responsabilidade compartilhada descreve isso como segurança na nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que é executada Serviços da AWS no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos seus dados, os requisitos da sua organização e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada modelo ao usar Oracle Database@AWS. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus Oracle Database@AWS recursos.

Você pode gerenciar o acesso aos seus Oracle Database@AWS recursos. O método usado para gerenciar o acesso depende do tipo de tarefa que você precisa executar com Oracle Database@AWS:

- Use políticas AWS Identity and Access Management (IAM) para atribuir permissões que determinam quem tem permissão para gerenciar Oracle Database@AWS recursos. Por exemplo, você pode usar o IAM para determinar quem tem permissão para criar, descrever, modificar e excluir a infraestrutura do Exadata, os clusters de VM ou os recursos de tags.
- Use os recursos de segurança do seu mecanismo de banco de dados Oracle para controlar quem pode fazer login nos bancos de dados em uma instância de banco de dados. Esses recursos funcionam como se o banco de dados estivesse em sua rede local.
- Use conexões Secure Socket Layers (SSL) ou Transport Layer Security (TLS) com bancos de dados Exadata. Para obter mais informações, consulte Preparar conexões TLS sem carteira.
- Oracle Database@AWS não é imediatamente acessível pela Internet e é implantado somente em sub-redes privadas. AWS

- Oracle Database@AWS usa muitas portas padrão do Protocolo de Controle de Transmissão (TCP) para várias operações. Para ver a lista completa de portas, consulte Atribuições de portas padrão.
- Para armazenar e gerenciar chaves usando a Transparent Data Encryption (TDE), que é ativada por padrão, Oracle Database@AWS usa cofres OCI ou Oracle Key Vault. Oracle Database@AWS não suporta AWS Key Management Service.
- Por padrão, o banco de dados é configurado usando chaves de criptografia gerenciadas pela Oracle. O banco de dados também oferece suporte a chaves gerenciadas pelo cliente.
- Para aprimorar a proteção de dados, use o Oracle Data Safe com Oracle Database@AWS o.

Os tópicos a seguir mostram como configurar para atender Oracle Database@AWS aos seus objetivos de segurança e conformidade.

Tópicos

Proteção de dados em Oracle Database@AWS

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com Centro de Identidade do AWS IAM ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.

- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para saber mais sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sensíveis, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Oracle Database@AWS ou outro Serviços da AWS usando o console, a API ou. AWS CLI AWS SDKs Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Criptografia de dados

Os bancos de dados Exadata usam o Oracle Transparent Data Encryption (TDE) para criptografar seus dados. Seus dados também são protegidos em espaços de tabela temporários, segmentos de desfazer, redo logs e durante operações internas do banco de dados, como JOIN e SORT. Para obter mais informações, consulte Segurança de dados.

Criptografia em trânsito

Os bancos de dados Exadata usam recursos nativos de criptografia e integridade do Oracle Net Services para proteger as conexões com o banco de dados. Para obter mais informações, consulte Segurança de dados em trânsito.

Gerenciamento de chaves

A criptografia transparente de dados inclui um armazenamento de chaves para armazenar com segurança as chaves mestras de criptografia e uma estrutura de gerenciamento para gerenciar

com segurança e eficiência o armazenamento de chaves e realizar as principais operações de manutenção. Para obter mais informações, consulte Para administrar as chaves de criptografia do Vault.

Gerenciamento de identidade e acesso para Oracle Database@AWS

AWS Identity and Access Management (IAM) é um AWS serviço que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do Oracle AWS Database@. O IAM é um AWS serviço que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte Solução de problemas Oracle Database@AWS de identidade e acesso).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte Como Oracle Database@AWS funciona com o IAM)
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte Políticas baseadas em identidade para o Oracle Database@AWS)

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte Como fazer login em sua Conta da AWS no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos Centro de Identidade do AWS IAM. Para saber mais, consulte O que é o IAM Identity Center? no Guia do usuário do Centro de Identidade do AWS IAM .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte Exigir que usuários humanos

usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias no Guia do usuário do IAM.

Um grupo do IAM especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma perfil do IAM é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função mudando de um usuário para uma função do IAM (console) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

As funções do IAM são úteis para acesso de usuários federados, permissões temporárias de usuários do IAM, acesso entre contas, acesso entre serviços e aplicativos executados na Amazon. EC2 Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissão JSON que você anexa a uma identidade (usuário, grupo ou perfil). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma

política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário especificar uma entidade principal em uma política baseada em recursos.

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — Especifique as permissões máximas para uma organização ou unidade organizacional em AWS Organizations. Para saber mais, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs) — Defina o máximo de permissões disponíveis para recursos em suas contas. Para obter mais informações, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como Oracle Database@AWS funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Oracle Database@AWS, saiba quais recursos do IAM estão disponíveis para uso com o Oracle Database@.AWS

Recurso do IAM	Oracle Database@AWS apoio
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Perfis vinculados ao serviço	Sim

Para ter uma visão de alto nível de como Oracle Database@AWS e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para Oracle Database@AWS

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que podem ser anexados a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para Oracle Database@AWS

Para ver exemplos de políticas AWS baseadas em identidade do Oracle Database@, consulte. Políticas baseadas em identidade para o Oracle Database@AWS

Políticas baseadas em recursos dentro Oracle Database@AWS

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. É necessário especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações políticas para Oracle Database@AWS

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de Oracle Database@AWS ações, consulte Ações definidas pelo Oracle Database@AWS na Referência de Autorização de Serviço.

As ações de política Oracle Database@AWS usam o seguinte prefixo antes da ação:

```
odb
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

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

Para ver exemplos de políticas AWS baseadas em identidade do Oracle Database@, consulte. Políticas baseadas em identidade para o Oracle Database@AWS

Recursos políticos para Oracle Database@AWS

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de Oracle Database@AWS recursos e seus ARNs, consulte Recursos definidos pelo Oracle Database@AWS na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo Oracle Database@.AWS

Para ver exemplos de políticas AWS baseadas em identidade do Oracle Database@, consulte. Políticas baseadas em identidade para o Oracle Database@AWS

Chaves de condição de política para Oracle Database@AWS

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista de chaves de Oracle Database@AWS condição, consulte Chaves de condição para Oracle Database@AWS na Referência de Autorização de Serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo Oracle Database@AWS.

Para ver exemplos de políticas AWS baseadas em identidade do Oracle Database@, consulte. Políticas baseadas em identidade para o Oracle Database@AWS

ACLs in Oracle Database@AWS

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com Oracle Database@AWS

Compatível com ABAC (tags em políticas): parcial

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos chamados de tags. Você pode anexar tags a entidades e AWS recursos do IAM e, em seguida, criar políticas ABAC para permitir operações quando a tag do diretor corresponder à tag no recurso.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para saber mais sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com Oracle Database@AWS

Compatível com credenciais temporárias: sim

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para ter mais informações, consulte Credenciais de segurança temporárias no IAM e Serviços da Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Permissões principais entre serviços para Oracle Database@AWS

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS serviço, combinadas com o AWS serviço solicitante para fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhamento de sessões de acesso.

Funções de serviço para Oracle Database@AWS

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar uma função para delegar permissões a um AWS serviço no Guia do usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper Oracle Database@AWS a funcionalidade. Edite as funções de serviço somente quando Oracle Database@AWS fornecer orientação para fazer isso.

Funções vinculadas a serviços para Oracle Database@AWS

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS serviço. O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções Oracle Database@AWS vinculadas a serviços, consulte. Usando funções vinculadas a serviços para Oracle Database@AWS

Políticas baseadas em identidade para o Oracle Database@AWS

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Oracle Database@AWS . Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo Oracle Database@AWS, incluindo o formato do ARNs para cada um dos tipos de recursos, consulte Ações, Recursos e Chaves de Condição do Oracle Database@AWS na Referência de Autorização de Serviço.

Tópicos

- Práticas recomendadas de política
- Usar o console do Oracle Database@AWS

- Permita que os usuários provisionem Oracle Database@AWS recursos
- Permitir que os usuários visualizem suas próprias permissões

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir AWS recursos do Oracle Database@ em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para saber mais, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de um AWS serviço específico, como CloudFormation. Para saber mais, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando

as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para saber mais, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para saber mais sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usar o console do Oracle Database@AWS

Para acessar o AWS console do Oracle Database@, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os AWS recursos do Oracle Database@ em seu. Conta da AWS Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Permita que os usuários provisionem Oracle Database@AWS recursos

Essa política permite que os usuários tenham acesso total aos Oracle Database@AWS recursos de provisionamento. Para configurar a resolução de DNS da sua VPC, crie um resolvedor de saída do Route 53 e adicione regras para encaminhar o tráfego DNS com o nome de domínio OCI para o IP do ouvinte DNS da 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": "*"
        }
    ]
}
```

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou 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 políticas gerenciadas para Oracle Database@AWS

Para adicionar permissões a conjuntos de permissões e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

Serviços da AWS manter e atualizar políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Ocasionalmente, os serviços adicionam permissões adicionais a uma política AWS gerenciada para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (conjuntos de permissões e perfis) às quais a política está anexada. É mais provável que os serviços atualizem uma política AWS gerenciada quando um novo recurso é lançado ou quando novas operações são disponibilizadas. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violam suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política `ReadOnlyAccess` AWS gerenciada fornece acesso somente de leitura a todos Serviços da AWS os recursos. Quando um serviço lança um novo recurso, AWS

adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de perfis de trabalho, consulte Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.

Tópicos

- AWS política gerenciada: Amazon ODBService RolePolicy

AWS política gerenciada: Amazon ODBService RolePolicy

Não é possível anexar a política `AmazonODBServiceRolePolicy` às suas entidades do IAM. Essa política está vinculada a uma função vinculada ao serviço que permite Oracle Database@AWS realizar ações em seu nome. Para obter mais informações, consulte Usando funções vinculadas a serviços para Oracle Database@AWS.

Para ver mais detalhes sobre a política, incluindo a versão mais recente do documento de política JSON, consulte Amazon ODBService RolePolicy no Guia de referência de políticas AWS gerenciadas.

Oracle Database@AWS autenticação e autorização no OCI

Quando você usa AWS APIs para criar recursos para Oracle Database@AWS, esses recursos residem logicamente em sua locação vinculada do Oracle Cloud Infrastructure (OCI). Para implantar esses recursos, AWS comunique-se com a OCI APIs em seu nome. Para mitigar o confuso problema do deputado, Oracle Database@AWS use o OCI AWS STS como uma entidade confiável e encaminhe sessões de acesso para autorizar sua intenção de usar o OCI APIs em sua locação vinculada. Consequentemente, os eventos são registrados para a `sts:getCallerIdentity` API a partir do espaço IP da OCI em suas AWS CloudTrail trilhas e histórico de eventos. Espere esses eventos ao usar Oracle Database@AWS APIs.

Solução de problemas Oracle Database@AWS de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Oracle Database@AWS e o IAM.

Tópicos

- Não estou autorizado a realizar uma ação em Oracle Database@AWS
- Não estou autorizado a realizar iam: PassRole

- Quero permitir que pessoas fora da minha Conta da AWS acessem meus Oracle Database@AWS recursos

Não estou autorizado a realizar uma ação em Oracle Database@AWS

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `odb:`*`GetWidget`* fictícias.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `odb:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o Oracle Database@AWS.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no Oracle Database@AWS. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha Conta da AWS acessem meus Oracle Database@AWS recursos

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Oracle Database@AWS oferece suporte a esses recursos, consulte. Como Oracle Database@AWS funciona com o IAM
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Validação de conformidade para Oracle Database@AWS

Sua responsabilidade de conformidade ao usar o Oracle Database@AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade da sua empresa e pelas leis e regulamentações aplicáveis. A documentação da Oracle sobre conformidade na nuvem está disponível no site da Oracle

Resiliência em Oracle Database@AWS

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, o Oracle Database@AWS oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Usando funções vinculadas a serviços para Oracle Database@AWS

Oracle Database@AWS usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. Oracle Database@AWS As funções vinculadas ao serviço são predefinidas Oracle Database@AWS e incluem todas as permissões que o serviço exige para ligar para outras pessoas Serviços da AWS em seu nome.

Uma função vinculada ao serviço Oracle Database@AWS facilita o uso porque você não precisa adicionar manualmente as permissões necessárias. Oracle Database@AWS define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só Oracle Database@AWS pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Você pode excluir os perfis somente depois de primeiro excluir seus recursos relacionados. Isso protege seus Oracle Database@AWS recursos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Permissões de função vinculadas ao serviço para Oracle Database@AWS

Oracle Database@AWS usa a função vinculada ao serviço chamada AWSService RoleFor ODB Oracle Database@AWS para permitir chamadas Serviços da AWS em nome de seus recursos.

A função vinculada ao serviço AWSService RoleFor ODB confia nos seguintes serviços para assumir a função:

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

Essa função vinculada a serviços tem uma política de permissões anexada a ela, chamada `AmazonODBServiceRolePolicy`, que concede permissões para operar na conta. Para obter mais informações, consulte AWS política gerenciada: Amazon ODBService RolePolicy.

Note

É necessário configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Se encontrar a seguinte mensagem de erro:
Impossível criar o recurso. Verifique se você tem permissão para criar uma função vinculada ao serviço. Caso contrário, aguarde e tente novamente mais tarde.
Certifique-se de que você tem as seguintes permissões ativadas:

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

Para ter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

Criação de uma função vinculada ao serviço para Oracle Database@AWS

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria um banco de dados Exadata, Oracle Database@AWS cria a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria um banco de dados Exadata, Oracle Database@AWS cria a função vinculada ao serviço para você novamente.

Editando uma função vinculada ao serviço para Oracle Database@AWS

Oracle Database@AWS não permite que você edite a função vinculada ao serviço AWSService RoleFor ODB. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, você pode editar a descrição da função usando o IAM. Para obter mais informações, consulte Edição de uma função vinculada ao serviço no Guia do usuário do IAM.

Excluindo uma função vinculada ao serviço para Oracle Database@AWS

Se você não precisar mais usar um atributo ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não terá uma entidade não utilizada que não seja ativamente monitorada ou mantida. No entanto, você deve excluir todos os seus recursos antes de excluir a função vinculada ao serviço.

Limpando uma função vinculada a serviços para Oracle Database@AWS

Antes de você poder usar o IAM para excluir uma função vinculada ao serviço, você deve primeiro confirmar que a função não tem sessões ativas e remover quaisquer recursos usados pela função.

Para verificar se a função vinculada ao serviço tem uma sessão ativa no console do IAM

1. Faça login no Console de gerenciamento da AWS e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do console do IAM, escolha Perfis. Em seguida, escolha o nome (não a caixa de seleção) da função AWSService RoleFor ODB.
3. Na página Summary Resumo) do perfil escolhido, escolha a guia Access Advisor (Consultor de acesso).
4. Na guia Consultor de Acesso, revise a atividade recente para a função vinculada ao serviço.

> **Note**
>
> Se você não tiver certeza se Oracle Database@AWS está usando a função AWSService RoleFor ODB, tente excluir a função. Se o serviço estiver usando a função, a exclusão falhará e você poderá ver Regiões da AWS onde a função está sendo usada. Se a função está sendo usada, você deve aguardar a sessão final antes de excluir a função. Não é possível revogar a sessão de uma função vinculada a um serviço.

Se quiser remover a função AWSService RoleFor ODB, você deve primeiro excluir todos os seus Oracle Database@AWS recursos.

Regiões suportadas para funções vinculadas a Oracle Database@AWS serviços

Oracle Database@AWS suporta o uso de funções vinculadas ao serviço em todos os lugares em Regiões da AWS que o serviço está disponível. Para obter mais informações, consulte Regiões da AWS e endpoints.

Oracle Database@AWS atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas Oracle Database@AWS desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do Oracle Database@AWS documento.

Alteração	Descrição	Data
Permissões de função vinculadas ao serviço para Oracle Database@AWS: atualizar para uma política existente.	Oracle Database@AWS adicionou novas permissões à função `AmazonODBServiceRolePolicy` `AWSServiceRoleForODB` vinculada ao serviço. Essas permissões permitem Oracle Database@AWS fazer o seguinte:	30 de junho de 2025

Alteração	Descrição	Data
	• Descreva os anexos do Amazon VPC Transit Gateways • Descreva os EC2 anexos da Amazon • Ativar uma EventBridge fonte da Amazon Para obter mais informações, consulte Permissões de função vinculadas ao serviço para Oracle Database@AWS.	
Permissões de função vinculadas ao serviço para Oracle Database@AWS: atualizar para uma política existente.	Oracle Database@AWS adicionou novas permissões à função `AmazonODBServiceRolePolicy` `AWSServiceRoleForODB` vinculada ao serviço. Essas permissões permitem Oracle Database@AWS fazer o seguinte: • Descreva uma EventBridge fonte da Amazon • Descreva e crie um ônibus de eventos Para obter mais informações, consulte Permissões de função vinculadas ao serviço para Oracle Database@AWS.	26 de junho de 2025
AWS política gerenciada: Amazon ODBService RolePolicy— Nova política de funções vinculadas a serviços	Oracle Database@AWS adicionou o `AmazonODB ServiceRolePolicy` para a função `AWSServiceRoleForODB` vinculada ao serviço. Para obter mais informações, consulte AWS política gerenciada: Amazon ODBService RolePolicy.	2 de dezembro de 2024
Oracle Database@AWS começou a rastrear alterações	Oracle Database@AWS começou a rastrear as mudanças em suas políticas AWS gerenciadas.	2 de dezembro de 2024

Monitorando o Oracle Database@AWS

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de Oracle Database@AWS suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para observar Oracle Database@AWS, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. Você pode coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas de suas EC2 instâncias da Amazon e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.
- O Amazon CloudWatch Logs permite que você monitore, armazene e acesse seus arquivos de log de EC2 instâncias da Amazon e de outras fontes. CloudTrail CloudWatch Os registros podem monitorar as informações nos arquivos de log e notificá-lo quando determinados limites forem atingidos. É possível também arquivar seus dados de log em armazenamento resiliente. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch Logs.
- A Amazon EventBridge pode ser usada para automatizar seus AWS serviços e responder automaticamente a eventos do sistema, como problemas de disponibilidade de aplicativos ou alterações de recursos. Os eventos dos AWS serviços são entregues quase EventBridge em tempo real. Você pode escrever regras simples para determinar quais eventos são do seu interesse, e as ações automatizadas a serem tomadas quando um evento corresponder à regra. Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.
- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o Guia do usuário do AWS CloudTrail.

Monitoramento Oracle Database@AWS com a Amazon CloudWatch

Você pode monitorar Oracle Database@AWS o uso CloudWatch, que coleta dados brutos e os processa em métricas legíveis e quase em tempo real. Essas estatísticas são mantidas por 15

meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como o aplicativo web ou o serviço está se saindo. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

CloudWatch Métricas da Amazon para Oracle Database@AWS

O Oracle Database@AWS serviço reporta métricas para a Amazon CloudWatch no `AWS/ODB` namespace para clusters de VM, bancos de dados de contêineres e bancos de dados conectáveis.

Tópicos

Métricas para clusters de VM na nuvem

O Oracle Database@AWS serviço relata as seguintes métricas no `AWS/ODB` namespace para clusters de VM na nuvem.

Métrica	Description	Unidades
`ASMDiskgroupUtilization`	A porcentagem de espaço utilizável usado em um grupo de discos. Espaço utilizável é o espaço disponível para crescimento. O grupo de discos DATA armazena nossos arquivos de banco de dados Oracle. O grupo de discos RECO contém arquivos de banco de dados para recuperação, como arquivos e registros de flashback.	Porcentagem
`CpuUtilization`	A porcentagem de utilização da CPU.	Porcentagem

Métrica	Description	Unidades
`FilesystemUtilization`	A porcentagem de utilização do sistema de arquivos provisionado.	Porcentagem
`LoadAverage`	A média de carga do sistema é de mais de 5 minutos.	Inteiro
`MemoryUtilization`	A porcentagem de memória disponível para iniciar novos aplicativos, sem troca. A memória disponível pode ser obtida por meio do seguinte comando: `cat /proc/meminfo`	Porcentagem
`NodeStatus`	Indica se o host está acessível.	Inteiro
`OcpusAllocated`	O número de OCPUs alocados.	Inteiro
`SwapUtilization`	A porcentagem de utilização do espaço total de swap.	Porcentagem

Métricas para bancos de dados de contêiner

O Oracle Database@AWS serviço relata as seguintes métricas no `AWS/ODB` namespace para bancos de dados de contêineres.

Métrica	Description	Unidades
`BlockChanges`	O número médio de blocos alterados por segundo.	Mudanças por segundo
`CpuUtilization`	A utilização da CPU expressa como uma porcentagem,	Porcentagem

Métrica	Description	Unidades
	agregada em todos os grupos de consumidores. A porcentagem de utilização é relatada com relação ao número CPUs do banco de dados que pode ser usado, que é duas vezes o número de OCPUs.	
`CurrentLogons`	O número de logons bem-sucedidos durante o intervalo selecionado.	Contagem
`ExecuteCount`	O número de chamadas recursivas e de usuário que executaram instruções SQL durante o intervalo selecionado.	Contagem
`ParseCount`	O número de análises rígidas e flexíveis durante o intervalo selecionado.	Contagem
`StorageAllocated`	Quantidade total de espaço de armazenamento alocado ao banco de dados no momento da coleta.	GB
`StorageAllocatedByTablespace`	Quantidade total de espaço de armazenamento alocado ao espaço de tabela no momento da coleta. No caso do banco de dados de contêiner, essa métrica fornece espaços de tabela do contêiner raiz.	GB

Métrica	Description	Unidades
`StorageUsed`	Quantidade total de espaço de armazenamento usado pelo banco de dados no momento da coleta.	GB
`StorageUsedByTablespace`	Quantidade total de espaço de armazenamento usado pelo tablespace no momento da coleta. No caso do banco de dados de contêiner, essa métrica fornece espaços de tabela do contêiner raiz.	GB
`StorageUtilization`	A porcentagem da capacidade de armazenamento provisionada atualmente em uso. Representa o espaço total alocado para todos os espaços de tabela.	Porcentagem
`StorageUtilizationByTablespace`	Isso indica a porcentagem de espaço de armazenamento utilizado pelo espaço de tabela no momento da coleta. No caso do banco de dados de contêiner, essa métrica fornece espaços de tabela do contêiner raiz.	Porcentagem
`TransactionCount`	O número combinado de confirmações e reversões de usuários durante o intervalo selecionado.	Contagem

Métrica	Description	Unidades
`UserCalls`	O número combinado de logons, análises e chamadas de execução durante o intervalo selecionado.	Contagem

Métricas para bancos de dados conectáveis

O Oracle Database@AWS serviço relata as seguintes métricas no `AWS/ODB` namespace para bancos de dados conectáveis.

Métrica	Description	Unidades
`AllocatedStorageUtilizationByTablespace`	A porcentagem de espaço usada pelo tablespace, de todo o espaço alocado. Para bancos de dados de contêineres, essa métrica fornece dados para espaços de tabela de contêineres raiz. (Estatística: média, intervalo: 30 minutos)	Percentual
`AvgGCCRBlockReceiveTime`	O tempo médio de recebimento do bloco CR (leitura consistente) do cache global. Somente para bancos de dados RAC/cluster. (Estatística: média, intervalo: 5 minutos)	Milissegundos
`AvgGCCurrentBlockReceiveTime`	O tempo médio de recebimento dos blocos atuais do cache global. A estatística relata o valor médio. Somente para bancos de dados do Real	Milissegundos

Métrica	Description	Unidades
	Application Cluster (RAC). (Estatística: média, intervalo: 5 minutos)	
`BlockChanges`	O número médio de blocos alterados por segundo. (Estatística: média, intervalo: 1 minuto)	mudanças por segundo
`BlockingSessions`	Sessões de bloqueio atuais. Não aplicável para bancos de dados de contêineres. (Estatística: Máximo, Intervalo : 15 minutos)	Contagem
`CPUTimeSeconds`	A taxa média de acúmulo de tempo de CPU por sessões em primeiro plano na instância do banco de dados durante o intervalo de tempo. O componente de tempo de CPU da média de sessões ativas. (Estatística: média, intervalo: 1 minuto)	Segundos por segundo
`CpuCount`	O número de CPUs durante o intervalo selecionado.	Contagem

Métrica	Description	Unidades
`CpuUtilization`	A utilização da CPU expressa como uma porcentagem, agregada em todos os grupos de consumidores. A porcentagem de utilização é relatada com relação ao número CPUs do banco de dados que pode ser usado, que é duas vezes o número de OCPUs. (Estatística: média, intervalo: 1 minuto)	Percentual
`CurrentLogons`	O número de logons bem-sucedidos durante o intervalo selecionado. (Estatísticas: soma, intervalo: 1 minuto)	Contagem
`DBTimeSeconds`	A taxa média de acúmulo de tempo do banco de dados (CPU + Espera) por sessões em primeiro plano na instância do banco de dados durante o intervalo de tempo. Também conhecida como média de sessões ativas. (Estatística: média, intervalo: 1 minuto)	Segundos por segundo

Métrica	Description	Unidades
`DbmgmtJobExecutionsCount`	O número de execuções de tarefas SQL em um único banco de dados gerenciado ou em um grupo de bancos de dados e seu status. As dimensões de status podem ser os seguintes valores: “Suceeded”, “Failed”, "InProgress.” (Estatística: soma, intervalo: 1 minuto)	Contagem
`ExecuteCount`	O número de chamadas recursivas e de usuário que executaram instruções SQL durante o intervalo selecionado. (Estatística: soma, intervalo: 1 minuto)	Contagem
`FRASpaceLimit`	O limite de espaço da área de recuperação flash. Não aplicável para bancos de dados conectáveis. (Estatística: Máximo, Intervalo: 15 minutos)	GB
`FRAUtilization`	A utilização da área de recuperação flash. Não aplicável para bancos de dados conectáveis. (Estatística: média, intervalo: 15 minutos)	Percentual

Métrica	Description	Unidades
GCCRBlocksReceived	Os blocos CR (leitura consistente) do cache global recebidos por segundo. Somente para bancos de dados RAC/cluster. (Estatística: média, intervalo: 5 minutos)	Blocos por segundo
GCCurrentBlocksReceived	Representa os blocos atuais do cache global recebidos por segundo. A estatística relata o valor médio. Somente para bancos de dados do Real Application Cluster (RAC). (Estatística: média, intervalo: 5 minutos)	Blocos por segundo
IOPS	O número médio de operações de entrada e saída por segundo. (Estatística: média, intervalo: 1 minuto)	Operações por segundo
IOThroughputMB	A taxa de transferência média em MB por segundo. (Estatística: média, intervalo: 1 minuto)	MB por segundo
InterconnectTrafficMB	A taxa média de transferência de dados do internódio. Somente para bancos de dados RAC/cluster. (Estatística: média, intervalo: 5 minutos)	MB por segundo

Métrica	Description	Unidades
`InvalidObjects`	Contagem inválida de objetos do banco de dados. Não aplicável para bancos de dados de contêineres. (Estatística: Máximo, Intervalo : 24 horas)	Contagem
`LogicalBlocksRead`	O número médio de blocos lidos SGA/Memory (cache de buffer) por segundo. (Estatíst ica: média, intervalo: 1 minuto)	Leituras por segundo
`MaxTablespaceSize`	O tamanho máximo possível do espaço de tabela. Para bancos de dados de contêiner es, essa métrica fornece dados para espaços de tabela de contêineres raiz. (Estatíst ica: Máximo, Intervalo: 30 minutos)	GB
`MemoryUsage`	Tamanho total do pool de memória em MB. (Estatística: média, intervalo: 15 minutos)	MB
`MonitoringStatus`	O status de monitoramento do recurso. Se uma coleta de métricas falhar, as informaçõ es de erro serão capturada s nessa métrica. (Estatística: média, intervalo: 5 minutos)	Não aplicável

Métrica	Description	Unidades
`NonReclaimableFRA`	A área de recuperação rápida não recuperável. Não aplicável para bancos de dados conectáveis. (Estatística: média, intervalo: 15 minutos)	Percentual
`OcpusAllocated`	O número real de OCPUs alocados pelo serviço durante o intervalo de tempo selecionado. (Estatística: contagem, intervalo: 1 minuto)	Inteiro
`ParseCount`	O número de análises rígidas e flexíveis durante o intervalo selecionado. (Estatística: soma, intervalo: 1 minuto)	Contagem
`ParsesByType`	O número de análises físicas ou flexíveis por segundo. (Estatística: média, intervalo: 1 minuto)	Análises por segundo
`ProblematicScheduledDBMSJobs`	Os trabalhos problemáticos agendados do banco de dados contam. Não aplicável para bancos de dados de contêineres. (Estatística: Máximo, Intervalo: 15 minutos)	Contagem
`ProcessLimitUtilization`	O limite de utilização do processo. Não aplicável para bancos de dados conectáveis. (Estatística: média, intervalo: 1 minuto)	Percentual

Métrica	Description	Unidades
`Processes`	Os processos do banco de dados contam. Não aplicável para bancos de dados conectáveis. (Estatística: Máximo, Intervalo: 1 minuto)	Contagem
`ReclaimableFRA`	A área de recuperação rápida recuperável. Não aplicável para bancos de dados conectáveis. (Estatística: média, intervalo: 15 minutos)	Percentual
`ReclaimableFRASpace`	O espaço recuperável da área de recuperação flash. Não aplicável para bancos de dados conectáveis. (Estatíst ica: média, intervalo: 15 minutos)	GB
`RedoSizeMB`	A quantidade média de redo gerada, em MB por segundo. (Estatística: média, intervalo: 1 minuto)	MB por segundo
`SessionLimitUtiliz ation`	A utilização do limite de sessão. Não aplicável para bancos de dados conectáveis. (Estatística: média, intervalo: 1 minuto)	Percentual
`Sessions`	O número de sessões no banco de dados. (Estatística: média, intervalo: 1 minuto)	Contagem

Métrica	Description	Unidades
`StorageAllocated`	A quantidade máxima de espaço alocada por espaço de tabela durante o intervalo . Para bancos de dados de contêineres, essa métrica fornece dados para espaços de tabela de contêineres raiz. (Estatística: Máximo, Intervalo : 30 minutos)	GB
`StorageAllocatedBy Tablespace`	A quantidade máxima de espaço alocada por espaço de tabela durante o intervalo . Para bancos de dados de contêineres, essa métrica fornece dados para espaços de tabela de contêineres raiz. (Estatística: Máximo, Intervalo : 30 minutos)	GB
`StorageUsed`	A quantidade máxima de espaço usada durante o intervalo. (Estatística: Máximo, Intervalo: 30 minutos)	GB
`StorageUsedByTable space`	A quantidade máxima de espaço usada pelo espaço de tabela durante o intervalo . Para bancos de dados de contêineres, essa métrica fornece dados para espaços de tabela de contêineres raiz. (Estatística: Máximo, Intervalo : 30 minutos)	GB

Métrica	Description	Unidades
`StorageUtilization`	A porcentagem da capacidade de armazenamento provisionada atualmente em uso. Representa o espaço total alocado para todos os espaços de tabela. (Estatística: média, intervalo: 30 minutos)	Percentual
`StorageUtilizationByTablespace`	A porcentagem do espaço utilizado, por espaço de tabela. Para bancos de dados de contêineres, essa métrica fornece dados para espaços de tabela de contêineres raiz. (Estatística: média, intervalo: 30 minutos)	Percentual
`TransactionCount`	O número combinado de confirmações e reversões de usuários durante o intervalo selecionado. (Estatística: soma, intervalo: 1 minuto)	Contagem
`TransactionsByStatus`	O número de transações confirmadas ou revertidas por segundo. (Estatística: média, intervalo: 1 minuto)	Transações por segundo
`UnusableIndexes`	Índices inutilizáveis contam no esquema do banco de dados. Não aplicável para bancos de dados de contêineres. (Estatística: Máximo, Intervalo: 24 horas)	Contagem

Métrica	Description	Unidades
`UsableFRA`	A área de recuperação rápida utilizável. Não aplicável para bancos de dados conectáveis. (Estatística: média, intervalo: 15 minutos)	Percentual
`UsedFRASpace`	O uso do espaço da área de recuperação flash. Não aplicável para bancos de dados conectáveis. (Estatística: Máximo, Intervalo: 15 minutos)	GB
`UserCalls`	O número combinado de logons, análises e chamadas de execução durante o intervalo selecionado. (Estatística: soma, intervalo: 1 minuto)	Contagem
`WaitTimeSeconds`	A taxa média de acúmulo de tempo de espera não ocioso por sessões em primeiro plano na instância do banco de dados durante o intervalo de tempo. O componente de tempo de espera da média de sessões ativas. (Estatística: média, intervalo: 5 minutos)	Segundos por segundo

CloudWatch Dimensões da Amazon para Oracle Database@AWS

Você pode filtrar dados de Oracle Database@AWS métricas usando qualquer dimensão na tabela a seguir.

Dimensão	Filtra os dados solicitados para . . .
`cloudVmClusterId`	O identificador de um cluster de VM.
`cloudExadataInfrastructureId`	O identificador da infraestrutura do Exadata.
`collectionName`	O nome de uma coleção.
`deploymentType`	O tipo de infraestrutura.
`diskgroupName`	Um nome de um grupo de discos
`errorCode`	Um código do erro.
`errorSeverity`	A gravidade de um erro.
`filesystemName`	O nome de um sistema de arquivos.
`hostName`	O nome da máquina host.
`instanceName`	O nome de uma instância de banco de dados.
`instanceNumber`	O número da instância de uma instância de banco de dados.
`ioType`	Um tipo de I/O operação.
`jobId`	Um identificador exclusivo para um trabalho.
`managedDatabaseGroupId`	O identificador de umManaged Database Group.
`managedDatabaseId`	O identificador de umManaged Database.
`memoryPool`	Um tipo de pool de memória.
`memoryType`	Um tipo de memória.
`ociCloudVmClusterId`	O identificador OCI de um cluster de VM.

Dimensão	Filtra os dados solicitados para . . .
`ociCloudExadataInfrastructureId`	O identificador OCI da infraestrutura do Exadata.
`parseType`	Um tipo de análise.
`resourceId`	O identificador de um recurso.
`resourceId_Database`	O identificador de um banco de dados.
`resourceId_DbNode`	O identificador de um nó de banco de dados.
`resourceName`	O nome de um recurso do .
`resourceName_Database`	O nome de um banco de dados.
`resourceName_DbNode`	O nome de um nó de banco de dados.
`resourceType`	Um tipo de banco de dados.
`schemaName`	O nome de um esquema.
`status`	O status de um banco de dados.
`tablespaceContents`	O conteúdo de um espaço de tabela.
`tablespaceName`	O nome de um espaço de tabela.
`tablespaceType`	Um tipo de espaço de tabela.
`transactionStatus`	O status de uma transação.
`waitClass`	Um evento de classe de espera.

Monitoramento de Oracle Database@AWS eventos na Amazon EventBridge

Você pode monitorar Oracle Database@AWS eventos em EventBridge, o que fornece um fluxo de dados em tempo real de aplicativos e AWS serviços. EventBridge encaminha esses dados para destinos como o AWS Lambda Amazon Simple Notification Service.

> **Note**
>
> EventBridge era anteriormente chamado de Amazon CloudWatch Events. Para obter mais informações, consulte EventBridge a evolução dos CloudWatch Eventos da Amazon no Guia do EventBridge Usuário da Amazon.

Visão geral dos Oracle Database@AWS eventos

Oracle Database@AWS eventos são mensagens estruturadas que indicam mudanças nos ciclos de vida dos recursos. Um barramento de eventos é um roteador que recebe eventos e os entrega a zero ou mais destinos ou alvos. Oracle Database@AWS os eventos podem ser gerados a partir das seguintes fontes:

Eventos de AWS

Esses eventos são Oracle Database@AWS APIs gerados AWS paralelamente e entregues no ônibus de eventos padrão em seu Conta da AWS.

Eventos da OCI

Esses eventos são gerados diretamente do OCI, como eventos relacionados à infraestrutura do Oracle Exadata ou clusters de VM. Quando você se inscreve Oracle Database@AWS, um barramento de eventos com prefixo `aws.partner/odb/` é criado no seu Conta da AWS para receber eventos da OCI.

Oracle Database@AWS eventos de AWS

Oracle Database@AWS os eventos de AWS incluem mudanças no ciclo de vida relacionadas à rede ODB durante a criação e a exclusão. Esses eventos são entregues no ônibus de eventos padrão em seu Conta da AWS. O tipo de entrega é o melhor esforço.

Eventos de rede ODB

Event	ID do evento	Mensagem
Criação	ODB-EVENT-0001	Rede ODB criada com sucesso ODBnet_ID
Falha na criação	ODB-EVENT-0011	Falha ao criar a rede ODB ODBNet_ID
Exclusão	ODB-EVENT-0002	Rede ODB ODBnet_ID excluída com sucesso
Falha na exclusão	ODB-EVENT-0012	Falha ao excluir ODBNet_ID da rede ODB

Exemplo: evento de criação de rede ODB

O exemplo a seguir mostra um evento para a criação bem-sucedida de uma rede ODB.

```
{
  "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 eventos da OCI

A maioria dos eventos é gerada diretamente do OCI. Oracle Database@AWS cria um barramento de eventos com prefixo `aws.partner/odb/` em seu Conta da AWS para receber eventos da OCI. Recomendamos que você não exclua esse barramento de eventos.

A OCI fornece tipos de eventos abrangentes, incluindo os seguintes:

- Infraestrutura Oracle Exadata
- Eventos de cluster de VM
- Eventos CDB
- Eventos PDB

Para obter mais informações sobre os tipos de eventos específicos e os detalhes que a OCI suporta, consulte Oracle Exadata Database Service on Dedicated Infrastructure Events and Events for Autonomous Database on Dedicated Exadata Infrastructure.

Filtrando eventos Oracle Database@AWS

Você pode seguir as melhores práticas EventBridge sugeridas na configuração de ônibus de eventos em Ônibus de eventos na Amazon EventBridge. Dependendo dos seus casos de uso, você pode configurar EventBridge regras para filtrar eventos e destinos para receber e usar eventos.

Filtrando eventos de rede ODB de AWS

Para eventos de rede ODB de AWS, você pode filtrar usando o seguinte padrão de evento:

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

Você pode aplicar esse padrão usando a EventBridge `put-rule` API com o barramento de eventos padrão. Para obter mais informações, consulte PutRulea Amazon EventBridge API Reference.

Filtrando Oracle Database@AWS eventos do OCI

Para Oracle Database@AWS eventos da OCI, você pode configurar uma regra usando um comando semelhante ao exemplo PutRulena Amazon EventBridge API Reference. Observe as seguintes diretrizes:

- Use um padrão de evento personalizado, dependendo dos tipos de eventos que você deseja filtrar.
- EventBusNameDefina o nome do ônibus Oracle Database@AWS criado.

Para obter mais informações sobre como filtrar eventos e configurar EventBridge metas em várias contas, consulte Envio e recebimento de eventos entre Contas da AWS na Amazon EventBridge.

Oracle Database@AWS Eventos de solução de problemas

Se você encontrar um problema com a entrega ou o conteúdo do evento, faça o seguinte:

- Para eventos de rede ODB, entre em contato AWS Support.
- Para Oracle Database@AWS eventos que não sejam eventos de rede ODB, entre em contato com o Oracle Cloud Support.

Para obter mais informações, consulte Obtendo suporte para o Oracle Database@AWS.

Registrando chamadas de Oracle Database@AWS API usando AWS CloudTrail

Oracle Database@AWS é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou um AWS service (Serviço da AWS). CloudTrail captura todas as chamadas de API Oracle Database@AWS como eventos. As chamadas capturadas incluem chamadas do Oracle Database@AWS console e chamadas de código para as operações Oracle Database@AWS da API. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita Oracle Database@AWS, o endereço IP do qual a solicitação foi feita, quando foi feita e detalhes adicionais.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário raiz ou credenciais de usuário.
- Se a solicitação foi feita em nome de um usuário do Centro de Identidade do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

> **Note**
>
> Oracle Database@AWS registra chamadas de `GetCallerIdentity` API de AWS Security Token Service (STS) em seus CloudTrail registros. Essas chamadas da API STS verificam

a identidade da Oracle Database@AWS interação com a OCI em seu nome. Eles são uma parte normal e segura das AWS operações e não expõem informações confidenciais.

CloudTrail está ativo Conta da AWS quando você cria a conta e você tem acesso automático ao histórico de CloudTrail eventos. O histórico de CloudTrail eventos fornece um registro visível, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento registrados em um. Região da AWS Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos no Guia AWS CloudTrail do usuário. Não há CloudTrail cobrança pela visualização do histórico de eventos.

Para um registro contínuo dos eventos dos Conta da AWS últimos 90 dias, crie uma trilha ou um armazenamento de dados de eventos do CloudTrailLake.

CloudTrail trilhas

Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Todas as trilhas criadas usando o Console de gerenciamento da AWS são multirregionais. Só é possível criar uma trilha de região única ou de várias regiões usando a AWS CLI. É recomendável criar uma trilha multirregional porque você captura todas as atividades Regiões da AWS em sua conta. Ao criar uma trilha de região única, é possível visualizar somente os eventos registrados na Região da AWS da trilha. Para obter mais informações sobre trilhas, consulte Criar uma trilha para a Conta da AWS e Criar uma trilha para uma organização no Guia do usuário do AWS CloudTrail .

Você pode entregar uma cópia dos seus eventos de gerenciamento contínuos para o bucket do Amazon S3 sem nenhum custo CloudTrail criando uma trilha. No entanto, há cobranças de armazenamento do Amazon S3. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços. Para receber informações sobre a definição de preços do Amazon S3, consulte Definição de preços do Amazon S3.

CloudTrail Armazenamentos de dados de eventos em Lake

CloudTrail O Lake permite que você execute consultas baseadas em SQL em seus eventos. CloudTrail O Lake converte eventos existentes no formato JSON baseado em linhas para o formato Apache ORC. O ORC é um formato colunar de armazenamento otimizado para recuperação rápida de dados. Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos baseados nos critérios selecionados com a aplicação de seletores de eventos avançados. Os seletores que aplicados a um armazenamento de dados de eventos controlam quais eventos persistem e estão disponíveis para consulta. Para

obter mais informações sobre o CloudTrail Lake, consulte Trabalhando com o AWS CloudTrail Lake no Guia AWS CloudTrail do Usuário.

CloudTrail Os armazenamentos e consultas de dados de eventos em Lake incorrem em custos. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Oracle Database@AWS eventos de gerenciamento em CloudTrail

Os eventos de gerenciamento fornecem informações sobre as operações de gerenciamento que são realizadas nos recursos do seu Conta da AWS. Também são conhecidas como operações de ambiente de gerenciamento. Por padrão, CloudTrail registra eventos de gerenciamento.

Oracle Database@AWS registra todas as operações do plano de Oracle Database@AWS controle como eventos de gerenciamento.

Oracle Database@AWS exemplos de eventos

Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a operação de API solicitada, a data e a hora da operação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, os eventos não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra um CloudTrail evento que demonstra a `CreateOdbNetwork` operação.


```
{
    "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"
    }
}
```


Para obter informações sobre o conteúdo do CloudTrail registro, consulte o conteúdo do CloudTrail registro no Guia AWS CloudTrail do usuário.

Solução de problemas do Oracle Database@AWS

Use as seções a seguir para ajudar a solucionar problemas de rede que você possa encontrar. Oracle Database@AWS

Tópicos

Falha na criação da rede ODB

Quando você não consegue criar uma rede ODB, as seguintes são as causas comuns:

Intervalos de CIDR restritos

A rede ODB usa intervalos CIDR específicos para as sub-redes cliente e de backup. Certifique-se de que os intervalos CIDR que você escolheu para essas sub-redes não se sobreponham a nenhum intervalo de endereço IP restrito ou reservado.

Os seguintes intervalos CIDR são reservados e não podem ser usados para a rede ODB:

- Intervalo reservado da nuvem Oracle: 169.254.0.0/16
- Classe reservada D: 224.0.0.0 - 239.255.255.255
- Classe reservada E: 240.0.0.0 - 255.255.255.255
- Uso futuro do OCI: 100.105.0.0/16

Siga as EC2 regras para intervalos de CIDR, conforme descrito na documentação da VPC. Para saber mais, consulte Restrições de associação de blocos CIDR.

Além disso, evite a sobreposição entre intervalos CIDR especificados e aqueles usados para conectividade VPC com a rede ODB.

CIDR VPC sobreposto

O intervalo CIDR que você especificou para a rede ODB não deve se sobrepor aos intervalos CIDR usados por nenhum dos seus existentes. VPCs A sobreposição de intervalos CIDR pode causar conflitos de roteamento e impedir a criação bem-sucedida da rede ODB. Verifique os

intervalos CIDR do emparelhamento de ODB VPCs e certifique-se de que o CIDR da rede ODB seja exclusivo e não se sobreponha.

Propriedade de VPCs

A rede ODB e a VPC à qual você está se conectando devem pertencer à mesma conta. AWS Se você estiver tentando emparelhar a rede ODB para uma VPC pertencente a uma conta diferente, a criação falhará. Verifique se a rede ODB e a VPC pertencem à mesma conta. AWS

Falta de um gateway de trânsito

Se você adicionar um intervalo CIDR à lista CIDR emparelhada da rede ODB sem anexar um gateway de trânsito à VPC, a operação de criação ou atualização falhará. Não há nenhuma exigência sobre os intervalos CIDR para os quais o anexo é usado.

Problemas de conectividade entre sua rede VPC e ODB ou clusters de VM

Quando você não consegue se conectar da sua VPC à rede ODB ou aos clusters de VM dentro dela, as seguintes são as causas comuns:

- Verificando a configuração da VPC — No console, localize Oracle Database@AWS a VPC que está emparelhada com a rede ODB. Confirme se o ID da VPC corresponde ao mostrado nos detalhes da rede ODB.
- Inspecionando tabelas de rotas — No console da Amazon VPC, encontre a tabela de rotas anexada à sub-rede em que seu aplicativo está sendo executado. Verifique se há uma rota com um CIDR de destino que corresponda ao CIDR da sub-rede do cliente da rede ODB. Confirme se essa rota aponta para o ARN correto da rede ODB. Se a rota estiver ausente, adicione uma nova ao CIDR da sub-rede cliente da rede ODB.
- Validando o peering CIDRs — revise a `Peered CIDRs` seção nos detalhes da rede ODB. Confirme se todos os blocos CIDR relevantes da sua VPC estão listados. Se um CIDR necessário estiver ausente, atualize o CIDRs emparelhado.
- Verificando as regras do grupo de segurança — No EC2 console da Amazon, localize os grupos de segurança para recursos em sua VPC. Revise as regras de entrada e saída, atualizando-as conforme necessário para permitir o tráfego necessário.
- Confirmação de zonas de disponibilidade — No console da Amazon VPC, identifique a zona de disponibilidade (AZ) da sua sub-rede. Verifique se a rede ODB também está implantada na mesma AZ da sua sub-rede.

- Evitar várias conexões de emparelhamento de rede ODB — Verifique suas conexões de emparelhamento de VPC no console. Oracle Database@AWS Verifique se você tem somente uma conexão ativa com uma rede ODB. Se você ver mais de um peering de rede ODB, remova os extras.

Nomes de host ou nomes de digitalização não resolvidos de clusters de VM da VPC

Se os nomes de host ou os nomes de digitalização dos clusters de VM não puderem ser resolvidos na sua VPC, configure o encaminhamento de DNS na VPC e os seguintes recursos para resolver registros DNS hospedados na rede ODB:

- Um endpoint de saída para enviar consultas de DNS para a rede ODB. Para obter mais informações, consulte Configurando um endpoint de saída em uma rede ODB no Oracle Database@AWS.
- Uma regra de resolução para especificar o nome de domínio das consultas DNS que o resolvedor encaminha para a rede DNS for ODB. Para obter mais informações, consulte Configurando uma regra de resolução em Oracle Database@AWS.

Obtendo suporte para o Oracle Database@AWS

Saiba como obter informações e suporte para o Oracle Database@AWS.

Escopo de suporte e informações de contato da Oracle

O Oracle Cloud Support é a primeira linha de suporte para todas as perguntas do Oracle Database@AWS . Para entrar em contato com o suporte, faça login no console do Oracle Cloud Infrastructure (OCI) e selecione o ícone do bote salva-vidas. Se você não tiver uma conta do My Oracle Cloud Support, consulteMinhas contas e acesso ao Oracle Cloud Support.

Exemplos de problemas com os quais o Oracle Support pode ajudá-lo incluem o seguinte:

- Problemas de conexão com o banco de dados (Oracle TNS)
- Problemas de desempenho do banco de dados Oracle
- Resolução de erros do banco de dados Oracle
- Problemas de rede relacionados às comunicações com a locação da OCI associada ao serviço

- A cota (limites) aumenta para receber mais capacidade (para obter mais informações, consulte Solicitando um aumento de limite para recursos de banco de dados)
- Dimensionamento para adicionar mais capacidade de computação e armazenamento à sua infraestrutura de banco de dados Oracle
- Atualizações de hardware de nova geração
- Problemas de cobrança relacionados às suas AWS Marketplace cobranças

Se você precisar entrar em contato com o Suporte da Oracle fora do Console OCI, informe ao seu agente do Oracle Support que seu problema está relacionado ao Oracle AWS Database@. Isso ocorre porque as solicitações desse serviço são tratadas por uma equipe de suporte da OCI especializada nessas implantações.

Entrando em contato com o suporte da Oracle por telefone

1. Ligue para 1-800-223-1711. Se você estiver fora dos Estados Unidos da América, visite o Diretório Global de Contatos de Suporte da Oracle para encontrar informações de contato do seu país ou região.
2. Escolha a opção “2" para abrir uma nova Solicitação de Serviço (SR).
3. Escolha a opção “4" para “inseguro”.
4. Informe ao agente que você tem um problema com seu sistema multicloud e o nome do produto. Uma solicitação de serviço interna será aberta em seu nome e um engenheiro de suporte da OCI entrará em contato diretamente com você.

Você também pode enviar uma pergunta para o fórum Multicloud na comunidade Cloud Customer Connect da Oracle. Essa opção está disponível para todos os clientes.

Minhas contas e acesso ao Oracle Cloud Support

Para criar tíquetes de solicitação de serviço do My Oracle Cloud Support, o administrador do AWS serviço Oracle Database@ da sua organização deve aprovar sua solicitação. Se você for o AWS administrador do Oracle Database@, conclua as instruções de integração do My Oracle Cloud Support incluídas no e-mail de ativação do serviço Oracle AWS Database@.

Você pode encontrar instruções para integração com o My Oracle Cloud Support nos seguintes tópicos:

- Configurando sua conta de suporte da Oracle

- Criando uma solicitação de suporte

Para obter instruções sobre como aprovar usuários para abrir solicitações de suporte do My Oracle Cloud Support, consulte Administrator Tasks for Support.

AWS Support escopo e informações de contato

AWS Support é sua primeira linha de suporte para todos os problemas e dúvidas AWS relacionados. Crie um AWS Support caso para seu problema, como você faz com outros AWS serviços. A AWS Support equipe colabora com o OCI Support conforme necessário.

Exemplos de AWS problemas do Oracle Database@ que AWS Support podem ajudá-lo incluem o seguinte:

- Problemas de rede virtual, incluindo aqueles que envolvem tradução de endereços de rede (NAT), firewalls, gerenciamento de tráfego e DNS e sub-redes AWS
- Problemas do Bastion e da máquina virtual (VM), incluindo conexão com o host do banco de dados, instalação de software, latência e desempenho do host
- Relatórios de métricas de cluster de VM do Exadata na Amazon CloudWatch
- Problemas de cobrança relacionados aos serviços AWS

Para obter informações sobre AWS Support, consulte Introdução ao AWS Support.

Acordos de nível de serviço da Oracle

Se você tiver dúvidas sobre o Oracle Database@AWS Service Level Agreements (SLAs) ou quiser solicitar créditos de serviço para violações de SLA, entre em contato com o gerente de contas da Oracle. Consulte Contratos de nível de serviço para obter mais informações.

Cotas para Oracle Database@AWS

Oracle Database@AWS é uma oferta multicloud. AWS não define nem impõe cotas para Oracle Database@AWS recursos. As cotas são aplicadas pela Oracle Cloud Infrastructure (OCI). Para obter mais informações sobre cotas de OCI, consulte Cotas e limites de serviço na documentação do Oracle Cloud Infrastructure.

Histórico de documentos para o Guia Oracle Database@AWS do usuário

A tabela a seguir descreve as versões de documentação do Oracle Database@AWS.

Alteração	Descrição	Data
Oracle Database@AWS suporta a região Ásia-Pacífico (Sydney) e a região do Canadá (Central)	Você pode criar seus Oracle Database@AWS recursos nessas regiões. Para obter mais informações, consulte Regiões suportadas para Oracle Database@AWS.	2 de fevereiro de 2026
Oracle Database@AWS suporta a região Ásia-Pacífico (Tóquio), a região Leste dos EUA (Ohio), a região da Europa (Frankfurt)	Você pode criar seus Oracle Database@AWS recursos nessas regiões. Para obter mais informações, consulte Regiões suportadas para Oracle Database@AWS.	22 de dezembro de 2025
Oracle Database@AWS suporta o compartilhamento de direitos entre Contas da AWS	Agora você pode compartilhar direitos do AWS Marketplace para o Oracle Database@ Contas da AWS na mesma AWS organização usando o AWS License Manager. AWS Para obter mais informações, consulte Compartilhamento de direitos no Oracle Database@ .AWS	19 de dezembro de 2025
Oracle Database@AWS suporta a modificação de filtros de dados de integração Zero-ETL	Oracle Database@AWS suporta a modificação de filtros de dados para integrações existentes de zero ETL	15 de outubro de 2025

	com o Amazon Redshift. Você pode atualizar os padrões de filtro de dados para incluir ou excluir esquemas e tabelas especificados da replicação de dados. Para obter mais informações, consulte Gerenciando integrações com ETL zero.	
Oracle Database@AWS suporta gerenciamento de CIDR de rede de pares para conexões de emparelhamento	Você pode especificar a rede ponto a ponto CIDRs ao criar ou atualizar conexões de emparelhamento ODB. Você controla quais sub-redes na VPC de mesmo nível têm acesso à sua rede ODB. Uma conta VPC pode atualizar os intervalos CIDR sem também possuir a rede ODB. Para obter mais informações, consulte Configurando o emparelhamento de ODB para uma Amazon VPC em. Oracle Database@AWS	10 de outubro de 2025
Oracle Database@AWS oferece suporte à integração sem ETL com o Amazon Redshift	Oracle Database@AWS agora se integra ao VPC Lattice para permitir a integração sem ETL com o Amazon Redshift. Para obter mais informações, consulte Integrações de serviços para Oracle AWS Database@.	02 de julho de 2025

Atualizar permissões de perfil vinculado a serviços do IAM	A `AmazonODBServiceRolePolicy` política agora concede permissões adicionais para descrever anexos do VPC Transit Gateway, descrever EC2 sub-redes da Amazon e ativar uma fonte da Amazon. EventBridge Para obter mais informações, consulte Oracle Database@AWS atualizações nas políticas AWS gerenciadas.	30 de junho de 2025
Atualizar permissões de perfil vinculado a serviços do IAM	A `AmazonODBServiceRolePolicy` política agora concede permissões adicionais para descrever eventos no Amazon EventBridge Scheduler e criar ou descrever um barramento de eventos. Para obter mais informações, consulte Oracle Database@AWS atualizações nas políticas AWS gerenciadas.	26 de junho de 2025
Oracle Database@AWS suporta a região Oeste dos EUA (Oregon)	Você pode criar seus Oracle Database@AWS recursos na região Oeste dos EUA (Oregon). Os AZ físicos suportados IDs são `usw2-az3` `usw2-az4` e. Para obter mais informações, consulte Regiões suportadas para Oracle Database@AWS.	26 de junho de 2025

Oracle Database@AWS suporta o compartilhamento de recursos entre Contas da AWS	Agora você pode compartilhar a infraestrutura do Exadata e os clusters de VM com outras pessoas Contas da AWS da sua organização usando AWS Resource Access Manager ().AWS RAM Você pode provisionar a infraestrutura uma vez e compartilhá-la em várias contas, reduzindo custos e mantendo a separação de responsabilidades. Para obter mais informações, consulte Compartilhamento de recursos no Oracle Database@AWS.	26 de junho de 2025
Oracle Database@AWS apoia eventos na Amazon EventBridge	Oracle Database@AWS entrega eventos para a Amazon EventBridge para monitorar as mudanças no ciclo de vida dos recursos. Os eventos são gerados de ambas as fontes AWS e da OCI, permitindo que você acompanhe alterações na rede ODB, na infraestrutura do Exadata, nos clusters de VM e nos bancos de dados. Para obter mais informações, consulte Monitoramento de Oracle Database@AWS eventos na Amazon EventBridge.	26 de junho de 2025

Oracle Database@AWS suporta assinatura entre regiões	Oracle Database@AWS oferece suporte à assinatura entre regiões, permitindo que você se inscreva uma vez e use o serviço em todas as opções disponíveis Regiões da AWS. Para obter mais informações, consulte Inscrever-se no Oracle Database@AWS em várias regiões.	26 de junho de 2025
Oracle Database@AWS suporta conexões de emparelhamento ODB como um recurso separado	As conexões de emparelhamento ODB agora são um recurso separado dedicado APIs à criação, visualização e exclusão de conexões de emparelhamento. Você pode criar conexões de emparelhamento entre uma rede ODB e uma Amazon VPC na mesma conta ou em contas diferentes. Para obter mais informações, consulte Trabalhando com conexões de emparelhamento ODB.	26 de junho de 2025
Oracle Database@AWS integra a rede ODB com o Amazon S3	Oracle Database@AWS agora se integra ao VPC Lattice para permitir backups gerenciados pela Oracle no Amazon S3 e acesso direto à rede ODB para o Amazon S3. Para obter mais informações, consulte Integrações de serviços para Oracle AWS Database@.	26 de junho de 2025

Oracle Database@AWS suporta clusters de VM autônomos	Agora você pode criar clusters de VMs autônomas na sua infraestrutura do Exadata. Os clusters de VM autônomos são bancos de dados totalment e gerenciados que automatiz am as principais tarefas de gerenciamento usando aprendizado de máquina e IA. Para obter mais informaçõ es, consulte Etapa 3: Criar um cluster de VM Exadata ou um cluster de VM autônomo em. Oracle Database@AWS	28 de maio de 2025
Oracle Database@AWS suporta janelas de manutençã o personalizáveis	Agora você pode configurar janelas de manutenção para sua infraestrutura do Exadata com opções para agendamen tos gerenciados pela Oracle ou pelo cliente. Você também pode selecionar os modos de aplicação de patches (contínuo ou não contínuo) e especificar as preferências de tempo de manutenção. Para obter mais informações, consulte Criar uma infraestr utura Oracle Exadata em. Oracle Database@AWS	1.º de maio de 2025

Oracle Database@AWS suporta uma nova zona de disponibilidade (AZ)	Agora você pode criar uma rede ODB em uma AZ com o ID físico `use1-az4` ou`use1-az6`. Para obter mais informações, consulte a infraestrutura do Oracle Exadata.	26 de março de 2025
Oracle Database@AWS é compatível com Amazon VPC Transit Gateways	Se você conectar um gateway de trânsito a uma VPC emparelhada a uma rede ODB, poderá conectar vários VPCs a esse gateway. Os aplicativos executados neles VPCs podem acessar um cluster de VM do Exadata em execução na sua rede ODB. Para obter mais informaçõ es, consulte Configurando os Amazon VPC Transit Gateways para. Oracle Database@AWS	26 de março de 2025
Oracle Database@AWS suporta tipos de servidores de banco de dados e armazenam ento para o Exadata X11M	Você pode especificar o tipo de servidor de banco de dados e o tipo de servidor de armazenamento ao criar uma infraestrutura usando o Exadata X11M. Para obter mais informações, consulte Criar uma infraestrutura Oracle Exadata em. Oracle Database@AWS	4 de fevereiro de 2025

Nova política de funções vinculadas a serviços	Oracle Database@AWS adicionou uma nova política `AmazonODBServiceRolePolicy` para a função `AWSServiceRoleForODB` vinculada ao serviço. Para obter mais informações, consulte Atualizações da Oracle Database@AWS para políticas gerenciadas pela AWS.	2 de dezembro de 2024
Lançamento inicial	Versão inicial do Guia Oracle Database@AWS do usuário	2 de dezembro de 2024

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.