Oracle Database@AWS Guía del usuario

Oracle Database@AWS

Oracle Database@AWS: Oracle Database@AWS Guía del usuario

Table of Contents

¿Qué es Oracle Database@AWS?

Oracle Database@AWS es una oferta que le permite acceder a la infraestructura de Oracle Exadata gestionada por Oracle Cloud Infrastructure (OCI) dentro AWS de los centros de datos. Puede migrar sus cargas de trabajo de Oracle Exadata, establecer una conectividad de baja latencia con las aplicaciones en ejecución e integrarlas con los servicios. AWS AWS Recibirá una sola factura AWS Marketplace, que se tendrá en cuenta para AWS los compromisos y las recompensas de Oracle Support.

El siguiente diagrama muestra una visión general de alto nivel de una región de OCI vinculada a un centro de AWS datos que aloja la infraestructura de Oracle Exadata. Dentro de una zona de AWS disponibilidad (AZ), puede conectar una Amazon VPC a una red privada vinculada al centro de datos. Al conectar estas redes, los servidores de aplicaciones de la VPC pueden acceder a las bases de datos de Oracle que se ejecutan en la infraestructura de Oracle Exadata.

Características de Oracle Database@AWS

Con Oracle Database@AWS, se beneficia de las siguientes características:

Migración de las cargas de trabajo de la base de datos Oracle Exadata a AWS

> Con él Oracle Database@AWS, puede migrar fácilmente sus cargas de trabajo de Oracle Exadata a Oracle Exadata Database Service en una infraestructura dedicada o a Oracle Autonomous Database en una infraestructura Exadata dedicada. AWS La migración ofrece cambios mínimos, disponibilidad total de funciones, compatibilidad arquitectónica y el mismo rendimiento que las implementaciones de Exadata locales. Puede utilizar las herramientas estándar de migración de bases de datos de Oracle, como Recovery Manager (RMAN), Oracle Data Guard, transportable tablespaces, Oracle Data Pump, Oracle, AWS Database Migration GoldenGate Service y Oracle Zero Downtime Migration.

Reducción de la latencia de las aplicaciones

> Puede establecer una conectividad de baja latencia entre Oracle Exadata y las aplicaciones en ejecución. AWS La proximidad a las aplicaciones alojadas AWS garantiza demoras mínimas en la red y mejora el rendimiento.

Innovación a través de la unificación de datos

Puede generar conocimientos más profundos y desarrollar nuevas innovaciones mediante el uso de integraciones sin ETL para unificar sus datos en Oracle y AWS para el análisis, el aprendizaje automático y la IA generativa. Con la integración sin ETL mediante Amazon Redshift, puede habilitar el análisis y el aprendizaje automático (ML) casi en tiempo real de los datos transaccionales almacenados en. Oracle Database@AWS

Administración y operaciones simplificadas

Puede beneficiarse de una experiencia unificada entre Oracle y de la AWS colaboración en materia de soporte, compras, administración y operaciones. El uso de los servicios de Oracle Database cumple los requisitos para sus AWS compromisos actuales y los beneficios de licencia de Oracle, como Oracle Support Rewards. Puede utilizar AWS herramientas e interfaces conocidas para comprar, aprovisionar y gestionar sus Oracle Database@AWS recursos. Puede aprovisionar y administrar sus recursos mediante AWS APIs CLI o SDKs. Luego, AWS APIs llame a la OCI correspondiente APIs necesaria para aprovisionar y administrar los recursos.

Integración perfecta con AWS los servicios

Puede integrarse con otros AWS servicios y aplicaciones que se ejecutan en el mismo entorno. Por ejemplo, Oracle Database@AWS se integra con Amazon EC2, Amazon VPC e IAM. También puede integrarse Oracle Database@AWS con AWS servicios como Amazon CloudWatch para la supervisión y Amazon EventBridge para la gestión de eventos. Para las copias de seguridad de bases de datos, puede utilizar Amazon S3, que está diseñado para superar los 11 9 segundos de durabilidad.

Relacionado Servicios de AWS

Oracle Database@AWS funciona con los siguientes servicios para mejorar la disponibilidad y la escalabilidad de las aplicaciones de bases de datos Oracle:

- Amazon EC2: proporciona servidores virtuales que funcionan como servidores de aplicaciones Oracle. Puede configurar su balanceador de carga para enrutar el tráfico a sus servidores de EC2 aplicaciones. Para obtener más información, consulta la Guía del EC2 usuario de Amazon.
- Amazon Virtual Private Cloud (VPC): le permite lanzar AWS recursos en una red virtual aislada de forma lógica que haya definido. La infraestructura de Oracle Exadata reside en una red especial denominada red ODB que se puede conectar a una VPC. A continuación, puede ejecutar

servidores de aplicaciones en su VPC y acceder a las bases de datos de Exadata. Para obtener más información, consulte la Guía del usuario de Amazon VPC.

- Amazon VPC Lattice: proporciona acceso nativo a AWS servicios como Amazon S3 y las copias de seguridad gestionadas por Oracle desde la red ODB. Para obtener más información, consulte ¿Qué es Amazon VPC Lattice? .
- Amazon CloudWatch: proporciona un servicio de monitoreo para Oracle Database@AWS. OCI recopila datos métricos sobre su sistema Oracle Exadata y los envía a. CloudWatch Para obtener más información, consulte Monitorización Oracle Database@AWS con Amazon CloudWatch.
- AWS Identity and Access Management (IAM): le ayuda a controlar de forma segura el acceso de sus usuarios a los Oracle Database@AWS recursos. Use la IAM para controlar quién puede usar sus AWS recursos (autenticación) y qué recursos pueden usar los usuarios y de qué manera (autorización). Para obtener más información, consulte Administración de identidades y accesos para Oracle Database@AWS.
- AWS servicios de análisis: proporcione un conjunto amplio y rentable de servicios de análisis que le ayuden a obtener información más rápida a partir de su base de datos de Exadata. Cada servicio está diseñado específicamente para una amplia gama de casos de uso del análisis, como el análisis interactivo, el procesamiento de macrodatos, el almacenamiento de datos, el análisis en tiempo real, el análisis operativo, los paneles y las visualizaciones. Para obtener más información, consulte Analytics en. AWS

Acceder Oracle Database@AWS

Puede crear, acceder y administrar Oracle Database@AWS mediante Consola de administración de AWS. Proporciona una interfaz web a la que puede acceder Oracle Database@AWS.

Precios para Oracle Database@AWS

Puede comprar Oracle Database@AWS ofertas en AWS Marketplace. Primero, póngase en contacto con un representante de ventas de Oracle. Luego, Oracle pone la oferta a su disposición en AWS Marketplace función del acuerdo de precios privado. En su AWS factura se muestran los cargos en función de su uso.

No hay cargos por transferencia de datos cuando la aplicación Oracle y la base de datos Oracle están alojadas en la misma zona de disponibilidad (AZ). Se aplican cargos estándar de transferencia de datos a las comunicaciones entre AZs.

Cuando se utilizan integraciones Oracle Database@AWS gestionadas como Zero-ETL, copias de seguridad gestionadas por Oracle y Amazon S3, se aplican los cargos estándar de procesamiento de datos por compartir y acceder a los recursos a través de VPC Lattice. Las integraciones gestionadas no cobran por hora. Oracle Database@AWS Para obtener más información, consulte los precios de Amazon VPC Lattice.

Siguientes pasos

Ahora está listo para empezar a crear sus recursos. Oracle Database@AWS

1. Obtenga información sobre cómo Oracle Database@AWS funciona. Para obtener más información, consulte Cómo Oracle Database@AWS funciona.

   > **Note**
   >
   > Si está familiarizado con AWS Oracle Exadata y quiere empezar de inmediato, omita este paso.

2. Solicite una oferta privada Oracle Database@AWS a través del y Consola de administración de AWS, a continuación, acéptela. Para obtener más información, consulte Solicite una oferta privada para Oracle Database@AWS.

   > **Note**
   >
   > Para solicitar una oferta privada en esta vista previa, debes ponerte en contacto con nosotros AWS para que te Cuenta de AWS agreguen a una lista de personas permitidas.

3. Cree su red ODB, la infraestructura de Oracle Exadata y los clústeres de máquinas virtuales de Exadata mediante la consola. AWS Cree sus bases de datos de Exadata con las herramientas de OCI. Para obtener más información, consulte Introducción a Oracle Database@AWS.
4. Comparta sus recursos entre cuentas con AWS Resource Access Manager ().AWS RAM Para obtener más información, consulte Trabajar con Oracle Database@AWS recursos compartidos en una cuenta de confianza.

Cómo Oracle Database@AWS funciona

Oracle Database@AWS integra Oracle Cloud Infrastructure (OCI) con. Nube de AWS En las siguientes secciones, puede obtener información sobre los componentes clave de esta arquitectura multinube.

El servicio de base de datos Oracle Exadata en una infraestructura dedicada es un servicio de OCI que proporciona la máquina de base de datos Exadata. Oracle Exadata Database Machine es una plataforma completa integrada, preconfigurada y probada previamente para su uso en centros de datos empresariales. Puede crear la infraestructura de Oracle Exadata y los clústeres de máquinas virtuales en una zona de AWS disponibilidad (AZ) mediante la AWS consola, la CLI o. APIs

Una vez que haya creado sus recursos AWS, utilizará OCI APIs para crear y gestionar las bases de datos de Oracle Exadata. Una red ODB, que se conecta a una VPC de Amazon, permite a los servidores de aplicaciones de EC2 Amazon acceder a las bases de datos de Exadata. De esta forma, las bases de datos Oracle Exadata se integran en el entorno. AWS

El siguiente diagrama muestra la Oracle Database@AWS arquitectura.

Sitios secundarios de OCI

Oracle Cloud Infrastructure se aloja en regiones y dominios de disponibilidad de OCI. Una región de OCI consta de dominios de disponibilidad de OCI (ADs), que son clústeres de centros de datos aislados dentro de una región de OCI. Un sitio secundario de OCI es un centro de datos que extiende un dominio de disponibilidad de OCI a una zona de disponibilidad (AZ) de una región. AWS La infraestructura de Exadata reside lógicamente en una región de OCI y reside físicamente en una región. AWS

El sitio secundario de OCI reside Oracle Database@AWS físicamente en un centro de AWS datos. AWS aloja la infraestructura de Exadata y OCI aprovisiona y mantiene el hardware de la infraestructura de Exadata dentro del centro de datos. Puede configurar la infraestructura, la red privada y los clústeres de máquinas virtuales de Exadata mediante la AWS consola, la CLI o. APIs Puede utilizar AWS servicios como Amazon EC2 y Amazon VPC para permitir el acceso de las aplicaciones a las bases de datos Oracle Exadata que se ejecutan en la infraestructura.

Infraestructura Oracle Exadata

La infraestructura Oracle Exadata es la arquitectura subyacente de los servidores de bases de datos y los servidores de almacenamiento que ejecutan las bases de datos Oracle Exadata. La infraestructura reside en una zona de AWS disponibilidad (AZ). Para crear clústeres de máquinas virtuales en la infraestructura de Exadata, utilice la AWS consola, la CLI o. APIs

La infraestructura de Oracle Exadata se distribuye en máquinas físicas denominadas servidores de bases de datos. Estos servidores proporcionan los recursos informáticos, de forma similar a los servidores EC2 dedicados de Amazon. Cada servidor de base de datos aloja una o más máquinas virtuales (VMs) que se ejecutan en un hipervisor. Para ver los diagramas de arquitectura que ilustran estas relaciones, consulte el Servicio de bases de datos de Exadata sobre arquitectura técnica de infraestructura dedicada.

Al crear la infraestructura de Exadata en Oracle Database@AWS, debe especificar información como la siguiente:

- El número total de servidores de bases de datos
- La cantidad total de servidores de almacenamiento
- El modelo de sistema Exadata (X11M)
- La zona de disponibilidad que aloja la infraestructura (consulte) Regiones compatibles para Oracle Database@AWS

Para obtener información sobre cómo crear una infraestructura de Oracle Exadata, consulte. Paso 2: Cree una infraestructura de Oracle Exadata en Oracle Database@AWS

Red ODB

Una red ODB es una red privada aislada que aloja la infraestructura OCI en una zona de AWS disponibilidad (AZ). La red ODB consta de un rango CIDR de direcciones IP. La red ODB se asigna directamente a la red que existe dentro del sitio secundario de la OCI y, por lo tanto, sirve como medio de comunicación entre una OCI. AWS Debe especificar una red ODB al crear los clústeres de máquinas virtuales de Exadata (consulte). Paso 3: Cree un clúster de máquinas virtuales de Exadata o un clúster de máquinas virtuales autónomas en Oracle Database@AWS

Los recursos se aprovisionan en una red ODB mediante Oracle Database@.AWS APIs La red ODB está gestionada por AWS, pero usted puede configurar una conexión de emparejamiento ODB para conectar una Amazon VPC a la red ODB. Para obtener más información, consulte en. Emparejamiento ODB

Al crear una red ODB, se especifica información como la siguiente:

- Zona de disponibilidad: la red ODB es específica de una zona de disponibilidad.

  Puede utilizarla de Oracle Database@AWS la siguiente manera: Regiones de AWS

  Este de EE. UU. (Norte de Virginia)

  Puede usarlo AZs con el IDs `use1-az4` y físico`use1-az6`.

  Oeste de EE. UU. (Oregón)

  Puede usarlo AZs con el IDs `usw2-az3` y físico`usw2-az4`.

  Asia-Pacífico (Tokio)

  Puede usarlo AZs con el IDs `apne1-az1` y físico`apne1-az4`.

  Este de EE. UU. (Ohio)

  Puede usarlo AZs con el IDs `use2-az1` y físico`use2-az2`.

  Europa (Fráncfort)

  Puede usarlo AZs con el IDs `euc1-az1` y físico`euc1-az2`.

  Canadá (centro)

  Puede usar la AZ con la identificación física`cac1-az4`.

  Asia-Pacífico (Sídney)

  Puede usar la AZ con la identificación física`apse2-az4`.

  Para buscar los nombres de AZ lógicos de su cuenta que se asignan a la AZ física anterior IDs, ejecute el siguiente comando.

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

- Direcciones CIDR del cliente: la red ODB requiere un CIDR de subred del cliente para los clústeres de máquinas virtuales de Exadata y los clústeres de máquinas virtuales autónomas.
- Direcciones CIDR de respaldo: la red ODB requiere un CIDR de subred de respaldo para las copias de seguridad administradas de las bases de datos de los clústeres de máquinas virtuales. La subred de respaldo es opcional para los clústeres de máquinas virtuales de Exadata.
- AWS integraciones de servicios: puede configurar una ruta de red para integraciones de AWS servicios como Amazon S3 y Zero-ETL con Amazon Redshift. Para obtener más información, consulte AWS integraciones de servicios.

Para obtener más información, consulte Paso 1: Cree una red ODB en Oracle Database@AWS.

Virtual Private Cloud (VPC) (Nube virtual privada)

Una Nube Privada Virtual (VPC) es una red virtual que se crea en la nube. AWS Está aislada lógicamente de otras redes virtuales de la AWS nube, lo que le proporciona un control total sobre el entorno de red virtual, incluida la selección de su propio rango de direcciones IP, la creación de subredes y la configuración de las tablas de enrutamiento y las puertas de enlace de red. Para obtener más información, consulte ¿Qué es Amazon VPC?

Puede lanzar EC2 instancias de Amazon en su VPC de Amazon. Las EC2 instancias pueden alojar servidores de aplicaciones que se comunican con las bases de datos de Oracle Exadata. Puede administrar e iniciar los servidores de aplicaciones como cualquier otra EC2 instancia de su VPC. Para obtener más información, consulta ¿Qué es Amazon EC2?

De forma predeterminada, la red ODB no tiene conectividad con VPCs. Para conectar la red ODB a la AWS infraestructura existente, cree una conexión de emparejamiento entre la red ODB y una VPC. Puede especificar la VPC al crear la red ODB. Para obtener más información, consulte Paso 1: Cree una red ODB en Oracle Database@AWS.

Emparejamiento ODB

El peering ODB es una conexión de red creada por el usuario que permite enrutar el tráfico de forma privada entre una Amazon VPC y una red ODB. Existe una relación 1:1 entre una VPC y una red ODB. Tras el emparejamiento, una EC2 instancia de Amazon dentro de la VPC puede comunicarse con una base de datos Oracle Exadata de la red ODB como si estuvieran dentro de la misma red.

> **Note**
>
> El emparejamiento de ODB es diferente del emparejamiento de VPC, que es una conexión de emparejamiento entre dos VPCs que enruta el tráfico entre ellos.

Puede emparejar una red ODB en una cuenta y una VPC en otra cuenta utilizando. AWS RAM Si compartes una red ODB con otra cuenta, la cuenta de confianza puede iniciar el emparejamiento directamente. La cuenta que inicia la conexión de emparejamiento ODB es la propietaria de la conexión y la administra.

Puede especificar una red homóloga CIDRs al crear o actualizar las conexiones de interconexión ODB. De esta forma, puede controlar qué subredes de la VPC homóloga tienen acceso a su red ODB. Una cuenta de VPC puede actualizar los rangos de CIDR sin ser propietaria también de la red ODB. Para obtener más información, consulte Configuración del emparejamiento de ODB a una Amazon VPC en. Oracle Database@AWS

Los recursos de una VPC pueden abarcar zonas de disponibilidad ()AZs. En una red ODB, los recursos están enlazados a una única zona de disponibilidad. Esta zona de disponibilidad se define al crear la red ODB.

Creación de una conexión de emparejamiento ODB

Una conexión de emparejamiento ODB no es una característica de una red ODB, sino que es un recurso independiente con su propio identificador (con el prefijo) y ciclo de vida. `odbpcx-` Una conexión de interconexión se gestiona con un conjunto de conexiones dedicadas. APIs Por ejemplo, puede crear una conexión de emparejamiento ODB a una red ODB existente mediante la consola Oracle AWS Database@ o la API. `CreateOdbPeeringConnection` Para obtener más información, consulte Creación de una conexión de emparejamiento ODB en Oracle Database@AWS.

Al crear una conexión de emparejamiento ODB, Oracle Database@ realiza las siguientes acciones automáticamente:AWS

1. Valida las configuraciones de red, incluida la comprobación de bloques CIDR superpuestos con el CIDR de Oracle VCN
2. Configura la infraestructura de interconexión de red subyacente

3. Configura las tablas de enrutamiento de la red ODB (no la VPC) con las direcciones CIDR de la VPC

Después de crear la conexión de emparejamiento ODB, actualice las tablas de enrutamiento de la VPC manualmente mediante el comando Amazon. EC2 `create-route` Para obtener más información, consulte Configuración de tablas de enrutamiento de VPC para el emparejamiento de ODB.

AWS integraciones de servicios

Para ofrecer opciones de conectividad y funcionalidad mejoradas para sus bases de datos Oracle, Oracle Database@AWS se integra con Servicios de AWS Amazon VPC Lattice. Puede configurar las rutas de red Servicios de AWS directamente desde su red ODB sin necesidad de configuraciones de red adicionales VPCs o complejas.

Oracle Database@AWS admite las siguientes AWS integraciones de servicios gestionados:

Amazon S3

Puede integrar Amazon S3 con Oracle Database@ de las siguientes AWS maneras:

- Oracle gestionó copias de seguridad automáticas en Amazon S3: Oracle Database@ permite AWS automáticamente el acceso a la red para realizar copias de seguridad automáticas. Esta integración no se puede deshabilitar. Si establece Amazon S3 como destino de backup gestionado en la consola de OCI, OCI carga las copias de seguridad automáticas en un bucket de S3.
- Acceso directo a Amazon S3 desde su red ODB: puede habilitar el acceso directo de red ODB a S3 y, a continuación, almacenar scripts, importar y exportar archivos y archivos relacionados en un bucket de S3. Puede deshabilitar este acceso. Esta configuración es independiente del acceso automático a la red para las copias de seguridad automáticas gestionadas por Oracle.

Integración sin ETL con Amazon Redshift

Puede habilitar la integración sin ETL de su red ODB con Amazon Redshift. Esta integración le permite replicar datos en Amazon Redshift desde sus bases de datos Oracle que se ejecutan en Oracle Database@AWS sin el proceso tradicional de extracción, transformación y carga (ETL). Esta integración permite el análisis en tiempo real y las cargas de trabajo de IA mediante la sincronización automática de los datos de Oracle con Amazon Redshift.

Además de las integraciones gestionadas para AWS los servicios, también puede utilizar VPC Lattice para acceder a los servicios y recursos alojados en VPCs otros, o acceder a las instancias de red de ODB desde su VPC. Puede administrar el acceso y los recursos mediante la consola VPC Lattice, la CLI y. APIs Para obtener más información, consulte los siguientes recursos:

- Realizar copias de seguridad en Oracle Database@AWS
- Integración de Oracle Database@AWS Zero-ETL con Amazon Redshift
- ¿Qué es Amazon VPC Lattice? y VPC Lattice para Oracle Database@AWS

Enrutar el tráfico desde múltiples VPCs

Para permitir que varios accedan VPCs a Oracle Database@AWS los recursos de una red ODB, puedes usar AWS Transit Gateway o AWS Cloud WAN.

AWS Transit Gateway

Una puerta de enlace de tránsito de Amazon VPC es un centro de tránsito de red que se utiliza para interconectar redes locales VPCs y locales. Una red ODB solo admite el emparejamiento one-to-one directo entre la red ODB y una sola VPC. Puede conectar su red ODB a una VPC y, a continuación, conectar esta VPC a una puerta de enlace de tránsito. La puerta de enlace se puede conectar a varias. VPCs Con esta configuración de puerta de enlace de tránsito, puede enrutar el tráfico entre varias subredes de VPC a una sola red ODB.

Para obtener más información, consulte Configuración de Amazon VPC Transit Gateways para Oracle Database@AWS.

AWS WAN en la nube

AWS La WAN en la nube es un servicio gestionado de redes de área amplia (WAN) que le permite crear, administrar y monitorear una red global unificada que conecte los recursos entre sus entornos de nube y locales. Con el panel central, puede conectar sucursales locales, centros de datos y VPCs toda la AWS red global.

Puedes conectar tu red ODB a una VPC y, a continuación, conectar esta VPC a la red principal de Cloud WAN. Con esta configuración, puedes usar Cloud WAN para enrutar el tráfico entre redes múltiples VPCs o locales y tu red ODB. Para obtener más información, consulte Configuración de AWS Cloud WAN para Oracle Database@AWS.

Clústeres de máquinas virtuales de Exadata

Un clúster de máquinas virtuales de Exadata es un conjunto de Exadata estrechamente acoplados. VMs Cada máquina virtual tiene una instalación completa de base de datos de Oracle que incluye todas las funciones de Oracle Enterprise Edition, incluidas Oracle Real Application Clusters (Oracle RAC) y Oracle Grid Infrastructure. Puede crear una o más bases de datos Oracle Exadata en un clúster de máquinas virtuales. Para ver diagramas que muestran la arquitectura de los clústeres de máquinas virtuales VMs y los clústeres, consulte Exadata Database Service on Dedicated Infrastructure Technical Architecture.

Al crear un clúster de máquinas virtuales, debe especificar información que incluye lo siguiente:

- Una red ODB
- Una infraestructura Oracle Exadata
- Los servidores de bases de datos en los que colocarlos VMs en el clúster
- La cantidad total de almacenamiento de Exadata utilizable

Puede configurar los núcleos de la CPU, la memoria y el almacenamiento local para cada máquina virtual de un clúster de máquinas virtuales. Para obtener más información, consulte Paso 3: Cree un clúster de máquinas virtuales de Exadata o un clúster de máquinas virtuales autónomas en Oracle Database@AWS.

Clústeres de máquinas virtuales autónomos

Los clústeres de máquinas virtuales autónomas son bases de datos totalmente gestionadas que automatizan las tareas de gestión clave mediante el aprendizaje automático y la IA. A diferencia de las bases de datos tradicionales, las bases de datos autónomas aprovisionan, protegen, actualizan, respaldan y ajustan automáticamente la base de datos sin necesidad de intervención humana.

Puede configurar el número de núcleos de la ECPU por máquina virtual, la memoria de la base de datos por CPU, el almacenamiento de la base de datos y el número máximo de bases de datos en contenedores autónomos. Para obtener más información, consulte Paso 3: Cree un clúster de máquinas virtuales de Exadata o un clúster de máquinas virtuales autónomas en Oracle Database@AWS.

Bases de datos Oracle Exadata

Oracle Exadata es un sistema diseñado que proporciona una plataforma de alto rendimiento para ejecutar bases de datos Oracle. Con ella Oracle Database@AWS, puede utilizar la AWS consola para crear la infraestructura de Oracle Exadata y los clústeres de máquinas virtuales que alojan las bases de datos de Exadata. A continuación, utilice OCI para crear y gestionar APIs las bases de datos de Oracle. Para obtener más información, consulte Paso 4: Cree bases de datos Oracle Exadata en Oracle Cloud Infrastructure.

Incorporación a Oracle Database@AWS

Antes de empezar a usarlo Oracle Database@AWS, asegúrate de estar registrado AWS y de crear los usuarios necesarios. Luego, puede comprar Oracle Database@AWS AWS Marketplace aceptando una oferta privada de Oracle.

Inscríbase para obtener una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar Tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión Consola de administración de AWScomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Solicite una oferta privada para Oracle Database@AWS

La función de oferta privada para AWS Marketplace vendedores le permite solicitar y recibir de Oracle los AWS precios de Oracle Database@ y las condiciones del EULA. Usted negocia los precios y las condiciones con Oracle y, a continuación, Oracle crea una oferta privada para la Cuenta de AWS que usted designe. Usted acepta la oferta privada y recibe el precio y las condiciones de uso negociados. En este momento, puedes usar el Oracle Database@AWS panel de control. Cuando el acuerdo de oferta privada llegue a su fecha de caducidad, pasará automáticamente a los precios públicos del producto o cancelará su suscripción a Oracle Database@.AWSPara obtener más información sobre las ofertas privadas, consulte Ofertas privadas en. AWS Marketplace

Para solicitar y aceptar una oferta privada de Oracle Database@AWS

1. Inicie sesión en Consola de administración de AWS.
2. Busque Oracle Database@ y, a continuación, elija Oracle Database@AWS.
3. Seleccione Solicitar oferta privada.

> **Note**
>
> El Oracle Database@AWS panel de control no estará disponible hasta que hayas aceptado una oferta privada.

4. En el sitio de Oracle Cloud Infrastructure (OCI), especifique detalles como la región y su información de contacto.
5. Espere a que un representante de la OCI se ponga en contacto con usted y ponga a su disposición una oferta privada.
6. En el Consola de administración de AWS, selecciona Ver oferta privada.
7. Selecciona la oferta y, a continuación, selecciona Ver oferta.
8. Selecciona Crear contrato y responde a las siguientes instrucciones para aceptar la oferta privada.
9. Tras aceptar la oferta privada, tendrás que activar tu cuenta OCI. Puede acceder a los enlaces de activación de Oracle directamente desde Consola de administración de AWS.

1. En la consola, vaya a la sección Cómo empezar.
2. Haga clic en el enlace de activación de Oracle que se proporciona en la consola. Como alternativa, también puede utilizar el enlace de activación que se le envió por correo electrónico.
3. En la página de activación de Oracle, elija si desea crear una nueva cuenta en la nube de Oracle o agregarla a una cuenta existente.
4. Complete el proceso de activación siguiendo las instrucciones que aparecen en pantalla.
5. Tras enviar la solicitud de activación, aparecerá el estado «Activación en curso» y el Consola de administración de AWS panel de control se desactivará temporalmente y se mostrará el motivo.
6. Una vez completada la activación, estará disponible el AWS panel de control de Oracle Database@, que le permitirá gestionar sus recursos.

10. En el Consola de administración de AWS, elija Panel de control.

Suscríbase a Oracle Database@AWS en varias regiones

Cuando se suscriba a Oracle Database@AWS través de la incorporación AWS Marketplace y termine de incorporarse, estará Cuenta de AWS vinculado a su arrendamiento de OCI. Este enlace, junto con los recursos relacionados, se replican automáticamente en todas AWS las regiones en las que está disponible. Oracle Database@AWS Te suscribes e incorporas una sola vez, en lugar de repetir el proceso para cada región.

Para usarlo Oracle Database@AWS en varias regiones, lleve a cabo los siguientes pasos:

1. Oracle Database@AWS Suscríbase AWS Marketplace y complete el proceso de incorporación.

   Cuando se suscribe por primera vez a Oracle Database@AWS, su cuenta se activa en una región de origen. La región de origen se especifica en Oracle Cloud Infrastructure (OCI).
2. Habilite las regiones que prefiera a través de la consola OCI.

   Si no habilita una región en OCI y, a continuación, cambia a esta región en la Oracle Database@AWS consola, recibirá un mensaje de error que indica que no se ha suscrito. En este caso, debe habilitar esta región en OCI para poder usar el Oracle Database@AWS panel de control de esta región.

3. Acceda Oracle Database@AWS desde cualquier AWS región compatible sin repetir el proceso de suscripción.

Introducción a Oracle Database@AWS

Para empezar a Oracle Database@AWS utilizarlos, puede crear los siguientes recursos mediante la Oracle Database@AWS consola, la CLI o APIs:

1. Red ODB
2. Infraestructura Oracle Exadata
3. Clúster de máquinas virtuales Exadata o clúster de máquinas virtuales autónomas
4. Conexión de emparejamiento ODB

Para crear bases de datos Oracle Exadata en su infraestructura, debe utilizar la consola o APIs el panel de control de Oracle Cloud Infrastructure (OCI). Oracle Database@AWS Por lo tanto, los recursos se despliegan en dos entornos de nube: los recursos de red e infraestructura se encuentran en AWS OCI y el plano de control de administración de la base de datos se encuentra en OCI. Para obtener más información, consulte Oracle Database@AWSla documentación de Oracle Cloud Infrastructure.

Requisitos previos para la configuración Oracle Database@AWS

Antes de configurar la infraestructura de Oracle Exadata, asegúrese de hacer lo siguiente:

- Realice los pasos que se indican en Incorporación a Oracle Database@AWS. Debe haber aceptado una oferta privada para poder utilizarla. Oracle Database@AWS
- Otorgue a su director de IAM los permisos de política que se indican enPermita a los usuarios aprovisionar Oracle Database@AWS recursos. Es necesario utilizar Oracle Database@AWS estos permisos.

Servicios de OCI compatibles en Oracle Database@AWS

Oracle Database@AWS admite los siguientes servicios de Oracle Cloud Infrastructure (OCI):

- Servicio de base de datos Oracle Exadata en una infraestructura dedicada: proporciona un entorno de Exadata dedicado y totalmente gestionado, al que se puede acceder desde dentro. AWS Para obtener más información, consulte el servicio de base de datos Oracle Cloud Exadata en infraestructura dedicada en la documentación de la OCI.

- Base de datos autónoma en una infraestructura Exadata dedicada: proporciona un entorno de base de datos altamente automatizado y totalmente gestionado que se ejecuta en OCI con recursos de hardware y software comprometidos. Para obtener más información, consulte Acerca de la base de datos autónoma en una infraestructura de Exadata dedicada en la documentación de la OCI.

Regiones compatibles para Oracle Database@AWS

Se puede utilizar Oracle Database@AWS en lo siguiente Regiones de AWS:

Este de EE. UU. (Norte de Virginia)

Puede usarlo AZs con el IDs `use1-az4` y físico`use1-az6`.

Oeste de EE. UU. (Oregón)

Puede usarlo AZs con el IDs `usw2-az3` y físico`usw2-az4`.

Asia-Pacífico (Tokio)

Puede usarlo AZs con el IDs `apne1-az1` y físico`apne1-az4`.

Este de EE. UU. (Ohio)

Puede usarlo AZs con el IDs `use2-az1` y físico`use2-az2`.

Europa (Fráncfort)

Puede usarlo AZs con el IDs `euc1-az1` y físico`euc1-az2`.

Canadá (centro)

Puede usar la AZ con la identificación física`cac1-az4`.

Asia-Pacífico (Sídney)

Puede usar la AZ con la identificación física`apse2-az4`.

Para buscar los nombres de AZ lógicos de su cuenta que se asignan a la AZ física anterior IDs, ejecute el siguiente comando.

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

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

Planeando el espacio de direcciones IP en Oracle Database@AWS

Planifique cuidadosamente el espacio de direcciones IP Oracle Database@AWS. Tenga en cuenta el consumo de direcciones IP en función del número de clústeres de máquinas virtuales, incluido el número de clústeres VMs por clúster que puede aprovisionar en la red ODB. Para obtener más información, consulte Diseño de red ODB en la documentación de Oracle Cloud Infrastructure.

Temas

- Restricciones de las direcciones IP en la red ODB
- Requisitos de CIDR de la subred del cliente para la red ODB
- Requisitos CIDR de subred de Backup para la red ODB
- Escenarios de consumo de IP para la red ODB

Restricciones de las direcciones IP en la red ODB

Tenga en cuenta las siguientes restricciones con respecto a los rangos de CIDR en la red ODB:

- No puede modificar el rango de CIDR de la subred de respaldo o del cliente para la red ODB después de crearla.
- No puede usar los rangos de CIDR de VPC de la columna Asociaciones restringidas de la tabla de restricciones de asociación de bloques de IPv4 CIDR.
- En el caso de Exadata X9M, la automatización de OCI reserva las direcciones IP 100.106.0.0/16 y 100.107.0.0/16 para la interconexión de clústeres, por lo que no puede hacer lo siguiente:
  - Asigne estos rangos al rango CIDR de cliente o de respaldo de la red ODB.
  - Utilice estos rangos para un CIDR de VPC que se utilice para conectarse a la red ODB.
- Los siguientes rangos de CIDR están reservados para Oracle Cloud Infrastructure y no se pueden usar para la red ODB:
  - Rango reservado CIDR 169.254.0.0/16 de Oracle Cloud
  - Clase D reservada 224.0.0.0 — 239.255.255.255
  - Clase E reservada 240.0.0.0 — 255.255.255
- No puede superponer los rangos CIDR de direcciones IP de las subredes de cliente y de respaldo.

- No puede superponer los rangos CIDR de direcciones IP asignados a las subredes de cliente y respaldo con los rangos CIDR de VPC utilizados para conectarse a la red ODB.
- No puedes aprovisionar VMs en un clúster de máquinas virtuales distintas redes ODB. La red es una propiedad del clúster de máquinas virtuales, lo que significa que solo puede aprovisionar la VMs red del clúster de máquinas virtuales en la misma red ODB.

Requisitos de CIDR de la subred del cliente para la red ODB

En la siguiente tabla, puede encontrar la cantidad de direcciones IP consumidas por el servicio y la infraestructura del CIDR de la subred del cliente. El tamaño mínimo del CIDR para la subred del cliente es /27 y el tamaño máximo es /16.

El número de direcciones IP estáticas	Consumido por	Notas
6	Oracle Database@AWS	Estas direcciones IP están reservadas independientemente del número de clústeres de máquinas virtuales que aprovisione en la red ODB. Oracle Database@AWS consume lo siguiente: • 3 direcciones IP reservadas para los recursos de red ODB en AWS • 3 direcciones IP reservadas para el servicio de red OCI
3	Cada clúster de máquinas virtuales	Estas direcciones IP están reservadas para los nombres de acceso de un solo cliente (SCANs), independientemente del número VMs que haya en cada clúster de máquinas virtuales.
4	Cada máquina virtual	Estas direcciones IP dependen únicamente del número de direcciones IP que VMs haya en la infraestructura.

Requisitos CIDR de subred de Backup para la red ODB

En la siguiente tabla, puede encontrar la cantidad de direcciones IP consumidas por el servicio y la infraestructura del CIDR de la subred de respaldo. El tamaño mínimo del CIDR para la subred de respaldo es /28 y el tamaño máximo es /16.

El número de direcciones IP estáticas	Consumido por	Notas
3	Oracle Database@AWS	Estas direcciones IP están reservadas independientemente del número de clústeres de máquinas virtuales que aprovisione en la red ODB. Oracle Database@AWS consume lo siguiente: • 2 direcciones IP al principio del rango CIDR • 1 dirección IP al final del rango CIDR
3	Cada máquina virtual	Estas direcciones IP dependen únicamente del número de direcciones IP que VMs haya en la infraestructura.

Escenarios de consumo de IP para la red ODB

En la siguiente tabla, puede ver las direcciones IP consumidas en la red ODB para las diferentes configuraciones de clústeres de máquinas virtuales. Si bien /28 es el rango CIDR mínimo desde el punto de vista técnico para que la subred del cliente implemente 1 clúster de máquinas virtuales con 2 VMs, le recomendamos que utilice al menos un rango CIDR de /27. En este caso, los clústeres de máquinas virtuales no consumen todo el rango de IP y permiten la asignación de direcciones IP adicionales.

Configuración	Cliente IPs consumido	Cliente IPs mínimo	Backup IPs consumido	Backup IPs mínimo
1 clúster de máquinas	17 (6 servicios + 3 clústeres + 4*2)	32 (rango CIDR de /27)	(93 servicios + 3*2)	16 (rango C/28 CIDR)

Configuración	Cliente IPs consumido	Cliente IPs mínimo	Backup IPs consumido	Backup IPs mínimo
virtuales con 2 VMs				
1 clúster de máquinas virtuales con 3 VMs	21 (6 servicios + 3 clústeres + 4*3)	32 (rango CIDR de /27)	12 (3 servicios + 3*3)	16 (rango C/28 CIDR)
1 clúster de máquinas virtuales con 4 VMs	25 (6 servicios + 3 clústeres + 4*4)	32 (rango CIDR de /27)	15 (3 servicios + 3*4)	16 (rango C/28 CIDR)
1 clúster de máquinas virtuales con 8 VMs	41 (6 servicios + 3 clústeres + 4*8)	64 (rango de /26 CIDR)	27 (3 servicios + 3*8)	32 (rango C/27 CIDR)

La siguiente tabla muestra cuántas instancias de cada configuración son posibles dado un rango de CIDR de cliente específico. Por ejemplo, 1 clúster de máquinas virtuales con 4 VMs consume 24 direcciones IP en la subred del cliente. Si el rango CIDR es /25, hay 128 direcciones IP disponibles. Por lo tanto, puede aprovisionar 5 clústeres de máquinas virtuales en la subred.

Configuración del clúster de máquinas virtuales	Número con /27 (32 IPs)	Número con /26 (64) IPs	Número con /25 (128) IPs	Número con /24 (256) IPs	Número cuando /23 (512) IPs	Número cuando /22 (1024) IPs
1 clúster de máquina virtual con 2 VMs (16 IPs)	1	3	7	15	30	60

Configuración del clúster de máquinas virtuales	Número con /27 (32 IPs)	Número con /26 (64) IPs	Número con /25 (128) IPs	Número con /24 (256) IPs	Número cuando /23 (512) IPs	Número cuando /22 (1024) IPs
1 clúster de máquinas virtuales con 3 VMs (20 IPs)	1	3	6	12	24	48
1 clúster de máquinas virtuales con 4 VMs (24 IPs)	1	2	5	10	20	40
2 clústeres de máquinas virtuales con 2 VMs cada uno (27 IPs)	1	2	4	9	18	36
2 clústeres de máquinas virtuales con 3 VMs cada uno (35 IPs)	0	1	3	7	14	28
2 clústeres de máquinas virtuales con 4 VMs cada uno (43 IPs)	0	1	2	5	11	23

Paso 1: Cree una red ODB en Oracle Database@AWS

Una red ODB es una red privada aislada que aloja la infraestructura OCI en una zona de disponibilidad (AZ). Una red ODB y una infraestructura Oracle Exadata son condiciones previas para el aprovisionamiento de clústeres de máquinas virtuales y la creación de bases de datos de Exadata. Puede crear la red ODB y la infraestructura de Oracle Exadata en cualquier orden. Para obtener más información, consulte Red ODB y Emparejamiento ODB.

En esta tarea se presupone que ha leído. Planeando el espacio de direcciones IP en Oracle Database@AWS Para modificar o eliminar la red ODB más adelante, consulteGestión de Oracle Database@AWS.

Para crear una red ODB

1. Inicie sesión en Consola de administración de AWS y abra la Oracle Database@AWS consola en https://console.aws.amazon.com/odb/.
2. Elige tu AWS región en la esquina superior derecha. Para obtener más información, consulte Regiones compatibles para Oracle Database@AWS.
3. En el panel izquierdo, selecciona redes ODB.
4. Seleccione Crear red ODB.
5. Para el nombre de red ODB, introduzca un nombre de red. El nombre debe tener entre 1 y 255 caracteres y empezar por un carácter alfabético o un guión bajo. No puede contener guiones consecutivos.
6. Para la zona de disponibilidad, elija un nombre de zona de disponibilidad. Para obtener información sobre AZs la compatibilidad, consulteRegiones compatibles para Oracle Database@AWS.
7. Para el CIDR de la subred del cliente, especifique un rango de CIDR para las conexiones del cliente. Para obtener más información, consulte Requisitos de CIDR de la subred del cliente para la red ODB.
8. En el CIDR de la subred de Backup, especifique un rango de CIDR para las conexiones de respaldo. Para aislar el tráfico de respaldo y mejorar la resiliencia, le recomendamos que no superponga el CIDR de respaldo y el CIDR del cliente. Para obtener más información, consulte Requisitos CIDR de subred de Backup para la red ODB.
9. Para la configuración de DNS, elija una de las siguientes opciones:

   Predeterminado

   En Prefijo de nombre de dominio, introduce un nombre para usarlo como prefijo de tu dominio. El nombre de dominio se fija como oraclevcn.com. Por ejemplo, si ingresa, el nombre de dominio completo es **`myhost`** myhost.oraclevcn.com.

   Nombre de dominio personalizado

   En Nombre de dominio, introduce un nombre de dominio completo. Por ejemplo, puede escribir myhost.myodb.com.

10. (Opcional) Para las integraciones de servicios, seleccione un servicio para integrarlo con su red mediante VPC Lattice. Oracle Database@AWS se integra con varios Servicios de AWS para ofrecer mejores opciones de funcionalidad y conectividad para sus bases de datos Oracle. Seleccione una de las siguientes integraciones:

    Amazon S3

    Habilite el acceso directo a la red ODB a Amazon S3. Sus bases de datos pueden acceder a S3 para importar o exportar datos o realizar copias de seguridad personalizadas. Puede introducir una política de JSON. Para obtener más información, consulte Backups gestionados por el usuario en Amazon S3 en Oracle Database@AWS.

    ETL cero

    Habilite el aprendizaje automático y el análisis en tiempo real de los datos transaccionales con Amazon Redshift. Para obtener más información, consulte Integración de Oracle Database@AWS Zero-ETL con Amazon Redshift.

    > **Note**
    >
    > Al crear su red ODB, Oracle Database@ preconfigura AWS automáticamente el acceso a la red para las copias de seguridad gestionadas por Oracle en Amazon S3. No puede activar ni desactivar esta integración. Para obtener más información, consulte AWS integraciones de servicios.

11. (Opcional) En el caso de las etiquetas, introduce hasta 50 etiquetas para la red. Una etiqueta es un par clave-valor que puede utilizar para organizar y realizar un seguimiento de sus recursos.
12. Elija Crear red ODB.

Después de crear una red ODB, puede sincronizarla con una VPC. El peering ODB es una conexión de red creada por el usuario que permite enrutar el tráfico de forma privada entre una Amazon VPC y una red ODB. Tras la interconexión, una EC2 instancia de Amazon dentro de la VPC puede comunicarse con los recursos de la red ODB como si estuvieran dentro de la misma red. Para obtener más información, consulte Configuración del emparejamiento de ODB a una Amazon VPC en Oracle Database@AWS.

Paso 2: Cree una infraestructura de Oracle Exadata en Oracle Database@AWS

La infraestructura Oracle Exadata es la arquitectura subyacente de los servidores de bases de datos, los servidores de almacenamiento y las redes que ejecutan las bases de datos Oracle Exadata. Elija Exadata X9M o X11M como modelo de sistema. A continuación, puede crear clústeres de máquinas virtuales en la infraestructura de Exadata mediante la consola. AWS

Puede crear la infraestructura de Oracle Exadata y la red ODB en cualquier orden. No es necesario especificar la información de la red al crear la infraestructura.

No puede modificar una infraestructura de Oracle Exadata después de crearla. Para eliminar una infraestructura de Exadata, consulte. Eliminar una infraestructura de Oracle Exadata en Oracle Database@AWS

Para crear una infraestructura de Exadata

1. Inicie sesión en Consola de administración de AWS y abra la Oracle Database@AWS consola en. https://console.aws.amazon.com/odb/
2. En el panel izquierdo, elija Exadata infrastructure.
3. Elija Crear infraestructura de Exadata.
4. Para el nombre de la infraestructura de Exadata, introduzca un nombre. El nombre debe tener entre 1 y 255 caracteres y empezar por un carácter alfabético o un guión bajo. No puede contener guiones consecutivos.
5. Para la zona de disponibilidad, elija una de las compatibles. AZs A continuación, elija Siguiente.
6. Para el modelo de sistema Exadata, elija Exadata.X9M o Exadata.X11M. Para Exadata.X11M, elija también los siguientes tipos de servidores:
   - Para el tipo de servidor de base de datos, elija el tipo de modelo de servidor de base de datos de su infraestructura de Exadata. Actualmente, la única opción es el X11M.
   - Para el tipo de servidor de almacenamiento, elija el tipo de modelo de servidor de almacenamiento de su infraestructura de Exadata. Actualmente, la única opción es el X11M-HC.
7. Para los servidores de bases de datos, deje el valor predeterminado de 2 o mueva el control deslizante para seleccionar un máximo de 32 servidores. Para especificar más de 2, solicite a OCI un aumento del límite.

Cada servidor de base de datos Exadata X9M admite 126. OCPUs Cada servidor de bases de datos Exadata X11M admite 760. ECPUs El recuento total de cómputos cambia a medida que se cambia la cantidad de servidores. Para obtener más información OCPUs y ECPUs, consulte los modelos de cálculo en Autonomous Database en la documentación de Oracle.

8. Para los servidores de almacenamiento, deje el valor predeterminado de 3 o mueva el control deslizante para seleccionar un máximo de 64 servidores. Para especificar más de 3, solicite a OCI un aumento del límite. Cada servidor de almacenamiento X9M proporciona 64 TB. Cada servidor de almacenamiento X11m proporciona 80 TB. El total de TB de almacenamiento cambia a medida que se cambia la cantidad de servidores. A continuación, elija Siguiente.
9. En la ventana de mantenimiento, configure cuándo se puede realizar el mantenimiento del sistema:

   a. En la preferencia de programación, seleccione una de las siguientes opciones:

      - Programa gestionado por Oracle: Oracle determina el momento óptimo para las actividades de mantenimiento.
      - Programación gestionada por el cliente: usted especifica cuándo pueden realizarse las actividades de mantenimiento.

   b. Para el modo de aplicación de parches, seleccione una de las siguientes opciones:

      - Continuamente: las actualizaciones se aplican a un nodo a la vez, lo que permite que la base de datos permanezca disponible durante la aplicación de parches.
      - De forma continua: las actualizaciones se aplican a todos los nodos simultáneamente, lo que puede requerir un tiempo de inactividad.

   c. Si seleccionó un programa gestionado por el cliente, configure los siguientes ajustes adicionales:

      - Para los meses de mantenimiento, seleccione los meses en los que se puede realizar el mantenimiento.
      - En Semana del mes, seleccione la semana del mes en que se puede realizar el mantenimiento (primera, segunda, tercera, cuarta o última).
      - En Día de la semana, seleccione el día en que se puede realizar el mantenimiento (de lunes a domingo).
      - En Hora de inicio, seleccione la hora en la que comienza el período de mantenimiento. La hora está en UTC.

- En el apartado Plazo de entrega de las notificaciones, selecciona con cuántos días de antelación quieres que te notifiquen las próximas tareas de mantenimiento.

> **Note**
>
> Oracle Cloud Infrastructure realiza el mantenimiento del sistema durante este período. Durante el mantenimiento, su infraestructura de Exadata permanece disponible, pero es posible que experimente breves períodos de mayor latencia.

10. (Opcional) Para los contactos de notificación de mantenimiento de OCI, introduzca hasta 10 direcciones de correo electrónico. AWS reenvía estas direcciones de correo electrónico a OCI. Cuando se producen actualizaciones, la OCI envía notificaciones por correo a las direcciones indicadas.
11. (Opcional) En el caso de las etiquetas, introduzca hasta 50 etiquetas para la infraestructura. Una etiqueta es un par clave-valor que puede utilizar para organizar y realizar un seguimiento de sus recursos.
12. Seleccione Siguiente y revise la configuración de su infraestructura.
13. Elija Crear infraestructura de Exadata.

Paso 3: Cree un clúster de máquinas virtuales de Exadata o un clúster de máquinas virtuales autónomas en Oracle Database@AWS

Un clúster de máquinas virtuales de Exadata es un conjunto VMs en el que puede crear bases de datos Oracle Exadata. Los clústeres de máquinas virtuales se crean en la infraestructura de Exadata. Puede implementar varios clústeres de máquinas virtuales con diferentes infraestructuras de Oracle Exadata en la misma red ODB. Tiene el control administrativo total sobre las bases de datos que crea en los clústeres de máquinas virtuales de Exadata.

Un clúster de máquinas virtuales autónomas es un conjunto preasignado de recursos informáticos y de almacenamiento de Oracle Exadata, virtualizado a nivel de máquina virtual, que ejecuta bases de datos autónomas (ADB). A diferencia de las bases de datos administradas por el usuario que se crean en un clúster de máquinas virtuales de Exadata, las bases de datos autónomas se ajustan y parchean automáticamente y son gestionadas por Oracle y no por un administrador de bases de datos.

Tenga en cuenta las siguientes limitaciones al crear clústeres de máquinas virtuales:

- Puede implementar un clúster de máquinas virtuales solo en la zona de disponibilidad en la que creó la red ODB y la infraestructura de Oracle Exadata.
- Si no comparte un clúster de máquinas virtuales entre cuentas, debe estar en la Cuenta de AWS misma infraestructura que la de Oracle Exadata. Si suele AWS RAM compartir una red ODB y una infraestructura de Oracle Exadata desde una AWS cuenta con una cuenta de confianza, la cuenta de confianza puede crear clústeres de máquinas virtuales en su propia cuenta.
- Solo puede implementar clústeres de máquinas virtuales en su red ODB. No se permiten otros recursos.
- No puede cambiar la asignación de almacenamiento después de crear un clúster de máquinas virtuales.

> **Important**
>
> El proceso de creación puede tardar más de 6 horas, según el tamaño del clúster de máquinas virtuales.

Exadata VM cluster

Para crear un clúster de máquinas virtuales de Exadata

1. Inicie sesión en Consola de administración de AWS y abra la Oracle Database@AWS consola en. https://console.aws.amazon.com/odb/
2. En el panel izquierdo, elija los clústeres de máquinas virtuales de Exadata.
3. Elija Crear clúster de máquinas virtuales.
4. Para el nombre del clúster de máquinas virtuales, introduce un nombre. El nombre debe tener entre 1 y 255 caracteres y empezar por un carácter alfabético o un guión bajo. No puede contener guiones consecutivos.
5. (Opcional) En el nombre del clúster de Grid Infrastructure, introduzca una versión de infraestructura de Grid para el clúster de máquinas virtuales que coincida con la versión de Oracle Database que esté utilizando. El nombre debe tener entre 1 y 11 caracteres y no puede contener guiones.
6. En Zona horaria, introduce una zona horaria.

7. Para ver las opciones de licencia, elija Bring Your Own License (BYOL) o License Included y, a continuación, elija Siguiente. Esta licencia es la licencia OCI proporcionada por Oracle, no una licencia proporcionada por. AWS
8. Configure los ajustes de infraestructura de Exadata de la siguiente manera:

   a. Para Infraestructura, elija lo siguiente:

      - Para el nombre de la infraestructura de Exadata, elija la infraestructura que se utilizará para este clúster de máquinas virtuales.
      - Para la versión Grid Infrastructure, elija la versión que se va a usar para este clúster de máquinas virtuales.
      - Para la versión de imagen de Exadata, elija la versión que se va a usar para este clúster de máquinas virtuales. Le recomendamos que elija la versión que se muestra, que es la versión más alta disponible.

   b. En el caso de los servidores de bases de datos, seleccione uno o más servidores de bases de datos para alojar el clúster de máquinas virtuales.

   c. Para la configuración, haga lo siguiente:

      - Elija el número de núcleos de la CPU, la memoria y el almacenamiento local para cada máquina virtual o acepte los valores predeterminados.
      - Elija la cantidad total de almacenamiento de Exadata para el clúster de máquinas virtuales o acepte la predeterminada.

   d. (Opcional) Para la asignación de almacenamiento, seleccione cualquiera de las siguientes opciones:

      - Habilite la asignación de almacenamiento para las instantáneas dispersas de Exadata
      - Habilite la asignación de almacenamiento para las copias de seguridad locales

      La asignación de almacenamiento utilizable cambia a medida que selecciona las opciones. No puedes cambiar esta asignación de almacenamiento más adelante. Revisa tu selección y, a continuación, selecciona Siguiente.

9. Configure la conectividad de la siguiente manera:

   a. Para la red ODB, elija una red ODB existente.

b. En el prefijo del nombre de host, introduzca un prefijo para el clúster de máquinas virtuales. Asegúrese de no incluir el nombre de dominio. El prefijo forma la primera parte del nombre de host del clúster de máquinas virtuales Oracle Exadata.

> **Note**
>
> El nombre de dominio del host se fija como oraclevcn.com.

c. Para el puerto de escucha SCAN (TCP/IP), introduzca un número de puerto que permita el acceso TCP al agente de escucha con nombre de acceso de cliente único (SCAN). El puerto predeterminado es 1521. O bien, puede introducir un puerto SCAN personalizado entre 1024 y 8999, excluyendo los siguientes números de puerto: 2484, 6100, 6200, 7060, 7070, 7085 y 7879. A continuación, elija Siguiente.

d. Para los pares de claves SSH, introduzca la parte de clave pública de uno o más pares de claves utilizados para el acceso SSH al clúster de máquinas virtuales. A continuación, elija Siguiente.

10. (Opcional) Elija los diagnósticos y las etiquetas de la siguiente manera:

    a. Elija si desea habilitar la recopilación de diagnósticos para las recopilaciones de eventos de diagnóstico, Health Monitor y registros y trazas de incidentes. Oracle puede utilizar esta información de diagnóstico para identificar, rastrear y resolver problemas.

    b. En el caso de las etiquetas, introduzca hasta 50 etiquetas para el clúster de máquinas virtuales. Una etiqueta es un par clave-valor que puedes usar para organizar y realizar un seguimiento de tus recursos. A continuación, elige Siguiente.

11. Revise la configuración. A continuación, selecciona Crear clúster de máquinas virtuales.

Autonomous VM cluster

Para crear un clúster de máquinas virtuales autónomas

1. Inicie sesión en Consola de administración de AWS y abra la Oracle Database@AWS consola en https://console.aws.amazon.com/odb/.
2. En el panel izquierdo, selecciona Clústeres de máquinas virtuales autónomas.
3. Elija Crear un clúster de máquinas virtuales autónomas.

4. Para el nombre del clúster de máquinas virtuales, introduzca un nombre. El nombre debe tener entre 1 y 255 caracteres y empezar por un carácter alfabético o un guión bajo. No puede contener guiones consecutivos.
5. En Zona horaria, introduce una zona horaria.
6. Para ver las opciones de licencia, elija Bring Your Own License (BYOL) o License Included y, a continuación, elija Siguiente. Esta licencia es la licencia OCI proporcionada por Oracle, no una licencia proporcionada por. AWS
7. Configure los ajustes de infraestructura de Exadata de la siguiente manera:

   a. En el nombre de la infraestructura de Exadata, elija la infraestructura que se utilizará para este clúster de máquinas virtuales autónomas.

   b. En el caso de los servidores de bases de datos, seleccione uno o más servidores de bases de datos para alojar su clúster de máquinas virtuales autónomas.

   c. Para la configuración, haga lo siguiente:

      - Elija el número de núcleos de la ECPU por máquina virtual, la memoria de la base de datos por CPU, el almacenamiento de la base de datos y el número máximo de bases de datos de contenedores autónomos o acepte los valores predeterminados.
      - Elija la cantidad total de almacenamiento de Exadata para el clúster de máquinas virtuales autónomas o acepte la predeterminada.
8. Configure la conectividad de la siguiente manera:

   a. Para la red ODB, elija una red ODB existente.

   b. Para el puerto de escucha SCAN (TCP/IP), introduzca un número de puerto para el puerto (no TLS). El puerto predeterminado es 1521. O bien, puede introducir un puerto (TLS) entre 1024 y 8999, excluyendo los siguientes números de puerto: 2484, 6100, 6200, 7060, 7070, 7085 y 7879. A continuación, elija Siguiente.

      Seleccione Habilitar la autenticación TLS mutua (mTLS) para permitir la autenticación TLS mutua.
9. (Opcional) Elija los diagnósticos y las etiquetas de la siguiente manera:

   a. Elija si desea programar la configuración de modificación según un programa gestionado por Oracle o un programa gestionado por el cliente. Si elige un programa gestionado por el cliente, defina los meses de mantenimiento, las semanas del mes, el día de la semana y la hora de inicio (UTC).

b. En el caso de las etiquetas, introduce hasta 50 etiquetas para el clúster de máquinas virtuales autónomas. Una etiqueta es un par clave-valor que puedes usar para organizar y realizar un seguimiento de tus recursos. A continuación, elige Siguiente.

10. Revise la configuración. A continuación, selecciona Crear un clúster de máquinas virtuales autónomas.

Paso 4: Cree bases de datos Oracle Exadata en Oracle Cloud Infrastructure

En Oracle Database@AWS, puede crear y administrar los siguientes recursos mediante la AWS consola, la CLI o APIs:

- Redes ODB
- Infraestructura Oracle Exadata
- Clústeres de máquinas virtuales de Exadata y clústeres de máquinas virtuales autónomas
- Conexiones de emparejamiento ODB

Para crear y gestionar las bases de datos de Oracle Exadata en la infraestructura que creó, debe utilizar la consola de Oracle Cloud Infrastructure en lugar del panel de control. Oracle Database@AWS Puede crear una base de datos de Exadata gestionada por el usuario en un clúster de máquinas virtuales de Exadata y una base de datos autónoma en un clúster de máquinas virtuales de Exadata autónomo. Para obtener información sobre la creación de bases de datos Oracle en OCI, consulte la base de datos de Exadata en la documentación de Oracle Cloud Infrastructure.

Para crear bases de datos Oracle Exadata

1. Inicie sesión en Consola de administración de AWS y abra la Oracle Database@AWS consola en. https://console.aws.amazon.com/odb/
2. En el panel izquierdo, elija clústeres de máquinas virtuales de Exadata o clústeres de máquinas virtuales autónomas.
3. Elija un clúster de máquinas virtuales para ver la página de detalles.
4. Seleccione Administrar en OCI para que se le redirija a la consola de Oracle Cloud Infrastructure.

5. Cree su base de datos Exadata gestionada por el usuario o su base de datos autónoma en OCI.

Configuración del emparejamiento de ODB a una Amazon VPC en Oracle Database@AWS

El peering ODB es una conexión de red creada por el usuario que permite enrutar el tráfico de forma privada entre una Amazon VPC y una red ODB. Existe una one-to-one relación entre una VPC y una red ODB. Después de crear una conexión de emparejamiento mediante la consola, la CLI o la API, asegúrese de actualizar las tablas de enrutamiento de la VPC y configurar la resolución de DNS. Para obtener una descripción general conceptual del emparejamiento de ODB, consulte. Emparejamiento ODB

Creación de una conexión de emparejamiento ODB en Oracle Database@AWS

Con las conexiones de emparejamiento ODB, puede establecer una conectividad de red privada entre su infraestructura de Oracle Exadata y las aplicaciones que se ejecutan en Amazon. VPCs Cada conexión de emparejamiento ODB es un recurso independiente que puede crear, ver y eliminar independientemente de la red ODB.

Al crear una conexión de emparejamiento ODB, puede especificar los rangos de CIDR de redes homólogas. Esta técnica limita el acceso de la red a las subredes requeridas, reduce los posibles objetivos de los ataques y permite una segmentación de la red más granular para cumplir con los requisitos de conformidad.

Puede crear los siguientes tipos de conexiones de emparejamiento ODB:

Emparejamiento ODB con la misma cuenta

- Puede crear una conexión de emparejamiento ODB entre una red ODB y una Amazon VPC en la misma cuenta. AWS

Emparejamiento ODB entre cuentas

- Puede crear una conexión de emparejamiento ODB entre una red ODB de una cuenta y una Amazon VPC de una cuenta diferente, después de compartir la red ODB mediante. AWS RAM Las cuentas de propietario de la VPC pueden administrar los rangos de CIDR especificados en la conexión de emparejamiento sin ser también propietarios de la red ODB.

Existe una relación 1:1 entre una VPC y una red ODB. No puede crear una conexión de emparejamiento ODB entre una VPC y varias redes ODB o entre una red ODB y varias. VPCs

Consola

1. Inicie sesión en Consola de administración de AWS y abra la consola en. Oracle Database@AWS https://console.aws.amazon.com/odb/
2. En el panel de navegación, elija conexiones de emparejamiento ODB.
3. Seleccione Crear conexión de emparejamiento ODB.
4. (Opcional) En el caso del nombre de emparejamiento de ODB, introduzca un nombre exclusivo para la conexión.
5. En el caso de la red ODB, elija la red ODB que desee realizar el emparejamiento.
6. Para la red de pares, elija Amazon VPC para sincronizarla con su red ODB.
7. (Opcional) Para la red CIDRs homóloga, especifique bloques CIDR adicionales de la VPC homóloga que puedan acceder a la red ODB. Si no lo especificas CIDRs, se permite el acceso CIDRs a todos los miembros de la VPC homóloga.
8. (Opcional) En Etiquetas, agrega un par de clave y valor.
9. Seleccione Crear conexión de emparejamiento ODB.

Tras crear una conexión de emparejamiento ODB, configure las tablas de enrutamiento de Amazon VPC para enrutar el tráfico a la red ODB interconectada. Para obtener más información, consulte Configuración de tablas de enrutamiento de VPC para el emparejamiento de ODB. Tenga en cuenta que Oracle Database@ configura AWS automáticamente las tablas de enrutamiento de la red ODB.

AWS CLI

Para crear una conexión de emparejamiento ODB, utilice el comando. `create-odb-peering-connection`

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

Para limitar el acceso a la red ODB a rangos de CIDR específicos, utilice el parámetro. `--peer-network-cidrs-to-be-added` Si no especifica los rangos de CIDR, todos los rangos tienen acceso.

```
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 ver una lista de sus conexiones de emparejamiento ODB, utilice el comando. `list-odb-peering-connections`

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

Para obtener detalles sobre una conexión de interconexión ODB específica, utilice el comando. `get-odb-peering-connection`

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

Actualización de una conexión de emparejamiento ODB

Puede actualizar una conexión de emparejamiento ODB existente para añadir o eliminar una red homóloga. CIDRs Usted controla qué subredes de la VPC homóloga tienen acceso a su red ODB.

Consola

1. Inicie sesión en Consola de administración de AWS y abra la consola en Oracle Database@AWS . https://console.aws.amazon.com/odb/
2. En el panel de navegación, elija conexiones de emparejamiento ODB.
3. Seleccione la conexión de emparejamiento ODB que desee actualizar.
4. Elija Acciones y, a continuación, elija Actualizar conexión de emparejamiento.
5. En la CIDRs sección Red de pares, agrega o elimina los bloques CIDR según sea necesario:
   - Para añadirlos CIDRs, selecciona Añadir CIDR e introduce el bloque CIDR.
   - Para eliminarlo CIDRs, selecciona la X situada junto al bloque CIDR que deseas eliminar.
6. Selecciona Actualizar conexión de emparejamiento.

AWS CLI

Para añadir una red CIDRs homóloga a una conexión de interconexión ODB, especifique el parámetro `--peer-network-cidrs-to-be-added` en el 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 eliminar la red CIDRs homóloga de una conexión de interconexión ODB, especifique el parámetro `--peer-network-cidrs-to-be-removed` en el 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"
```

Configuración de tablas de enrutamiento de VPC para el emparejamiento de ODB

Las tablas de enrutamiento contienen conjuntos de reglas, denominadas rutas, que determinan adónde se dirige el tráfico de red desde la subred o puerta de enlace. El CIDR de destino de una tabla de enrutamiento es un rango de direcciones IP al que desea que vaya el tráfico. Si especificó una VPC para el emparejamiento de ODB con la red de ODB, actualice la tabla de enrutamiento de la VPC con el rango de IP de destino de la red de ODB. Para obtener más información sobre el emparejamiento de ODB, consulte. Emparejamiento ODB

Para actualizar una tabla de rutas, utilice el AWS CLI `ec2 create-route` comando. Los siguientes ejemplos actualizan las tablas de enrutamiento de Amazon VPC. Para obtener más información, consulte Configuración de tablas de enrutamiento de VPC para el emparejamiento 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
```

Las tablas de enrutamiento de red ODB se actualizan automáticamente con la VPC CIDRs. Para permitir el acceso a la red ODB solo para una subred específica CIDRs en CIDRs lugar de para todas las de la VPC, puede especificar la red del mismo nivel CIDRs al crear una conexión de emparejamiento ODB o actualizar una conexión de emparejamiento ODB existente para agregar o eliminar rangos de CIDR emparejados. Para obtener más información, consulte Creación de una conexión de emparejamiento ODB en Oracle Database@AWS y Actualización de una conexión de emparejamiento ODB.

Para obtener más información sobre las tablas de enrutamiento de VPC, consulte Tablas de enrutamiento de subred en la Guía del usuario de Amazon Virtual Private Cloud y ec2 create-route en la Referencia de comandos.AWS CLI

Configuración de DNS para Oracle Database@AWS

Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad que puede utilizar para el enrutamiento de DNS. Al crear una conexión de emparejamiento de ODB entre la red de ODB y una VPC, se necesita un mecanismo para resolver las consultas de DNS para los recursos de la red de ODB desde la VPC. Puede usar Amazon Route 53 para configurar los siguientes recursos:

- Un punto final de salida

  El punto final es necesario para enviar consultas de DNS a la red ODB.
- Una regla de resolución

  Esta regla especifica el nombre de dominio de las consultas de DNS que el solucionador de Route 53 reenvía al DNS de la red ODB.

Cómo funciona el DNS en Oracle Database@AWS

Oracle Database@AWS administra automáticamente la configuración del Sistema de nombres de dominio (DNS) para la red ODB. Para el nombre de dominio, puede especificar un prefijo personalizado para el nombre de dominio predeterminado `oraclevcn.com` o un nombre de dominio totalmente personalizado. Para obtener más información, consulte Paso 1: Cree una red ODB en Oracle Database@AWS.

Cuando Oracle Database@AWS aprovisiona una red ODB, crea los siguientes recursos:

- Una red de nube virtual (VCN) de Oracle Cloud Infrastructure (OCI) con los mismos bloques de CIDR que la red ODB

  Este VCN reside en el arrendamiento de OCI vinculado del cliente. Existe un mapeo 1:1 entre una red ODB y una OCI VCN. Cada red ODB está asociada a una OCI VCN.
- Un solucionador de DNS privado dentro de la OCI VCN

  Este solucionador de DNS gestiona las consultas de DNS dentro de la OCI VCN. La automatización de OCI crea registros para el clúster de máquinas virtuales. Los escaneos utilizan el nombre de dominio `*.oraclevcn.com` completo (FQDN).
- Un punto final de escucha de DNS dentro de la OCI VCN para el solucionador de DNS privado

  Puede encontrar el terminal de escucha de DNS en la página de detalles de la red ODB de la consola. Oracle Database@AWS

Configurar un punto final de salida en una red ODB en Oracle Database@AWS

Un punto final saliente permite enviar consultas de DNS desde la VPC a una dirección de red o IP. El punto final especifica las direcciones IP desde las que se originan las consultas. Para reenviar las consultas de DNS desde la VPC a la red de ODB, cree un punto final saliente mediante la consola Route 53. Para obtener más información, consulte Reenviar consultas DNS salientes a la red.

Para configurar un punto final saliente en una red ODB

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en https://console.aws.amazon.com/route53/.
2. En el panel izquierdo, selecciona Outbound Endpoints.
3. En la barra de navegación, elija la región de la VPC en la que desee crear el punto final de salida.
4. Elija Create outbound endpoint (Crear punto de conexión de salida).
5. Complete la sección Configuración general del punto final saliente de la siguiente manera:

   a. Elija un grupo de seguridad que permita la conectividad TCP y UDP saliente con lo siguiente:

      - Direcciones IP que los solucionadores utilizan para las consultas de DNS en su red ODB

- Puertos que los resolutores utilizan para las consultas de DNS en la red ODB

b. En Endpoint Type (Tipo de punto de enlace), seleccione IPv4.

c. Para los protocolos de este punto final, elija Do53.

6. En las direcciones IP, proporcione la siguiente información:

- Especifique las direcciones IP o deje que el Route 53 Resolver elija las direcciones IP por usted entre las direcciones disponibles en la subred. Elija entre un mínimo de 2 y un máximo de 6 direcciones IP para las consultas de DNS. Le recomendamos que elija direcciones IP en al menos dos zonas de disponibilidad diferentes.
- En Subred, elija subredes que tengan lo siguiente:
  - Tablas de rutas que incluyen rutas a las direcciones IP del agente de escucha de DNS en la red ODB
  - Listas de control de acceso a la red (ACLs) que permiten el tráfico UDP y TCP a las direcciones IP y los puertos que utilizan los solucionadores para las consultas de DNS en la red ODB
  - Red ACLs que permite el tráfico de los resolutores en el rango de puertos de destino entre 1024 y 65535

7. (Opcional) En el caso de las etiquetas, especifique las etiquetas del punto final.

8. Seleccione Enviar.

Configurar una regla de resolución en Oracle Database@AWS

Una regla de resolución es un conjunto de criterios que determina cómo enrutar las consultas de DNS. Reutilice o cree una regla que especifique el nombre de dominio de las consultas de DNS que el solucionador reenvía al DNS de la red ODB.

Uso de una regla de resolución existente

Para usar una regla de resolución existente, la acción depende del tipo de regla:

Una regla para el mismo dominio en la misma AWS región que la VPC de su Cuenta de AWS

Asocie la regla a su VPC en lugar de crear una nueva regla. Elija la regla en el panel de reglas y asóciela a la que sea aplicable VPCs en la AWS región.

Una regla para el mismo dominio en la misma región que tu VPC, pero en una cuenta diferente

Se usa AWS Resource Access Manager para compartir la regla de la cuenta remota a la suya. Cuando compartes una regla, también compartes el punto final de salida correspondiente. Después de compartir la regla con su cuenta, selecciónela en el panel de reglas y asóciela a la VPCs de su cuenta. Para obtener más información, consulta Administrar las reglas de reenvío.

Crear una nueva regla de resolución

Si no puede volver a utilizar una regla de resolución existente, cree una nueva con la consola de Amazon Route 53.

Para crear una nueva regla de resolución

1. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en https://console.aws.amazon.com/route53/.
2. En el panel izquierdo, selecciona Reglas.
3. En la barra de navegación, elija la región de la VPC en la que se encuentra el punto final de salida.
4. Seleccione Creación de regla.
5. Complete las secciones de la regla para el tráfico saliente de la siguiente manera:
   a. En Tipo de regla, elija Regla de reenvío.
   b. En Nombre de dominio, especifique el nombre de dominio completo de la red ODB.
   c. Para VPCs ello, utilice esta regla y asóciela a la VPC desde donde se reenvían las consultas DNS a su red ODB.
   d. Para el punto final de salida, elija el punto de enlace de salida en el que lo creó. Configurar un punto final de salida en una red ODB en Oracle Database@AWS

   > **Note**
   >
   > La VPC asociada a esta regla no necesita ser la misma VPC en la que creó el punto final saliente.

6. Complete la sección de direcciones IP de destino de la siguiente manera:
   a. Para la dirección IP, especifique la dirección IP de la IP del receptor de DNS en su red ODB.

b. En Puerto, especifique 53. Este es el puerto que utiliza la resolución para las consultas de DNS.

> **Note**
>
> El Route 53 Resolver reenvía las consultas de DNS que cumplen con esta regla y se originan en una VPC asociada a esta regla al punto final de salida al que se hace referencia. Estas consultas se reenvían a las direcciones IP de destino que especifique en las direcciones IP de destino.

c. Para el protocolo de transmisión, elija Do53.

7. (Opcional) En el caso de las etiquetas, especifique las etiquetas de la regla.
8. Seleccione Enviar.

Probar la configuración de DNS en Oracle Database@AWS

Después de crear el punto final de salida y la regla de resolución, compruebe que el DNS se resuelve correctamente. Con una EC2 instancia de Amazon en la VPC de la aplicación, realice una resolución de DNS de la siguiente manera:

Para Linux o macOS

Use un comando del formulario`dig` *`record-name record-type`*.

Para Windows

Use un comando del formulario`nslookup -type=`*`record-name record-type`*.

Configuración de Amazon VPC Transit Gateways para Oracle Database@AWS

Amazon VPC Transit Gateways es un centro de tránsito de red que interconecta nubes privadas virtuales (VPCs) y redes locales. Cada VPC de la hub-and-spoke arquitectura puede conectarse a la pasarela de tránsito para acceder a otras VPC conectadas. VPCs AWS Transit Gateway admite el tráfico tanto para como para IPv4 . IPv6

En Oracle Database@AWS, una red ODB admite una conexión de emparejamiento a una sola VPC. Si conecta una puerta de enlace de tránsito a una VPC que está interconectada a una red ODB,

puede conectar varias VPCs a esta puerta de enlace. Las aplicaciones que se ejecutan en estas diferentes máquinas VPCs pueden acceder a un clúster de máquinas virtuales de Exadata que se ejecute en su red ODB.

El siguiente diagrama muestra una puerta de enlace de tránsito que está conectada a dos redes locales VPCs y a una red local.

En el diagrama anterior, una VPC está conectada a una red ODB. En esta configuración, la red ODB puede enrutar el tráfico a todas las personas VPCs conectadas a la puerta de enlace de tránsito. La tabla de enrutamiento de cada VPC incluye tanto la ruta local como las rutas que envían el tráfico destinado a la red ODB a la pasarela de tránsito.

En AWS Transit Gateway, se te cobra por la cantidad de conexiones que realices a la pasarela de tránsito por hora y por la cantidad de tráfico que fluye. AWS Transit Gateway Para obtener información sobre los costos, consulta AWS Transit Gateway los precios.

Requisitos

Asegúrese de que su Oracle Database@AWS entorno cumpla los siguientes requisitos:

- La VPC que está conectada a la red ODB debe estar en la misma. Cuenta de AWS Si la VPC interconectada se encuentra en una cuenta diferente a la de la red ODB, los adjuntos de la puerta de enlace de tránsito fallan independientemente de las configuraciones de uso compartido.
- La VPC que está conectada a la red ODB debe tener un adjunto de puerta de enlace de tránsito.

> **Note**
>
> Si la puerta de enlace de tránsito está configurada para compartir, puede residir en cualquier cuenta. Por lo tanto, la puerta de enlace en sí misma no necesita estar en la misma cuenta que la red de VPC y ODB.

- El adjunto de la puerta de enlace de tránsito debe estar en la misma zona de disponibilidad (AZ) que la red ODB.

Limitaciones

Tenga en cuenta las siguientes limitaciones de Amazon VPC Transit Gateways para: Oracle Database@AWS

- Amazon VPC Transit Gateways no ofrece una integración nativa para usar una red ODB como adjunto. Por lo tanto, las funciones de VPC como las siguientes no están disponibles:
  - Resolución de nombres de host DNS públicos a direcciones IP privadas
  - Notificación de eventos sobre cambios en la topología de la red ODB, el enrutamiento y el estado de la conexión
- No se admite el tráfico de multidifusión a la red ODB.

Instalación y configuración de una puerta de enlace de tránsito

Puede crear y configurar una pasarela de tránsito mediante la consola o `aws ec2` los comandos de Amazon VPC. El siguiente procedimiento supone que no tiene una red ODB enlazada a una VPC en su. Cuenta de AWS Si una red ODB y una VPC ya están emparejadas en su cuenta, omita los pasos 1 a 3.

> **Note**
>
> Si adjunta o vuelve a conectar los archivos adjuntos a la VPC, asegúrese de volver a introducir los rangos CIDR en la red ODB ODB.

Para instalar y configurar una puerta de enlace de tránsito para Oracle Database@AWS

1. Cree una red ODB. Para obtener más información, consulte Paso 1: Cree una red ODB en Oracle Database@AWS.
2. Cree una VPC con la misma cuenta que contiene la red ODB. Para obtener más información, consulte Crear una VPC en la Guía del usuario de Amazon VPC.
3. Cree una conexión de emparejamiento ODB entre la red ODB y la VPC. Para obtener más información, consulte Configuración del emparejamiento de ODB a una Amazon VPC en Oracle Database@AWS.
4. Configure una pasarela de tránsito siguiendo los pasos que se indican en Cómo empezar a utilizar las pasarelas de tránsito de Amazon VPC. La puerta de enlace debe estar en la Cuenta de AWS misma posición que la red ODB y la VPC, o bien debe estar compartida por otra cuenta.

> **Important**
>
> Cree el adjunto de la pasarela de tránsito en la misma zona de disponibilidad que la red ODB.

5. Agregue rangos CIDR a su red ODB para las redes locales VPCs y locales que planea conectar a su red principal. Para obtener más información, consulte Actualizar una red ODB en Oracle Database@AWS.

   Si utiliza la CLI, ejecute el comando `update-odb-network` con `--peered-cidrs-to-be-added` y`--peered-cidrs-to-be-removed`. Para obtener más información, consulte la Referencia de comandos de la AWS CLI.

Configuración de AWS Cloud WAN para Oracle Database@AWS

AWS Cloud WAN es un servicio de redes de área amplia (WAN) gestionado. Puedes usar AWS Cloud WAN para crear, administrar y monitorear una red global unificada que conecte los recursos que se ejecutan en tus entornos de nube y locales.

En AWS Cloud WAN, una red global es una red privada única que actúa como contenedor de alto nivel para los objetos de la red. Una red principal es la parte de la red global gestionada por AWS.

AWS La WAN en la nube ofrece las siguientes ventajas clave:

- Administración de red centralizada que simplifica las operaciones y, al mismo tiempo, mantiene la seguridad en varias regiones
- Redes principales con segmentación integrada para aislar el tráfico a través de varios dominios de enrutamiento
- Support para políticas para automatizar la administración de la red y definir configuraciones consistentes en toda su red global

En Oracle Database@AWS, una red ODB admite el emparejamiento a una sola VPC. Si conectas una red principal de AWS Cloud WAN a una VPC interconectada, se habilita el enrutamiento del tráfico global. Las aplicaciones conectadas a varias VPCs regiones pueden acceder a los clústeres de máquinas virtuales de Exadata en su red ODB. Puede aislar el tráfico de la red ODB en su propio segmento o permitir el acceso a otros segmentos.

En el siguiente diagrama, se muestra una red principal de AWS Cloud WAN que está conectada a tres redes locales VPCs y a una red local.

AWS Cloud WAN no ofrece una integración nativa para usar una red ODB como adjunto. Por lo tanto, las funciones de VPC como las siguientes no están disponibles:

- Resolución de nombres de host DNS públicos a direcciones IP privadas
- Notificación de eventos sobre cambios en la topología de la red ODB, el enrutamiento y el estado de la conexión

En AWS Cloud WAN, se te cobra por hora lo siguiente:

- Número de regiones (ejes de la red principal)
- Número de conexiones de la red principal
- La cantidad de tráfico que fluye a través de la red principal a través de los archivos adjuntos

Para obtener información detallada sobre los precios, consulta los precios de AWS Cloud WAN.

Para configurar una red principal para Oracle Database@AWS

1. Agregue rangos de CIDR a su red ODB para las redes locales VPCs y las redes locales que planea conectar a su red principal. Para obtener más información, consulte Actualizar una red ODB en Oracle Database@AWS.

   > **Note**
   >
   > Si adjunta o vuelve a conectar los archivos adjuntos a la VPC, asegúrese de volver a introducir los rangos CIDR en la red ODB ODB.

2. Siga los pasos que se indican en Crear una red global y una red central WAN AWS en la nube.

Distribución de derechos en Oracle Database@AWS

Con Oracle Database@AWS, puede compartir los derechos de AWS Marketplace para Oracle Database@AWS en la misma organización. Cuentas de AWS AWS Esto permite a otras cuentas aprovisionar su propia infraestructura de Oracle Exadata y sus propios recursos de red ODB mediante su suscripción.

Métodos de uso compartido

Oracle Database@AWS admite dos métodos de uso compartido:

Uso compartido de derechos con License Manager AWS

- Otorgue a otras cuentas la posibilidad de aprovisionar su propia infraestructura de Oracle Exadata y sus propios recursos de red ODB
- Cada cuenta funciona de forma independiente con un control total del ciclo de vida de los recursos
- Lo mejor para permitir el aprovisionamiento de autoservicio en todos los equipos o unidades de negocio

Uso compartido de recursos con AWS Resource Access Manager ()AWS RAM

- Comparta la infraestructura Oracle Exadata y los recursos de red ODB ya aprovisionados
- Centralice la administración de la infraestructura y permita que las cuentas de los destinatarios creen clústeres de máquinas virtuales
- Optimice los costos haciendo que varias cuentas usen la misma infraestructura

Puede utilizar ambos métodos de uso compartido simultáneamente en función de las necesidades de su organización.

Limitaciones del reparto de derechos de Oracle Database@AWS

Al compartir los AWS derechos de Oracle Database@, tenga en cuenta las siguientes limitaciones:

- Solo puede compartir con miembros de su organización Cuentas de AWS AWS

- No puedes compartir con una unidad organizativa (OU) completa ni con toda la organización
- Una cuenta solo puede recibir derechos de una cuenta de comprador (de una oferta privada)
- Una cuenta de comprador no puede compartir los derechos con otra cuenta de comprador
- Las cuentas de los destinatarios deben inicializar el AWS servicio Oracle Database@ antes de poder utilizar el derecho compartido
- Las operaciones de concesión de derechos solo se pueden realizar desde la región EE. UU. Este (Virginia del Norte)

Compartir los AWS derechos de Oracle Database@ entre cuentas

Para permitir la colaboración y, al mismo tiempo, optimizar los costes, comparta los AWS derechos de Oracle Database@ con otras personas de la misma organización. Cuentas de AWS AWS En este tema se explica cómo compartir derechos mediante AWS License Manager.

Requisitos previos para compartir derechos

Antes de compartir los AWS derechos de Oracle Database@, asegúrese de tener lo siguiente:

- Una AWS suscripción activa a Oracle Database@ (debe ser la cuenta del comprador que aceptó la oferta privada) AWS Marketplace
- La IDs de las AWS cuentas de su organización con las que desea compartir los derechos
- Permisos necesarios para que el otorgante y el concesionario utilicen los recursos y las operaciones del AWS License Manager (para obtener más información, consulte Administración de identidad y acceso para License Manager en la Guía del usuario de License ManagerAWS)
- Los permisos para usted (otorgante) y el destinatario del derecho (concesionario) se enumeran a continuación

Se requieren permisos para compartir los derechos

Además de los permisos AWS de License Manager, Oracle Database@AWS requiere los siguientes permisos:

Permisos del otorgante

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

- `odb:DeleteGrantShare`

Permisos del concesionario

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

Compartir los AWS derechos de Oracle Database@ con otra cuenta mediante License Manager AWS

Para compartir derechos con otra AWS cuenta, debe crear una concesión mediante AWS License Manager. Para obtener más información, consulte Distribuir los derechos de License Manager en la Guía del usuario de AWS License Manager.

Tras crear la concesión, el destinatario (beneficiario) debe:

- Aceptar y activar la subvención. Para obtener más información, consulte Conceder la aceptación y activación en License Manager en la Guía del usuario de AWS License Manager.
- Siga las instrucciones de inicialización de Oracle AWS Database@.

Una vez completada la inicialización, el concesionario puede aprovisionar los recursos de Oracle AWS Database@ mediante el derecho compartido.

Uso compartido de recursos en Oracle Database@AWS

Con Oracle Database@AWS, puede compartir la infraestructura de Exadata y su red ODB entre varios miembros de la misma organización. Cuentas de AWS AWS Podrá aprovisionar la infraestructura una sola vez y reutilizarla en cuentas de confianza, lo que le permite reducir los costos y separar las responsabilidades.

Al compartir recursos:

- La cuenta propietaria del recurso (cuenta de propietario) mantiene el control sobre el ciclo de vida del recurso.
- Las cuentas que reciben acceso a recursos compartidos (cuentas de confianza) pueden ver y usar estos recursos en función de los permisos otorgados.
- Las cuentas de confianza pueden crear sus propios recursos en una infraestructura compartida, pero no pueden eliminar los recursos compartidos subyacentes.

Integración de Oracle Database@AWS con AWS RAM

Oracle Database@AWS utiliza AWS Resource Access Manager (AWS RAM) para permitir el intercambio seguro y controlado de los recursos entre las cuentas. Con él AWS RAM, puede compartir de forma segura sus AWS recursos de Oracle Database@ entre varias AWS cuentas de la misma organización. AWS AWS RAM simplifica el intercambio de recursos, reduce los gastos operativos y proporciona seguridad y visibilidad de los recursos compartidos de Oracle Database@.AWS

Con AWS RAM, puede compartir los recursos de su propiedad mediante la creación de un recurso compartido. Un recurso compartido especifica los recursos que se van a compartir y Cuentas de AWS con quién se van a compartir.

Ventajas del uso compartido de recursos en Oracle Database@AWS

Compartir los AWS recursos de Oracle Database@ entre cuentas ofrece los siguientes beneficios:

- Optimización de costos: aprovisione la costosa infraestructura de Exadata una sola vez a través de una cuenta administrativa y compártala con varias cuentas, lo que reduce los costos generales.

- Separación de responsabilidades: mantenga límites claros entre los administradores de la infraestructura y los usuarios de las bases de datos y, al mismo tiempo, permita la colaboración.
- Administración simplificada: centralice el aprovisionamiento y la administración de la infraestructura y, al mismo tiempo, permita las operaciones de bases de datos distribuidas.
- Gobierno coherente: aplique políticas y controles coherentes en todos los recursos compartidos.

Por ejemplo, un administrador puede aprovisionar la infraestructura de Oracle Exadata y la red ODB en sus cuentas Cuenta de AWS y compartirlas con las de los desarrolladores. De este modo, los desarrolladores pueden crear clústeres de máquinas virtuales en esta infraestructura compartida sin necesidad de aprovisionar su costoso hardware. Este enfoque reduce significativamente los costos y, al mismo tiempo, mantiene una separación adecuada de responsabilidades entre las cuentas.

Cómo funciona el intercambio de recursos en Oracle Database@AWS

Puede compartir los siguientes recursos de Oracle AWS Database@:

- Infraestructura Oracle Exadata
- Red ODB

Oracle Database@AWS comparte los recursos anteriores mediante el siguiente proceso:

1. La cuenta del comprador (la cuenta que acepta la oferta AWS privada de Oracle Database@ a través de AWS Marketplace) aprovisiona los AWS recursos de Oracle Database@, como la infraestructura de Exadata y una red ODB.
2. La cuenta del comprador crea un recurso compartido especificando los recursos que se van AWS RAM a compartir y las cuentas de confianza con las que se van a compartir.
3. Los recursos compartidos de las cuentas de confianza de la misma organización se aceptan automáticamente.
4. Antes de utilizar los recursos compartidos, las cuentas de confianza deben inicializar el AWS servicio Oracle Database@ en su cuenta mediante el `aws odb initialize-service` comando o seleccionando Activar cuenta en la consola Oracle Database@.AWS
5. Tras la inicialización, las cuentas de confianza pueden crear sus propios recursos en la infraestructura compartida, como clústeres de máquinas virtuales en la infraestructura compartida de Exadata y en la red ODB.

Permisos sobre recursos compartidos para cuentas de confianza

Al compartir recursos, Oracle Database@ selecciona AWS automáticamente acciones específicas (permisos gestionados) para cada tipo de recurso:

Para la infraestructura de Exadata

Oracle Database@AWS concede los siguientes permisos a las cuentas de confianza:

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

Para la red ODB

Se conceden los siguientes permisos a las cuentas de confianza:

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

El intercambio de recursos respeta la naturaleza jerárquica de los recursos de Oracle Database@AWS . Por ejemplo, si comparte la infraestructura de Exadata, las cuentas de confianza pueden crear clústeres de máquinas virtuales en esta infraestructura, pero no pueden modificar ni eliminar la propia infraestructura de Exadata.

Cuando un recurso no se comparte, las cuentas de confianza pierden la capacidad de crear nuevos recursos en la infraestructura compartida. Sin embargo, todos los recursos que ya hayan creado siguen siendo accesibles y funcionales.

Limitaciones del uso compartido de recursos de Oracle Database@AWS

Antes de compartir recursos, tenga en cuenta las siguientes limitaciones.

Limitaciones para compartir recursos

Al compartir los AWS recursos de Oracle Database@, tenga en cuenta las siguientes limitaciones:

- Solo puede compartir recursos con. Cuenta de AWS IDs
- Solo puedes compartir recursos Cuentas de AWS dentro de la misma AWS organización.
- Compartes los recursos dentro de una AWS región específica. Para compartir recursos entre regiones, debe crear recursos compartidos independientes en cada región.
- Al crear un recurso compartido, las acciones (permisos gestionados) de cada tipo de recurso se seleccionan automáticamente y no se pueden modificar.
- No puede utilizar Oracle Database@AWS como recurso y compartirlo con otros. Cuentas de AWS
- Una cuenta de confianza solo puede usar los recursos compartidos de una cuenta de comprador (de una oferta privada). Por lo tanto, dos cuentas de comprador no pueden compartir recursos con la misma cuenta de confianza.
- Una cuenta de comprador no puede compartir recursos con otra cuenta de comprador.
- Los recursos compartidos con una cuenta de confianza deben compartirlos primero con la cuenta del comprador en la región de origen del comprador.
- Cuando dejes de compartir un recurso, te recomendamos que esperes unos 15 minutos antes de volver a compartir el mismo recurso con la misma cuenta de confianza.

Limitaciones para crear y usar recursos compartidos

Al crear o utilizar los AWS recursos de Oracle Database@, tenga en cuenta las siguientes limitaciones:

- Solo la cuenta del comprador puede crear la infraestructura de Exadata y los recursos de red ODB. La cuenta del comprador es la que acepta la oferta privada de Oracle AWS Database@.
- Las cuentas de confianza solo pueden crear recursos en la infraestructura de Exadata compartida por la cuenta del comprador.

- Las cuentas de confianza deben inicializar el AWS servicio Oracle Database@ en su cuenta antes de poder utilizar los recursos compartidos.

Limitaciones para eliminar recursos compartidos

- No puede eliminar la infraestructura de Exadata que tenga clústeres de máquinas virtuales creados por cuentas de confianza hasta que se eliminen esos clústeres de máquinas virtuales.
- No puede eliminar una red ODB que tenga una conexión de emparejamiento ODB creada por una cuenta de confianza hasta que se haya eliminado la conexión de emparejamiento ODB.
- La cuenta del comprador no puede eliminar los recursos de Oracle AWS Database@ creados por cuentas de confianza.
- Las cuentas de confianza pueden ver los recursos compartidos, pero no pueden modificar ni eliminar los AWS recursos de Oracle Database@ propiedad de la cuenta del comprador.

Compartir Oracle Database@AWS recursos entre cuentas

Para permitir la colaboración y, al mismo tiempo, optimizar los costos, comparta los AWS recursos de Oracle Database@ con otros miembros Cuentas de AWS de la misma AWS organización. En este tema se explica cómo compartir recursos mediante AWS Resource Access Manager ()AWS RAM.

Temas

Requisitos previos para compartir recursos

Antes de compartir los AWS recursos de Oracle Database@, asegúrese de disponer de lo siguiente:

- Una AWS suscripción activa a Oracle Database@ (debe ser la cuenta del comprador que aceptó la oferta privada) AWS Marketplace
- Los IDs o los nombres de los recursos que desea compartir, como la infraestructura de Exadata o las redes ODB

- Las AWS cuentas IDs de su organización con las que desea compartir recursos
- Los permisos necesarios para crear recursos compartidos en AWS RAM
- La posibilidad de compartir recursos con el AWS Organizations uso AWS RAM (para obtener más información, consulte Habilitar el uso compartido de recursos AWS Organizations en la Guía del AWS Resource Access Manager usuario)

Compartir los AWS recursos de Oracle Database@ con otra cuenta mediante AWS RAM

Para compartir una infraestructura de Exadata o una red ODB con otra AWS cuenta, cree un recurso compartido mediante. AWS RAM Esto permite que la cuenta de confianza cree clústeres de máquinas virtuales en su infraestructura de Exadata.

Consola

1. Abra la AWS RAM consola en. https://console.aws.amazon.com/ram/
2. Elija Crear recurso compartido.
3. En Nombre, introduzca un nombre descriptivo para el recurso compartido.
4. En Seleccione el tipo de recurso, elija uno de los siguientes recursos:
   - Red Oracle Database@ ODB AWS
   - Infraestructura Oracle Database@ Exadata AWS
5. Seleccione los recursos de infraestructura de Exadata que desee compartir. Elija Siguiente hasta llegar a Otorgar acceso a los directores.
6. En Directores, selecciona y Cuentas de AWS, a continuación, introduce la AWS cuenta con la IDs que quieres compartir.
7. En Permisos administrados, seleccione los siguientes permisos para permitir que la cuenta de confianza cree clústeres de máquinas virtuales en la infraestructura compartida de Exadata:
   - AWSRAMDefaultPermisoODBNetwork
   - AWSRAMDefaultPermisoODBCloudExadataInfrastructure
8. Elija Crear recurso compartido.

AWS CLI

Para compartir recursos mediante el AWS CLI, utilice el `aws ram create-resource-share` comando. En el siguiente ejemplo, se crea un recurso compartido denominado `ExadataInfraShare` que comparte la infraestructura de Exadata especificada con la cuenta 222222222222, lo que permite a esta cuenta crear clústeres de máquinas virtuales en la infraestructura compartida.

```
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
```

Visualización de sus recursos compartidos

Para ver los recursos que has compartido y las cuentas con las que los has compartido:

Consola

1. Abre la AWS RAM consola en https://console.aws.amazon.com/ram/.
2. Selecciona Recursos compartidos para ver los recursos que has compartido con otras cuentas.
3. Selecciona un recurso compartido para ver sus detalles, incluidos los recursos compartidos y las entidades con las que se comparten.

AWS CLI

Para ver tus recursos compartidos mediante el AWS CLI, usa el `get-resource-shares` comando:

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

Para ver los recursos de un recurso compartido específico, utilice el `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 los principales (cuentas) con los que se comparte un recurso compartido, utilice el `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
```

Actualizar o eliminar recursos compartidos mediante AWS RAM

Para dejar de compartir un recurso con una cuenta de confianza mediante AWS RAM, realice una de las siguientes acciones:

- Elimine el recurso del recurso compartido.
- Elimine la cuenta de confianza del recurso compartido.
- Elimine el recurso compartido.

Antes de revocar el acceso a un recurso compartido o eliminarlo, tenga en cuenta las siguientes implicaciones:

- Las cuentas de confianza ya no pueden crear nuevos recursos en la infraestructura no compartida.
- Los recursos existentes creados por cuentas de confianza en la infraestructura compartida de Exadata siguen funcionando y permanecen accesibles para ellas. Cuentas de AWS
- No puede eliminar la infraestructura de Exadata que tenga clústeres de máquinas virtuales creados por cuentas de confianza hasta que se eliminen esos clústeres de máquinas virtuales.

Antes de dejar de compartir los recursos, le recomendamos que se coordine con las cuentas de confianza para garantizar una transición fluida.

Para obtener más información, consulte Actualizar un recurso compartido AWS RAM y Eliminar un recurso compartido AWS RAM en la Guía del AWS Resource Access Manager usuario.

Inicialización Oracle Database@AWS en una cuenta de confianza

Una cuenta de confianza es aquella Cuenta de AWS que usted designa como apta para recibir recursos compartidos. Debe ser otra persona Cuenta de AWS de su AWS organización. Antes de poder utilizar los AWS recursos compartidos de Oracle Database@ en una cuenta de confianza, debe inicializar el servicio. La inicialización crea los metadatos necesarios y establece la conexión entre usted Cuenta de AWS y Oracle Cloud Infrastructure.

Temas

¿Qué es la inicialización de Oracle Database@?AWS

Después de compartir un recurso con su cuenta, debe inicializar el AWS servicio Oracle Database@ antes de poder acceder al recurso compartido o utilizarlo. Si intenta utilizar Oracle Database@AWS APIs sin inicializar primero el servicio, recibirá un error.

La inicialización es un proceso que se realiza una sola vez. Crea los metadatos necesarios y establece una conexión entre usted Cuenta de AWS y Oracle Cloud Infrastructure.

Puede inicializar el servicio mediante la consola de AWS gestión o el AWS CLI.

Consola

1. Abra la consola Oracle Database@ en AWS . https://console.aws.amazon.com/odb/
2. Si es la primera vez que accede a la AWS consola Oracle Database@ de esta cuenta, verá una página de bienvenida.
3. Seleccione Activar cuenta.
4. Comienza el proceso de inicialización del servicio. Este proceso puede tardar unos minutos en completarse.
5. Actualice la página de bienvenida periódicamente hasta que el botón Activar cuenta pase a ser el botón Panel de control.
6. Seleccione Dashboard para empezar a utilizar Oracle Database@AWS.

AWS CLI

Para inicializar Oracle Database@AWS en su cuenta de confianza mediante el, utilice el AWS CLI comando. `initialize-service`

```
aws odb initialize-service
```

Para comprobar el estado de inicialización, utilice el comando. `get-oci-onboarding-status`

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

Cuando se completa la inicialización, el resultado muestra un estado de`ACTIVE_LIMITED`, lo que indica que su cuenta puede acceder a los recursos compartidos, pero no puede crear una nueva infraestructura de Exadata o una nueva red ODB.

Siguientes pasos

Tras inicializar Oracle Database@AWS en su cuenta de confianza, puede hacer lo siguiente:

- Vea los recursos compartidos mediante los `get` comandos `list` y o en la consola. AWS
- Cree clústeres de máquinas virtuales y clústeres de máquinas virtuales autónomas en una infraestructura Exadata y una red ODB compartidas.
- Cree una conexión de emparejamiento ODB en una red ODB compartida.

Para obtener más información sobre cómo trabajar con recursos compartidos, consulte. Trabajar con Oracle Database@AWS recursos compartidos en una cuenta de confianza

Trabajar con Oracle Database@AWS recursos compartidos en una cuenta de confianza

Una vez que se haya compartido un recurso con su cuenta de confianza y haya inicializado el AWS servicio Oracle Database@, podrá ver y utilizar el recurso compartido. En este tema se explica cómo trabajar con recursos compartidos en una cuenta de confianza.

Temas

- Limitaciones de los recursos compartidos en una cuenta de confianza
- Crear clústeres de máquinas virtuales en una infraestructura compartida de Exadata
- Visualización de los recursos compartidos en una cuenta de confianza
- Configuración del emparejamiento de ODB con redes ODB compartidas

Limitaciones de los recursos compartidos en una cuenta de confianza

Cuando trabaje con AWS recursos compartidos de Oracle Database@, tenga en cuenta las siguientes limitaciones:

- El uso compartido de recursos solo se admite dentro de la misma AWS organización.
- Solo la cuenta del comprador (la cuenta que acepta la oferta AWS privada de Oracle Database@) puede crear la infraestructura de Exadata y los recursos de red ODB.
- Solo puede crear recursos en una infraestructura compartida y solo si tiene los permisos necesarios.
- Las acciones específicas (permisos administrados) de cada tipo de recurso se seleccionan automáticamente durante la creación del recurso compartido y no se pueden modificar.
- No puedes modificar ni eliminar los recursos que sean propiedad de otra cuenta.
- Los recursos que cree en una infraestructura compartida son propiedad de su cuenta y se tienen en cuenta para sus cuotas de OCI. Lo mismo se aplica a los recursos principales.
- Si la cuenta propietaria deja de compartir un recurso, ya no podrá crear nuevos recursos en esta infraestructura compartida. Sin embargo, los recursos existentes siguen funcionando.
- No se admite el uso compartido de recursos entre regiones. Solo puedes compartir recursos dentro de la misma AWS región.
- Los recursos de la cuenta de confianza se facturan al comprador de la suscripción a Oracle Database@AWS .
- Cuando utilice un recurso compartido, debe proporcionar el nombre del recurso de Amazon (ARN).

Crear clústeres de máquinas virtuales en una infraestructura compartida de Exadata

Si su cuenta de confianza tiene acceso a una infraestructura de Exadata y a una red ODB compartidas, puede crear clústeres de máquinas virtuales de Exadata, clústeres de máquinas virtuales autónomas o pares de ODB en esta infraestructura.

> **Note**
>
> Cuando utilice un recurso compartido con usted, en lugar de especificar únicamente el ID del recurso, debe especificar el nombre del recurso de Amazon (ARN).

Consola

1. Abra la consola Oracle Database@ en AWS . https://console.aws.amazon.com/odb/

2. En el panel de navegación, elija clústeres de máquinas virtuales de Exadata o clústeres de máquinas virtuales autónomas.
3. Elija Crear clúster de máquinas virtuales o Crear clúster de máquinas virtuales autónomas.
4. Para la infraestructura de Exadata, seleccione la infraestructura de Exadata compartida en la que desee crear el clúster de máquinas virtuales.
5. Complete los campos restantes según sea necesario para la configuración del clúster de máquinas virtuales.
6. Elija Crear un clúster de máquinas virtuales o Crear un clúster de máquinas virtuales autónomo.

AWS CLI

Para crear un clúster de máquinas virtuales en una infraestructura compartida de Exadata mediante el AWS CLI, utilice el `create-cloud-vm-cluster` comando:

```
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 crear un clúster de máquinas virtuales autónomo en una infraestructura compartida de Exadata mediante el AWS CLI, utilice el 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
```

El clúster de máquinas virtuales se crea en la infraestructura compartida de Exadata especificada y es propiedad de su cuenta de confianza.

Visualización de los recursos compartidos en una cuenta de confianza

Puede ver los recursos que se han compartido con su cuenta mediante la Consola AWS de administración o la AWS CLI.

Consola

1. Abra la AWS consola Oracle Database@ en. https://console.aws.amazon.com/odb/
2. En el panel de navegación, elija el tipo de recurso que desee ver: infraestructura Exadata o red ODB.
3. La consola muestra los recursos compartidos con usted.
4. Seleccione un recurso compartido para ver sus detalles.

AWS CLI

Para ver los recursos compartidos mediante el AWS CLI, utilice el `list` comando correspondiente al tipo de recurso. Por ejemplo, para enumerar la infraestructura de Exadata:

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

La respuesta muestra los recursos compartidos con usted.

Para obtener información detallada sobre un recurso compartido específico, usa el `get` comando correspondiente con el ID del recurso:

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

Configuración del emparejamiento de ODB con redes ODB compartidas

Para habilitar la comunicación entre sus aplicaciones y bases de datos en redes ODB compartidas, puede configurar el emparejamiento ODB entre su VPC y la red ODB compartida. Para obtener más información sobre el emparejamiento de ODB, consulte. Creación de una conexión de emparejamiento ODB en Oracle Database@AWS

Consola

1. Abra la consola Oracle Database@ en AWS . https://console.aws.amazon.com/odb/
2. En el panel de navegación, elija el peering de ODB.

3. Seleccione Crear emparejamiento de red ODB.
4. Para la red ODB, seleccione la red ODB compartida con la que desee realizar la interconexión.
5. Para Peer Network, seleccione su VPC.
6. Elija Crear emparejamiento de red ODB.

AWS CLI

Para crear una conexión de emparejamiento de red entre la VPC y una red ODB compartida mediante AWS CLI el, utilice el comando. `create-odb-peering-connection`

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

Tras crear la conexión de emparejamiento, actualice las tablas de enrutamiento para habilitar el tráfico entre las redes interconectadas.

```
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
```

Gestión de Oracle Database@AWS

Puede modificar y eliminar algunos Oracle Database@AWS recursos después de crearlos.

Actualizar una red ODB en Oracle Database@AWS

Puede actualizar los siguientes recursos de red ODB:

- El nombre de la red ODB
- La Amazon VPC que se utilizará para establecer una conexión de emparejamiento ODB a la red ODB
- Los rangos CIDR de VPC que pueden acceder a los recursos de Exadata en la red ODB

> **Note**
>
> Al especificar los rangos de CIDR, se limita la conectividad a las subredes de VPC necesarias en lugar de poner toda la VPC a disposición de la red de ODB.

En esta sección se supone que ya has creado una red ODB en. Paso 1: Cree una red ODB en Oracle Database@AWS

Para actualizar una red ODB

1. Inicie sesión en Consola de administración de AWS y abra la Oracle Database@AWS consola en https://console.aws.amazon.com/odb/.
2. En el panel izquierdo, selecciona redes ODB.
3. Seleccione la red que desee modificar.
4. Elija Modificar.
5. (Opcional) Para el nombre de la red ODB, introduzca un nombre de red nuevo. El nombre debe tener entre 1 y 255 caracteres y empezar por un carácter alfabético o un guión bajo. No puede contener guiones consecutivos.
6. (Opcional) En Peered CIDRs, especifique los rangos de CIDR de la VPC emparejada que necesitan conectividad a la red ODB. Para limitar el acceso, le recomendamos que especifique los rangos de CIDR mínimos requeridos.

7. (Opcional) Para configurar integraciones de servicios, seleccione o deseleccione Amazon S3 o Zero-ETL.
8. Seleccione Continuar y, a continuación, seleccione Modificar.

Eliminar una red ODB en Oracle Database@AWS

Puede eliminar una red ODB. En esta sección se supone que ya ha creado una red ODB en. Paso 1: Cree una red ODB en Oracle Database@AWS No puede eliminar una red ODB que esté siendo utilizada actualmente por un clúster de máquinas virtuales.

Para eliminar una red ODB

1. Inicie sesión en Consola de administración de AWS y abra la Oracle Database@AWS consola en https://console.aws.amazon.com/odb/.
2. En el panel izquierdo, selecciona redes ODB.
3. Seleccione la red que desee eliminar.
4. Elija Eliminar.
5. (Opcional) Elija Eliminar los recursos de OCI asociados para eliminar los recursos de OCI que se crearon junto con la red ODB.
6. Escriba **`delete me`** en el cuadro de texto.
7. Elija Eliminar.

Eliminar un clúster de máquinas virtuales en Oracle Database@AWS

Puede eliminar un clúster de máquinas virtuales de Exadata o un clúster de máquinas virtuales autónomas. En esta sección se asume que ya ha creado un clúster de máquinas virtuales en. Paso 3: Cree un clúster de máquinas virtuales de Exadata o un clúster de máquinas virtuales autónomas en Oracle Database@AWS

Para eliminar un clúster de máquinas virtuales

1. Inicie sesión en Consola de administración de AWS y abra la Oracle Database@AWS consola en https://console.aws.amazon.com/odb/.

2. En el panel izquierdo, elija clústeres de máquinas virtuales de Exadata o clústeres de máquinas virtuales autónomas.
3. Elija un clúster de máquinas virtuales para eliminarlo.
4. Elija Eliminar.
5. Cuando se le solicite, introduzca **`delete me`** y, a continuación, seleccione Eliminar.

Eliminar una infraestructura de Oracle Exadata en Oracle Database@AWS

Puede eliminar una infraestructura de Oracle Exadata. En esta sección se supone que ya ha creado una infraestructura de Oracle Exadata en. Paso 2: Cree una infraestructura de Oracle Exadata en Oracle Database@AWS No puede eliminar una infraestructura de Exadata que esté siendo utilizada actualmente por un clúster de máquinas virtuales.

Para eliminar una infraestructura de Oracle Exadata

1. Inicie sesión en Consola de administración de AWS y abra la Oracle Database@AWS consola en. https://console.aws.amazon.com/odb/
2. En el panel izquierdo, seleccione Infraestructuras de Exadata.
3. Elija una infraestructura de Exadata para eliminarla.
4. Elija Eliminar.
5. Cuando se le solicite, introduzca **`delete me`** y, a continuación, seleccione Eliminar.

Eliminar una conexión de emparejamiento ODB

Cuando ya no necesite una conexión de emparejamiento ODB, puede eliminarla. Debe eliminar todas las conexiones de emparejamiento ODB para poder eliminar una red ODB.

Consola

1. Inicie sesión en Consola de administración de AWS y abra la consola en Oracle Database@AWS . https://console.aws.amazon.com/odb/
2. En el panel de navegación, elija conexiones de emparejamiento ODB.
3. Seleccione la conexión de emparejamiento ODB que desee eliminar.

4. Elija Eliminar.
5. Para confirmar la eliminación, introduzca **`delete me`** y seleccione Eliminar.

AWS CLI

Para eliminar una conexión de emparejamiento ODB, utilice el `delete-odb-peering-connection` comando.

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

Realizar copias de seguridad en Oracle Database@AWS

Oracle Database@AWS ofrece múltiples opciones de respaldo para proteger sus bases de datos Oracle. Puede utilizar copias de seguridad gestionadas por Oracle que se integran perfectamente con Amazon S3 o crear sus propias copias de seguridad gestionadas por el usuario mediante Oracle Recovery Manager (RMAN).

Oracle gestionó copias de seguridad en Amazon S3

Al crear una red ODB, Oracle Database@ configura AWS automáticamente el acceso a la red para las copias de seguridad gestionadas por Oracle en Amazon S3. OCI configura las entradas de DNS y las listas de seguridad necesarias. Estas configuraciones permiten el tráfico entre la red de nube virtual (VCN) de OCI y Amazon S3. La red ODB no habilita ni controla las copias de seguridad automáticas.

OCI gestiona en su totalidad las copias de seguridad gestionadas por Oracle. Al crear su base de datos Oracle Exadata, puede activar las copias de seguridad automáticas seleccionando Activar las copias de seguridad automáticas en la consola de OCI. Elija uno de los siguientes destinos de copia de seguridad:

- Amazon S3
- Almacenamiento de objetos OCI
- Servicio de recuperación autónoma

Para obtener más información, consulte Backup Exadata Database en la documentación de OCI.

Backups gestionados por el usuario en Amazon S3 en Oracle Database@AWS

Con Oracle Database@AWS, puede crear copias de seguridad de su base de datos administradas por los usuarios mediante el servicio de bases de datos Exadata en una infraestructura dedicada. Realiza una copia de seguridad de sus datos con Oracle Recovery Manager (RMAN) y los almacena en sus buckets de Amazon S3. Tiene el control total sobre la programación de las copias de seguridad, las políticas de retención y los costos de almacenamiento, al tiempo que mantiene las ventajas del servicio gestionado de Oracle Database@.AWS

> **Note**
>
> Oracle Database@AWS no admite copias de seguridad administradas por el usuario para bases de datos autónomas en infraestructuras dedicadas.

Las copias de seguridad administradas por el usuario complementan las soluciones de copias de seguridad AWS administradas que ofrece Oracle Database@.AWS Puede utilizar copias de seguridad manuales para cumplir con los requisitos de conformidad, la recuperación ante desastres entre regiones o la integración con los flujos de trabajo de gestión de copias de seguridad existentes.

Puede utilizar las siguientes técnicas de copia de seguridad administradas por el usuario:

Oracle Secure Backup

: Transmita las copias de seguridad directamente a Amazon S3 con un rendimiento óptimo.

Storage Gateway

: Use Storage Gateway para las copias de seguridad basadas en archivos que utilizan un recurso compartido de NFS.

Punto de montaje S3

: Utilice un cliente de archivos para montar un bucket de Amazon S3 como sistema de archivos local.

Requisitos previos para las copias de seguridad administradas por el usuario en Amazon S3 en Oracle Database@AWS

Antes de poder realizar una copia de seguridad de las bases de datos de Oracle Exadata en Amazon S3, haga lo siguiente:

1. Habilite el acceso directo a Amazon S3 desde su red ODB.
2. Configure la conectividad de red y el enrutamiento entre Oracle Database@AWS y Amazon S3.

Habilitar el acceso desde su red ODB a Amazon S3

Para realizar una copia de seguridad manual de su base de datos en Amazon S3, habilite el acceso directo a S3 desde su red ODB. Esta técnica permite que sus bases de datos accedan a Amazon

S3 para satisfacer las necesidades de su empresa, como la importación/exportación de datos o las copias de seguridad gestionadas por los usuarios. Tiene pleno control sobre el destino de destino del almacenamiento de copias de seguridad y puede utilizar políticas para restringir el acceso a Amazon S3 mediante VPC Lattice.

El acceso directo a Amazon S3 desde la red ODB no está habilitado de forma predeterminada. Puede habilitar el acceso a S3 al crear o modificar su red ODB.

Consola

Para habilitar el acceso directo a Amazon S3 desde su red ODB

1. Abra la consola Oracle Database@ en AWS . https://console.aws.amazon.com/odb/
2. En el panel de navegación, elija redes ODB.
3. Seleccione la red ODB para la que desee habilitar el acceso a Amazon S3.
4. Elija Modificar.
5. Seleccione Amazon S3.
6. (Opcional) Configure un documento de política de Amazon S3 para controlar el acceso a Amazon S3. Si no especifica una política, la política predeterminada le otorga acceso total.
7. Seleccione Continuar y, a continuación, Modificar.

AWS CLI

Para habilitar el acceso directo a Amazon S3 desde su red ODB, utilice el `update-odb-network` comando con el `s3-access` parámetro:

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

Para configurar un documento de política de Amazon S3, utilice el `--s3-policy-document` parámetro:

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

Cuando el acceso a Amazon S3 está habilitado, puede acceder a Amazon S3 desde su red ODB mediante el DNS `s3.region.amazonaws.com` regional. OCI configura este nombre DNS de forma predeterminada. Para usar un nombre DNS personalizado, modifique el DNS de VCN para asegurarse de que el DNS personalizado se resuelva en la dirección IP del punto final de la red de servicio.

Configuración de la conectividad de red entre Oracle Database@AWS y Amazon S3

Para permitir las copias de seguridad administradas por el usuario en Amazon S3, su máquina virtual debe poder acceder al punto de enlace de Amazon VPC de S3. En la consola OCI, puede editar las reglas de seguridad de un grupo de seguridad de red (NSG) para controlar el tráfico de entrada y salida. En el caso de las copias de seguridad administradas por el usuario, el tráfico fluye a través de la subred del cliente y no a través de la subred de copia de seguridad. En los siguientes pasos, debe actualizar la subred del cliente NSGs para agregar la regla de salida para la dirección IP del punto final de la VPC.

Para permitir el acceso de la máquina virtual al punto de conexión Amazon S3

1. Abra la AWS consola Oracle Database@ en. https://console.aws.amazon.com/odb/
2. Elija redes ODB.
3. Elija el nombre de la red ODB.
4. Elija los recursos de OCI.
5. Elija la pestaña Integraciones de servicios.
6. En Amazon S3, anote la siguiente información:
   - La IPv4 dirección del punto de conexión S3 de Amazon VPC. Necesitará esta información más adelante. Por ejemplo, la dirección IP puede ser`192.168.12.223`.
   - El nombre de dominio del punto de conexión S3 de Amazon VPC. Necesitará esta información más adelante. Por ejemplo, el nombre de dominio puede sers`3.us-east-1.amazonaws.com`.
7. En el panel de navegación izquierdo, elija los clústeres de máquinas virtuales de Exadata y, a continuación, elija el nombre del clúster de máquinas virtuales.
8. En la parte superior de la página, seleccione la pestaña Resumen.
9. Elija Máquinas virtuales y, a continuación, elija el nombre de la máquina virtual.
10. Anote el valor en el nombre de DNS. Este es el nombre de host que se especifica cuando se conecta a la máquina virtual mediante`ssh`.

11. En la parte superior derecha, selecciona Administrar en OCI. Esto abre la consola de OCI.
12. En la página de lista de redes de nube virtual, elija la VCN que contiene el grupo de seguridad de red (NSG) para la subred del cliente de red ODB (). `exa_static_nsg` Para obtener más información, consulte Gestión de las reglas de seguridad de un NSG en la documentación de la OCI.
13. En la página de detalles, lleve a cabo una de las siguientes acciones en función de la opción que aparezca:
    - En la pestaña Seguridad, vaya a Grupos de seguridad de red.
    - En Recursos, elija Grupos de seguridad de red.
14. Elija el NSG para la subred del cliente ()`exa_static_nsg`.
15. Agregue una regla de salida para la dirección de punto final de la VPC que indicó anteriormente.

Para probar la conectividad a S3 desde su máquina virtual

1. `ssh`Utilícelo para conectarse `root` a la máquina virtual cuyo nombre DNS obtuvo anteriormente. Cuando se conecte, especifique un `.pem` archivo con sus claves SSH.
2. Ejecute los siguientes comandos para asegurarse de que la máquina virtual pueda acceder al punto de enlace Amazon VPC de Amazon S3. Utilice el nombre de dominio S3 que anotó 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
```

Realizar copias de seguridad en Amazon S3 mediante Oracle Secure Backup

Oracle Secure Backup actúa como una interfaz SBT para su uso con Recovery Manager (RMAN). Puede utilizar RMAN con Oracle Secure Backup para realizar copias de seguridad de sus AWS bases de datos Oracle Database@ directamente en Amazon S3. Oracle Secure Backup ofrece las siguientes ventajas:

- Oracle Secure Backup optimiza la transferencia de datos entre RMAN y S3.
- No es necesario un almacenamiento de respaldo intermedio.

- Oracle Secure Backup gestiona el ciclo de vida de sus medios de respaldo.

Para realizar copias de seguridad en Amazon S3 mediante Oracle Secure Backup

1. Instale el módulo Oracle Secure Backup en su servidor Exadata VM. Sustituya los valores de los marcadores de posición por la clave de AWS acceso y la clave de acceso secreta. Para obtener más información, consulte la documentación de Oracle en 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. Conéctese a RMAN y configure el canal de respaldo y el tipo de dispositivo predeterminado.

```
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 la configuración.

```
RMAN> SHOW ALL;
```

4. Haga una copia de seguridad de la base de datos.

```
RMAN> BACKUP DATABASE;
```

5. Compruebe que la copia de seguridad se haya completado correctamente.

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

Realizar copias de seguridad en Amazon S3 mediante AWS Storage Gateway Amazon EC2

AWS Storage Gateway es un servicio híbrido que conecta su entorno local con los servicios de Nube de AWS almacenamiento. Para las AWS copias de seguridad de Oracle Database@, puede

utilizar Storage Gateway para crear un flujo de trabajo de copias de seguridad basado en archivos que escriba directamente en Amazon S3. A diferencia de la técnica Oracle Secure Backup, usted gestiona el ciclo de vida de las copias de seguridad.

En esta solución, se crea una EC2 instancia de Amazon independiente para configurar Storage Gateway. También agrega un volumen de Amazon EBS para almacenar en caché las lecturas y escrituras en Amazon S3.

Esta técnica ofrece las siguientes ventajas:

- No necesita un administrador de contenido multimedia como Oracle Secure Backup.
- No es necesario un almacenamiento de respaldo intermedio.

Para implementar su Storage Gateway y crear un recurso compartido de archivos

1. Abra Consola de administración de AWS at https://console.aws.amazon.com/storagegateway/home/ y elija la AWS región en la que desea crear su puerta de enlace.
2. Implemente y active una puerta de enlace de archivos de Amazon S3 utilizando una EC2 instancia de Amazon como centro. Siga las instrucciones de Implementación de un EC2 host Amazon personalizado para S3 File Gateway en la Guía del usuario de Storage Gateway.

   Al configurar la puerta de enlace de archivos, asegúrese de hacer lo siguiente:

   - Añada al menos un volumen de Amazon EBS para el almacenamiento en caché, con un tamaño mínimo de 150 GiB.
   - Abra el TCP/UDP puerto 2049 para acceder a NFS en su grupo de seguridad. Esto le permite crear recursos compartidos de archivos NFS.
   - Abra el puerto TCP 80 para el tráfico entrante para permitir el acceso HTTP por única vez durante la activación de la puerta de enlace. Tras la activación, puede cerrar este puerto.
3. Cree un punto de conexión de Amazon VPC para la conectividad privada entre la red ODB y Storage Gateway. Para obtener más información, consulte Acceder a un AWS servicio mediante un punto final de VPC de interfaz.
4. Cree un recurso compartido de archivos para su bucket de Amazon S3 a través de la consola Storage Gateway. Para obtener más información, consulte Crear un recurso compartido de archivos.

Para hacer una copia de seguridad de su base de datos en Amazon S3 mediante Storage Gateway

1. En un terminal, utilícelo `ssh` para conectarse al nombre DNS de la máquina virtual de Exadata. Para buscar el nombre DNS, consulte. Requisitos previos para las copias de seguridad administradas por el usuario en Amazon S3 en Oracle Database@AWS
2. Cree un directorio en el servidor de clústeres de máquinas virtuales de Exadata para el montaje de NFS. El siguiente ejemplo crea el directorio `/home/oracle/sgw_mount/`.

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

3. Monte el recurso compartido de NFS en el directorio que acaba de crear. En el siguiente ejemplo, se crea el recurso compartido en el directorio`/home/oracle/sgw_mount/`. *SG-IP-address*Sustitúyala por la dirección IP de Storage Gateway y *your-bucket-name* por el nombre del bucket de S3.

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

4. Conéctese a RMAN y haga una copia de seguridad de la base de datos en el directorio montado. En el siguiente ejemplo, se crea el canal `rman_local_bkp` y se utiliza la ruta del punto de montaje para formatear las piezas de respaldo.

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

5. Compruebe que los archivos de respaldo se hayan creado en el directorio de montaje. El siguiente ejemplo muestra dos piezas de respaldo.

```
$ 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
```

Realizar copias de seguridad en Amazon S3 mediante un punto de montaje S3

Puede utilizar el punto de montaje de Amazon S3 para crear copias de seguridad primero de forma local y, a continuación, copiarlas en Amazon S3. Esta técnica crea copias de seguridad en el almacenamiento local y, a continuación, las transfiere a Amazon S3 mediante la interfaz de punto de montaje. El tiempo de copia de seguridad es mayor que en otras técnicas porque es necesario hacer copias de seguridad de los datos dos veces.

> **Note**
>
> No se admite la copia de seguridad directa en Amazon S3 mediante el punto de montaje, sin almacenamiento provisional. RMAN requiere permisos de sistema de archivos específicos que no son compatibles con la interfaz de punto de montaje de Amazon S3.

Esta técnica no requiere que se otorgue una licencia a un administrador multimedia como Oracle Secure Backup. Usted gestiona el ciclo de vida de sus copias de seguridad.

Para realizar copias de seguridad en Amazon S3 mediante un punto de montaje S3

1. En un terminal, utilícelo `ssh` para conectarse al nombre DNS de la máquina virtual de Exadata. Para buscar el nombre DNS, consulte. Requisitos previos para las copias de seguridad administradas por el usuario en Amazon S3 en Oracle Database@AWS
2. Instale el punto de montaje Amazon S3 en el servidor de clústeres de máquinas virtuales de Exadata. Para obtener más información sobre la instalación y la configuración, consulte Mountpoint for Amazon S3 en la Guía del usuario de Amazon S3.

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

3. Verifique la instalación ejecutando el `mount-s3` comando.

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

4. Cree un directorio de respaldo intermedio en el almacenamiento local del servidor de clústeres Exadata VM. Hará una copia de seguridad de la base de datos en este directorio local y, a

continuación, copiará la copia de seguridad en su bucket de S3. En el siguiente ejemplo, se crea un directorio`/u02/rman_bkp_local`.

```
mkdir /u02/rman_bkp_local
```

5. Cree un directorio para el punto de montaje de Amazon S3. En el siguiente ejemplo, se crea un directorio`/home/oracle/s3mount`.

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

6. Monte su bucket de Amazon S3 mediante el punto de montaje. En el siguiente ejemplo, se monta un bucket de S3 en un directorio`/home/oracle/s3mount`. *`your-s3-bucket-name`*Sustitúyalo por el nombre real de su bucket de Amazon S3.

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

7. Compruebe que puede acceder al contenido del bucket de Amazon S3.

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

8. Conecte RMAN a su base de datos de destino y haga una copia de seguridad en su directorio provisional local. En el siguiente ejemplo, se crea el canal `rman_local_bkp` y se utiliza la ruta `/u02/rman_bkp_local/` para formatear las piezas de respaldo.

```
$ rman TARGET /

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

9. Compruebe que las copias de seguridad se crean en el directorio 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 los archivos de respaldo del directorio provisional local al punto de montaje de Amazon S3.

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

11. Compruebe que ha copiado los archivos correctamente en 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
```

Inhabilitar el acceso directo a Amazon S3

Si ya no necesita acceso directo a Amazon S3 desde su red ODB, puede deshabilitarlo. La activación o desactivación del acceso directo a la red a S3 no afecta al acceso de red a las copias de seguridad gestionadas por Oracle en Amazon S3.

Consola

Para deshabilitar el acceso directo a Amazon S3

1. Abra la AWS consola Oracle Database@ en. https://console.aws.amazon.com/odb/
2. En el panel de navegación, elija redes ODB.
3. Seleccione la red ODB para la que desee deshabilitar el acceso a Amazon S3.
4. Elija Modificar.
5. Desactive la casilla Habilitar el acceso a S3.
6. Seleccione Modificar la red ODB.

AWS CLI

Utilice el comando `update-odb-network` con el parámetro `s3-access`.

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

Solución de problemas de la integración de Amazon S3

Si tiene problemas con las copias de seguridad gestionadas por Oracle en Amazon S3 o con el acceso directo a Amazon S3, tenga en cuenta los siguientes pasos de solución de problemas:

No puede acceder a Amazon S3 desde su base de datos

Comprueba lo siguiente:

- Compruebe que el acceso a Amazon S3 esté habilitado para su red ODB. Utilice la `GetOdbNetwork` acción para comprobar si el `s3Access` estado es`Enabled`.
- Asegúrese de utilizar el nombre DNS regional correcto:`s3.region.amazonaws.com`.
- Compruebe que su base de datos Oracle tiene los permisos necesarios para acceder a Amazon S3.

Los respaldos gestionados por Oracle fallan

Comprueba lo siguiente:

- Las copias de seguridad gestionadas por Oracle en Amazon S3 están habilitadas de forma predeterminada y no se pueden deshabilitar. Si las copias de seguridad fallan, compruebe los registros de la base de datos de Oracle para ver si hay mensajes de error específicos.
- Compruebe que los recursos de Amazon VPC Lattice estén configurados correctamente consultando los recursos de integración de servicios.
- Póngase en contacto con Oracle Support para obtener ayuda con los problemas de backup automático gestionado por Oracle. Para obtener más información, consulte Obtener soporte para Oracle Database@AWS.

Integración de Oracle Database@AWS Zero-ETL con Amazon Redshift

La integración Zero-ETL es una solución totalmente gestionada que permite que los datos transaccionales y operativos estén disponibles en Amazon Redshift desde múltiples fuentes. Con esta solución, puede replicar datos en Amazon Redshift desde sus bases de datos Oracle que se ejecutan en Oracle Exadata o Autonomous Database en una infraestructura Exadata dedicada. La sincronización automática evita el proceso tradicional de extracción, transformación y carga (ETL). También permite el análisis en tiempo real y las cargas de trabajo de IA. Para obtener más información, consulte Integraciones sin ETL en la Guía de administración de Amazon Redshift.

La integración sin ETL ofrece las siguientes ventajas:

- Replicación de datos en tiempo real: sincronización continua de datos desde las bases de datos de Oracle a Amazon Redshift con una latencia mínima
- Eliminación de los complejos procesos de ETL: no es necesario crear ni mantener soluciones de integración de datos personalizadas
- Reducción de los gastos operativos: configuración y administración automatizadas mediante AWS APIs
- Arquitectura de integración de datos simplificada: integración perfecta entre Oracle Database@AWS y AWS los servicios de análisis
- Seguridad mejorada: cifrado integrado y controles de acceso a AWS IAM

Amazon Redshift no cobra ninguna tarifa adicional por la integración sin ETL con Oracle Database@.AWS Usted paga por los recursos de Amazon Redshift existentes que se utilizan para crear y procesar los datos de cambios creados como parte de una integración sin ETL. Para obtener más información, consulte Precios de Amazon Redshift.

Versiones de bases de datos compatibles para la integración sin ETL en Oracle Database@AWS

La integración Zero-ETL admite las siguientes versiones de bases de datos Oracle:

- Oracle Exadata: base de datos Oracle 19c
- Base de datos autónoma en infraestructura dedicada: Oracle Database 19c y 23ai

Cómo funciona la integración sin ETL en Oracle Database@AWS

La integración sin ETL permite a Oracle Database@AWS replicar datos en Amazon Redshift. La integración aprovecha Amazon VPC Lattice para crear una conectividad de red segura. La tecnología Change Data Capture (CDC) garantiza la sincronización de los datos en tiempo real. La integración se gestiona mediante AWS Glue APIs.

La arquitectura de integración Zero-ETL incluye lo siguiente:

- Conectividad segura: utiliza el SSL/TLS cifrado a través del puerto TLS 2484 para la transferencia de datos
- AWS Secrets Manager: almacena las credenciales y los certificados de la base de datos de forma segura mediante el servicio de administración de AWS claves
- AWS Integración con Glue: proporciona una interfaz de administración unificada para integraciones sin ETL

La replicación se realiza mediante los siguientes pasos:

1. Establecer una conexión segura a la base de datos Oracle mediante SSL en el puerto 2484
2. Realizar un volcado inicial completo de las bases de datos, esquemas y tablas seleccionadas
3. Configuración de la captura de datos de cambios (CDC) para una replicación continua en tiempo real
4. Escribir los datos replicados en el clúster de Amazon Redshift de destino

> **Important**
>
> La integración sin ETL no está habilitada de forma predeterminada. Debe configurarla mediante. AWS Glue APIs No puede configurar la integración sin ETL directamente mediante Oracle Database@.AWS APIs

Requisitos previos para la integración sin ETL en Oracle Database@AWS

Antes de configurar la integración sin ETL, asegúrese de cumplir los siguientes requisitos previos.

Requisitos previos generales

- AWS Configuración de Oracle Database@: asegúrese de tener al menos un clúster de máquinas virtuales aprovisionado y en ejecución.
- Integración con cero ETL activado: asegúrese de que su clúster de máquinas virtuales o clúster de máquinas virtuales autónomas esté asociado a una red ODB que tenga activado cero ETL.
- Versiones de Oracle Database compatibles: debe utilizar Oracle Database 19c (Oracle Exadata) o Oracle Database 19c/23ai (base de datos autónoma en infraestructura dedicada).
- Misma AWS región: la base de datos Oracle de origen y el clúster de Amazon Redshift de destino deben estar en la misma AWS región.

Requisitos previos de la base de datos Oracle

Debe configurar su base de datos Oracle con los siguientes parámetros.

Configuración del usuario de replicación

Cree un usuario de replicación dedicado en cada base de datos conectable (PDB) que desee replicar:

- Para Oracle Exadata: cree un usuario `ODBZEROETLADMIN` con una contraseña segura.
- Para una base de datos autónoma en una infraestructura dedicada: utilice el usuario existente`GGADMIN`.

Otorgue los siguientes permisos al usuario de replicación.

```
-- 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 suplementario

Habilite el registro adicional en su base de datos Oracle para capturar los datos de los cambios.

```
-- 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 una integración sin ETL entre Oracle Database@ y Amazon AWS Redshift, debe configurar SSL.

Para las bases de datos Oracle Exadata

Debe configurar manualmente el SSL en el puerto 2484. Esta tarea implica lo siguiente:

- Configurando `(PROTOCOL=tcps)(PORT=2484)` en `listener.ora`
- Configuración de la cartera mediante `sqlnet.ora`
- Generación y configuración de certificados SSL (consulte Cómo configurar SSL/TCPS Exadata Cloud Database (ExACC/EXACS) (ID de documento 2947301.1) en la documentación de My Oracle Support)

Para bases de datos autónomas

El SSL en el puerto 2484 está activado de forma predeterminada. No se necesita configuración adicional.

> **Important**
>
> El puerto SSL está fijado en 2484.

AWS requisitos previos del servicio

Antes de configurar la integración sin ETL, configure AWS Secrets Manager y configure los permisos de IAM.

Configurar AWS Secrets Manager

Guarde las credenciales de su base de datos Oracle en AWS Secrets Manager de la siguiente manera:

1. Cree una clave gestionada por el cliente (CMK) en AWS Key Management Service.
2. Guarde las credenciales de la base de datos en AWS Secrets Manager mediante la CMK.
3. Configure las políticas de recursos para permitir el acceso a Oracle Database@AWS .

Para obtener el identificador de clave y la contraseña de TDE, utilice la técnica descrita en Métodos de cifrado compatibles para utilizar Oracle como fuente de AWS Database Migration Service. El siguiente comando genera la cartera base64.

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

El siguiente ejemplo muestra un secreto de Oracle Exadata. Para*asm_service_name*, *111.11.11.11* representa la IP virtual del nodo de máquina virtual. También puede registrar el listener de ASM con 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"
  }
}
```

El siguiente ejemplo muestra el secreto de una base de datos autónoma en una infraestructura 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 los permisos de IAM

Cree políticas de IAM que permitan operaciones de integración sin ETL. El siguiente ejemplo de política permite describir, crear, actualizar y eliminar operaciones para un clúster de máquinas virtuales de Exadata. Para un clúster de máquinas virtuales autónomas, utilice el valor `cloud-autonomous-vm-cluster` en lugar del `cloud-vm-cluster` ARN del recurso.

Consideraciones para la integración sin ETL en Oracle Database@AWS

Al configurar la integración sin ETL entre Amazon Redshift Oracle Database@AWS y Amazon Redshift, tenga en cuenta las siguientes pautas:

Tiempo inicial de carga de datos

El tiempo de carga total inicial depende del tamaño de la base de datos. Las bases de datos grandes pueden tardar varias horas o días en completar la sincronización inicial.

Rendimiento de las bases de datos Oracle

Los cambios en la captura de datos pueden afectar al rendimiento de las bases de datos Oracle, especialmente cuando hay grandes volúmenes de transacciones. Tras habilitar la integración sin ETL, supervise el rendimiento de la base de datos.

Cambios de esquema

Los cambios en el lenguaje de definición de datos (DDL) en la base de datos Oracle de origen pueden requerir que intervenga manualmente para volver a crear la integración. Planifique los cambios en el esquema con cuidado.

Para obtener información general, consulte Consideraciones al utilizar integraciones sin ETL con Amazon Redshift.

Limitaciones de la integración sin ETL en Oracle Database@AWS

Tenga en cuenta las siguientes limitaciones generales:

PDB única por integración

Cada integración de Zero-ETL solo puede replicar datos de una base de datos conectable (PDB). No se admiten filtros de datos como este. `include: pdb1.*.*, include: pdb2.*.*`

Integración única por base de datos autónoma o infraestructura de Exadata

Cada integración sin ETL solo puede replicar datos de una base de datos autónoma en una infraestructura dedicada.

Puerto SSL fijo

Las conexiones SSL deben usar el puerto 2484.

Requisito de la misma región

El clúster Oracle Database@AWS VM de origen y el clúster Amazon Redshift de destino deben estar en la misma región. AWS No se admite la replicación entre regiones.

No es compatible con mTLS

No se admite el TLS mutuo (mTLS). Si su base de datos OCI tiene el mTLS activado, debe deshabilitarlo para utilizar la integración sin ETL.

Configuración de integración inmutable

Después de crear la clave de ARN o KMS secreta asociada a una integración, no podrá modificarla. Debe eliminar y volver a crear la integración para cambiar esta configuración.

Cifrado TDE a nivel de columna

El cifrado de datos transparente (TDE) a nivel de columna no es compatible con las bases de datos Oracle Exadata. Solo se admite el TDE a nivel de espacio de tablas.

Compatibilidad con tipos de datos

Es posible que algunos tipos de datos específicos de Oracle no sean totalmente compatibles o que requieran una transformación durante la replicación. Pruebe minuciosamente sus tipos de datos específicos antes de implementar la base de datos en producción.

Configuración de las AWS integraciones de Oracle Database@ con Amazon Redshift

Para configurar la integración sin ETL entre la base de datos de Oracle y Amazon Redshift, siga estos pasos:

1. Habilite el ETL cero en su red ODB.
2. Configure los requisitos previos de la base de datos Oracle.
3. Configure AWS Secrets Manager y AWS Key Management Service.
4. Configurar los permisos de IAM.
5. Configure las políticas de recursos de Amazon Redshift.
6. Cree la integración sin ETL.
7. Cree la base de datos de destino en Amazon Redshift.

Paso 1: Habilite Zero-ETL para su red ODB

Puede habilitar la integración sin ETL para la red ODB asociada a su clúster de máquinas virtuales de origen. De forma predeterminada, esta integración está deshabilitada.

Consola

Para habilitar la integración sin ETL

1. Abra la consola Oracle Database@ en AWS . https://console.aws.amazon.com/odb/
2. En el panel de navegación, elija redes ODB.
3. Seleccione la red ODB para la que desee habilitar la integración sin ETL.
4. Elija Modificar.
5. Seleccione Zero-ETL.
6. Seleccione Continuar y, a continuación, Modificar.

AWS CLI

Para habilitar la integración sin ETL, utilice el `update-odb-network` comando con el `--zero-etl-access` parámetro:

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

Para habilitar la integración sin ETL en la red ODB asociada al clúster de máquinas virtuales de origen, utilice el comando. `update-odb-network` Este comando configura la infraestructura de red necesaria para la integración sin ETL.

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

Paso 2: Configure su base de datos Oracle

Complete la configuración de la base de datos Oracle tal y como se describe en los requisitos previos:

- Cree los usuarios de replicación y conceda los permisos necesarios.
- Habilite los redo logs archivados.
- Configure SSL (solo Oracle Exadata).
- Configure los usuarios de ASM, si corresponde (solo Oracle Exadata).

Paso 3: Configurar AWS Secrets Manager y AWS Key Management Service

Cree una clave gestionada por el cliente (CMK) y almacene las credenciales de su base de datos.

1. Cree una CMK en el servicio de administración de AWS claves mediante el `create-key` comando.

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

2. Guarde las credenciales de su base de datos en 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. Adjunte una política de recursos al secreto para permitir el acceso a Oracle Database@AWS .

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

En el comando anterior, `secret-resource-policy.json` contiene el siguiente JSON.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "zetl.odb.amazonaws.com"
      },
      "Action": [
```

```
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": "*"
    }
  ]
}
```

4. Adjunte una política de recursos a la CMK. La política de recursos de CMK debe incluir permisos tanto para el principal de servicio de Oracle Database@ como para el principal de AWS servicio de Amazon Redshift a fin de admitir la integración cifrada sin ETL.

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

El `cmk-resource-policy.json` archivo debe incluir las siguientes declaraciones de política. La primera declaración permite el acceso al AWS servicio Oracle Database@ y la segunda permite a Amazon Redshift crear concesiones en la clave KMS para operaciones de datos cifrados.

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"
          ]
        }
      }
    }
  ]
}
```

Paso 4: Configurar los permisos de IAM

Cree y adjunte políticas de IAM que permitan operaciones de integración sin 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
```

La siguiente política otorga los permisos necesarios.

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": "*"
    }
  ]
}
```

Paso 5: Configurar las políticas de recursos de Amazon Redshift

Configure políticas de recursos en su clúster de Amazon Redshift para autorizar las integraciones entrantes.

```
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, puede usar la opción Fix it for me de la consola. AWS Esta opción configura automáticamente las políticas de Amazon Redshift requeridas sin que tenga que hacerlo manualmente.

Paso 6: Cree la integración Zero-ETL mediante AWS Glue

Cree la integración Zero-ETL mediante el comando. AWS Glue `create-integration` En este comando, se especifica el clúster de máquinas virtuales de origen y el espacio de nombres de Amazon Redshift de destino.

El siguiente ejemplo crea una integración con un PDB denominado `pdb1` ejecutándose en un clúster de máquinas virtuales de Exadata. También puede crear un clúster de máquinas virtuales autónomas `cloud-vm-cluster` sustituyéndolo por `cloud-autonomous-vm-cluster` en el ARN de origen. Especificar una clave KMS es opcional. Si especifica una clave, puede ser diferente de la que creóPaso 3: Configurar AWS Secrets Manager y 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"
```

El comando devuelve un ARN de integración y establece el estado en. `creating` Puede supervisar el estado de la integración mediante el `describe-integrations` comando.

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

> **Important**
>
> Solo se admite un PDB por integración. El filtro de datos debe especificar una única PDB, por ejemplo,. `include: pdb1.*.*` La fuente debe estar en la misma AWS región y cuenta en las que se está creando la integración.

Paso 7: Crear una base de datos de destino en Amazon Redshift

Cuando la integración esté activa, cree una base de datos de destino en el clúster de 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";
```

Tras crear la base de datos de destino, puede consultar los datos replicados.

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

-- Connect to the new database
\c target_database_name

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

Compruebe la integración sin ETL

Compruebe que la integración funciona consultando el estado de la integración AWS Glue y asegurándose de que los cambios de Oracle se estén replicando en Amazon Redshift.

Para comprobar que la integración de Zero-ETL funciona correctamente

1. Compruebe el estado de la integración.

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

   El estado debe ser `ACTIVE` o`REPLICATING`.
2. Compruebe la replicación de datos realizando cambios en la base de datos de Oracle y comprobando que aparecen en Amazon Redshift.
3. Supervise las métricas de replicación en Amazon CloudWatch (si están disponibles).

Filtrado de datos para integraciones sin ETL en Oracle Database@AWS

Oracle Database@AWS Las integraciones Zero-ETL admiten el filtrado de datos. Puede utilizarla para controlar qué datos replica su base de datos Oracle Exadata de origen en su almacén de datos de destino. En lugar de replicar toda la base de datos, puede aplicar uno o más filtros para incluir o excluir selectivamente tablas específicas. Esto lo ayuda a optimizar el almacenamiento y el rendimiento de las consultas al garantizar que solo se transfieran los datos relevantes. El filtrado se limita a los niveles de base de datos y tablas. No se admite el filtrado a nivel de columnas y filas.

Oracle Database y Amazon Redshift gestionan las mayúsculas y minúsculas de los nombres de los objetos de forma diferente, lo que afecta a la configuración del filtro de datos y a las consultas de destino. Tenga en cuenta lo siguiente:

- Oracle Database almacena los nombres de bases de datos, esquemas y objetos en mayúsculas, a menos que se indique explícitamente en la instrucción `CREATE`. Por ejemplo, si crea `mytable` (sin comillas), el diccionario de datos de Oracle almacena el nombre de la tabla como `MYTABLE`. Si cita el nombre del objeto en la declaración de creación, el diccionario de datos de Oracle conserva las mayúsculas y minúsculas.

- Los filtros de datos zero-ETL distinguen entre mayúsculas y minúsculas y deben coincidir exactamente con las mayúsculas y minúsculas de los nombres de los objetos tal como aparecen en el diccionario de datos de Oracle. Por ejemplo, si el diccionario de Oracle almacena el esquema y el nombre de la tabla`REINVENT.MYTABLE`, cree un filtro utilizando`include: ORCL.REINVENT.MYTABLE`.
- Las consultas de Amazon Redshift utilizan de forma predeterminada los nombres de objetos en minúscula, a menos que se cite explícitamente. Por ejemplo, una consulta de `MYTABLE` (sin comillas) busca `mytable`.

Tenga en cuenta las diferencias entre mayúsculas y minúsculas cuando cree el filtro de Amazon Redshift y consulte los datos. Las consideraciones de filtrado para Amazon RDS for Oracle Oracle Database@AWS son las mismas que para Amazon RDS for Oracle. Para ver ejemplos de cómo los mayúsculas y minúsculas pueden afectar a los filtros de datos de una base de datos de Oracle, consulte los ejemplos de RDS for Oracle en la Guía del usuario de Amazon Relational Database Service.

Supervisión de la integración sin ETL

La supervisión periódica de su integración con Zero-ETL garantiza un rendimiento óptimo y ayuda a identificar los problemas a tiempo.

Supervisión del estado de la integración

Supervisa el estado de tus integraciones sin ETL con 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
```

Los estados de integración incluyen:

- creación: se está configurando la integración
- activo: la integración consiste en ejecutar y replicar datos
- modificar: la configuración de la integración se está actualizando
- needs_attention — La integración requiere una intervención manual

- fallido: se ha producido un error en la integración
- eliminar: se está eliminando la integración

Supervisión del rendimiento

Supervise los siguientes aspectos del rendimiento de su integración sin ETL:

- Retraso de replicación: diferencia de tiempo entre el momento en que se produce un cambio en Oracle y el momento en que aparece en Amazon Redshift
- Rendimiento de datos: volumen de datos que se replican por unidad de tiempo
- Tasas de error: frecuencia de errores o fallas de replicación
- Utilización de recursos: uso de la CPU, la memoria y la red en los sistemas de origen y de destino

Usa Amazon CloudWatch para monitorear estas métricas y configurar alarmas para los umbrales críticos.

Gestión de integraciones sin ETL en Oracle Database@AWS

Tras crear una integración sin ETL, puede realizar diversas operaciones de administración, como modificar y eliminar integraciones. En esta sección se describe la administración continua de sus integraciones sin ETL.

Modificación de integraciones sin ETL

Solo puede modificar el nombre, la descripción y las opciones de filtrado de datos para una integración sin ETL en un almacén de datos compatible. No puede modificar la AWS clave del servicio de administración de claves utilizada para cifrar la integración ni las bases de datos de origen o destino.

Requisitos previos para modificar las integraciones

Antes de modificar una integración sin ETL, asegúrese de tener lo siguiente:

- Permisos necesarios: su usuario o rol de IAM debe tener el `odb:UpdateOutboundIntegration` permiso además de los permisos estándar. AWS Glue
- Integración en estado activo: la integración debe estar en un `ACTIVE` estado, no en`CREATING`, `MODIFYINGDELETING`, o`FAILED`.

- Sintaxis de filtro de datos válida: los filtros de datos nuevos deben seguir la sintaxis de include/exclude patrones admitida.

Modificación de los filtros de datos

Puede cambiar las tablas o esquemas que se replican modificando el filtro de datos. De esta forma, puede añadir o eliminar objetos de la base de datos de la replicación sin tener que volver a crear toda la integración.

Para modificar el filtro de datos de una integración, utilice el `modify-integration` comando.

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

También puede modificar el nombre y la descripción de la integración al mismo tiempo. En el siguiente ejemplo, se modifican el nombre, las descripciones y los filtros de dos esquemas de la integración. `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**
>
> Al modificar el filtro de datos, la integración entra en un `modifying` estado y realiza una resincronización de los datos. La integración detiene la replicación, aplica la nueva configuración del filtro y reanuda la replicación con una operación de destino de recarga. Supervise el estado de la integración para garantizar que la modificación se complete correctamente.

Consideraciones sobre las modificaciones de los filtros de datos en las integraciones sin ETL

Tenga en cuenta lo siguiente al modificar los filtros de datos:

- Limitación de una sola PDB: solo puede especificar una base de datos conectable (PDB) por integración. No se admiten filtros de datos como este `include: pdb1.*.*, include: pdb2.*.*`
- Interrupción de la replicación: la replicación de los datos se detiene durante el proceso de modificación y se reanuda después de aplicar el nuevo filtro.
- Recarga de datos: la integración realiza una recarga completa de los datos que coinciden con los nuevos criterios del filtro.
- Impacto en el rendimiento: los cambios de gran tamaño en el filtro de datos pueden tardar bastante en completarse y pueden afectar al rendimiento de la base de datos de origen durante la recarga.

Limitaciones de las modificaciones de la configuración de integración sin ETL

No puede modificar la siguiente configuración después de crear una integración sin ETL:

- ARN secreto: el secreto de AWS Secrets Manager que contiene las credenciales de la base de datos
- Clave KMS: la clave administrada por el cliente que se utiliza para el cifrado
- ARN de origen: el clúster Oracle Database@ VM AWS
- ARN de destino: el clúster o el espacio de nombres de Amazon Redshift

Para cambiar esta configuración, elimine la integración Zero-ETL existente y cree una nueva.

Eliminación de las integraciones sin ETL

Cuando ya no necesite una integración sin ETL, puede eliminarla para detener la replicación y limpiar los recursos asociados.

Eliminación mediante AWS Glue

Elimine una integración sin ETL mediante la API de AWS Glue.

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

Puedes eliminar integraciones en los siguientes estados:

- activa

- necesita_atención
- error
- sincronizando

Efectos de la eliminación

Al eliminar una integración sin ETL, tenga en cuenta los siguientes efectos:

La replicación se detiene.

Oracle Database@AWS no replica los cambios nuevos de Amazon Redshift.

Se conservan los datos existentes.

Los datos ya replicados en Amazon Redshift permanecen disponibles.

La base de datos de destino permanece.

La base de datos de Amazon Redshift creada a partir de la integración no se elimina automáticamente.

> **Important**
>
> La eliminación es irreversible. Si necesita reanudar la replicación tras la eliminación, cree una nueva integración que realice una carga inicial completa.

Mejores prácticas para la administración sin ETL

Siga estas prácticas recomendadas para garantizar un rendimiento, una seguridad y una rentabilidad óptimos de sus integraciones sin ETL.

Prácticas operativas recomendadas

Estas prácticas operativas ayudan a mantener integraciones sin ETL confiables y eficientes.

Monitoreo regular

Configure CloudWatch alarmas para monitorear las métricas de rendimiento y estado de la integración.

Rotación de credenciales

Cambie periódicamente las contraseñas de las bases de datos y actualícelas en AWS Secrets Manager.

Verificación de Backup

Compruebe periódicamente que las copias de seguridad de sus bases de datos Oracle incluyen los componentes necesarios para la recuperación ante desastres.

Pruebas de rendimiento

Compruebe el impacto de la integración sin ETL en el rendimiento de su base de datos Oracle, especialmente durante los períodos de mayor uso.

Planificación de cambios de esquema

Planifique y pruebe los cambios de esquema en un entorno de desarrollo antes de aplicarlos a la producción.

Prácticas recomendadas de seguridad

Implemente estas medidas de seguridad para proteger su integración y sus datos sin ETL.

Acceso con privilegios mínimos

Otorgue solo los permisos mínimos necesarios a los usuarios de replicación y a las funciones de AWS IAM.

Seguridad de la red

Utilice grupos de seguridad y NACLs restrinja el acceso a la red únicamente a los puertos y fuentes necesarios.

Cifrado en reposo

Asegúrese de que tanto las bases de datos de Oracle como los clústeres de Amazon Redshift utilicen el cifrado en reposo.

Registro de auditoría

Habilite el registro de auditoría en Oracle y Amazon Redshift para realizar un seguimiento del acceso a los datos y los cambios.

Administración de secretos

Utilice las funciones de rotación automática de AWS Secrets Manager siempre que sea posible.

Optimización de costos

Aplique estas estrategias para optimizar los costos y, al mismo tiempo, mantener un rendimiento efectivo de integración sin ETL.

Filtrado de datos

Utilice filtros de datos precisos para replicar solo los datos que necesita, lo que reduce los costes de almacenamiento y procesamiento.

Optimización de Amazon Redshift

Utilice los tipos de nodos de Amazon Redshift adecuados e implemente la compresión de datos para optimizar los costes.

Uso de la monitorización

Revise periódicamente el uso y los costos de su integración sin ETL a través de AWS Cost Explorer.

Limpie las integraciones no utilizadas

Elimine las integraciones que ya no sean necesarias para evitar cargos continuos.

Solución de problemas de integración Zero-ETL

Esta sección proporciona orientación para resolver problemas comunes relacionados con la integración sin ETL.

Fallos en la configuración de la integración sin ETL

Errores de autenticación

- Compruebe que el usuario de replicación existe y tiene la contraseña correcta en AWS Secrets Manager.
- Asegúrese de que se hayan otorgado todos los permisos necesarios al usuario de replicación.
- Compruebe que el ARN secreto es correcto y que Oracle Database@ puede acceder a él.AWS

- Compruebe que la política de recursos de CMK permita el acceso del director de servicio de Oracle Database@.AWS

Problemas de conectividad de red

- Asegúrese de que su red ODB tenga habilitada la integración sin ETL.
- Compruebe que el SSL esté configurado correctamente en el puerto 2484 (solo Exadata).
- Compruebe que el detector de bases de datos Oracle se esté ejecutando y aceptando conexiones.
- Asegúrese de que la red agrupe y NACLs permita el tráfico en el puerto 2484.
- Compruebe que el nombre del servicio que figura en su secreto coincide con el nombre real del servicio de Oracle.

Errores de permisos

- Compruebe que su usuario o rol de IAM tenga los permisos necesarios para las operaciones de AWS Glue integración.
- Compruebe que la política de recursos de Amazon Redshift permita las integraciones entrantes desde su clúster de máquinas virtuales.
- Asegúrese de que Oracle Database@AWS tenga acceso a sus secretos y AWS a la clave del Servicio de administración de claves.

Problemas de replicación

Fallos de carga inicial

- Compruebe que la base de datos Oracle tiene recursos suficientes para soportar la operación de carga completa.
- Asegúrese de que el registro suplementario esté habilitado en la base de datos de origen.
- Compruebe si hay bloqueos o restricciones a nivel de tabla que puedan impedir la extracción de datos.

Cambie los problemas de captura de datos

- Compruebe que la base de datos Oracle tenga el espacio y la retención adecuados en los registros de redo.
- Compruebe que el usuario de replicación tenga acceso a los redo logs archivados.
- En el caso de los sistemas habilitados para ASM, asegúrese de que el usuario de ASM esté configurado correctamente.

- Supervise el rendimiento de la base de datos Oracle para asegurarse de que los CDC no estén provocando una contención de recursos.

Alto retraso en la replicación

- Supervise las métricas de retraso en la replicación CloudWatch.
- Compruebe si hay grandes volúmenes de transacciones o transacciones grandes en la base de datos de origen.
- Compruebe que el clúster de Amazon Redshift tenga la capacidad adecuada para gestionar los datos entrantes.

Problemas de coherencia de los datos

Datos faltantes o incompletos

- Compruebe que el filtro de datos incluye todos los esquemas y tablas necesarios.
- Compruebe si hay tipos de datos no compatibles que puedan estar provocando errores de replicación.
- Asegúrese de que el usuario de replicación tenga permisos SELECT en todas las tablas obligatorias.

Errores de conversión de tipos de datos

- Revise las asignaciones de tipos de datos admitidas entre Oracle y Redshift.
- Compruebe si hay tipos de datos específicos de Oracle que puedan requerir un tratamiento personalizado.
- Considere la posibilidad de modificar su esquema de Oracle para utilizar tipos de datos más compatibles.

Monitoreo y depuración

Utilice los siguientes enfoques para supervisar y depurar los problemas de integración sin ETL:

- Supervisión del estado de la integración: compruebe periódicamente el estado de la integración mediante. `aws glue describe-integrations`
- CloudWatch métricas: supervise CloudWatch las métricas disponibles para comprobar el rendimiento y los errores de la replicación.
- Supervisión de bases de datos Oracle: supervise el rendimiento y la utilización de los recursos de las bases de datos Oracle.

- Supervisión de Redshift: supervise el rendimiento del clúster de Amazon Redshift y la utilización del almacenamiento.

Para problemas complejos que no se puedan resolver con esta guía de solución de problemas, póngase en contacto AWS Support con la siguiente información:

- ARN de integración y estado actual.
- Los mensajes de error de la integración describen las operaciones.
- Configuraciones de bases de datos Oracle y clústeres de Amazon Redshift.
- Cronología del momento en que comenzó a producirse el problema.

Seguridad en Oracle Database@AWS

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre OCI AWS y usted. El modelo de responsabilidad compartida describe esto como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que se ejecuta Servicios de AWS en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de cuando se utiliza el Oracle Database@AWS. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus Oracle Database@AWS recursos.

Puede administrar el acceso a sus Oracle Database@AWS recursos. El método que utilice para administrar el acceso depende del tipo de tarea con la que deba realizar Oracle Database@AWS:

- Utilice políticas AWS Identity and Access Management (IAM) para asignar permisos que determinen quién puede administrar Oracle Database@AWS los recursos. Por ejemplo, puede usar IAM para determinar quién puede crear, describir, modificar y eliminar la infraestructura de Exadata, los clústeres de máquinas virtuales o etiquetar los recursos.
- Utilice las funciones de seguridad del motor de base de datos de Oracle para controlar quién puede iniciar sesión en las bases de datos de una instancia de base de datos. Estas características funcionas de igual forma que si la base de datos estuviera en su red local.
- Utilice conexiones Secure Socket Layers (SSL) o Transport Layer Security (TLS) con las bases de datos de Exadata. Para obtener más información, consulte Prepararse para las conexiones TLS Walletless.
- Oracle Database@AWS no se puede acceder inmediatamente a él desde Internet y se implementa únicamente en subredes privadas. AWS

- Oracle Database@AWS utiliza muchos puertos predeterminados del Protocolo de control de transmisión (TCP) para diversas operaciones. Para ver la lista completa de puertos, consulte Asignaciones de puertos predeterminadas.
- Para almacenar y gestionar las claves mediante el cifrado transparente de datos (TDE), que está activado de forma predeterminada, se Oracle Database@AWS utilizan almacenes OCI o Oracle Key Vault. Oracle Database@AWS no es compatible. AWS Key Management Service
- De forma predeterminada, la base de datos se configura mediante claves de cifrado gestionadas por Oracle. La base de datos también admite claves gestionadas por el cliente.
- Para mejorar la protección de los datos, utilice Oracle Data Safe with. Oracle Database@AWS

Los siguientes temas le muestran cómo configurarlo Oracle Database@AWS para cumplir sus objetivos de seguridad y conformidad.

Temas

Protección de datos en Oracle Database@AWS

Para proteger los datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.

- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados que contienen Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Oracle Database@AWS u otro dispositivo Servicios de AWS mediante la consola, la API o. AWS CLI AWS SDKs Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos

Las bases de datos de Exadata utilizan Oracle Transparent Data Encryption (TDE) para cifrar sus datos. Sus datos también están protegidos en espacios de tablas temporales, deshacer segmentos, rehacer registros y durante las operaciones internas de la base de datos, como JOIN y SORT. Para obtener más información, consulte Seguridad de datos.

Cifrado en tránsito

Las bases de datos de Exadata utilizan las capacidades nativas de cifrado e integridad de Oracle Net Services para proteger las conexiones a la base de datos. Para obtener más información, consulte Seguridad de los datos en tránsito.

Administración de claves

El cifrado de datos transparente incluye un almacén de claves para almacenar de forma segura las claves de cifrado maestras y un marco de administración para administrar de manera segura y eficiente el almacén de claves y realizar operaciones de mantenimiento de claves. Para obtener más información, consulte Para administrar las claves de cifrado de Vault.

Administración de identidades y accesos para Oracle Database@AWS

AWS Identity and Access Management (IAM) es un AWS servicio que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para utilizar los recursos de Oracle Database@.AWS La IAM es un AWS servicio que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Solución de problemas Oracle Database@AWS de identidad y acceso).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte ¿Cómo Oracle Database@AWS funciona con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Políticas de Oracle Database@AWS basadas en identidades).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en la Cuenta de AWS en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la

federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un Rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de un rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Las funciones de IAM son útiles para el acceso de usuarios federados, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon. EC2 Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

El acceso se controla creando políticas y AWS adjuntándolas a identidades o recursos. AWS Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear

una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden ser políticas insertadas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCPs): establece los permisos máximos disponibles para los recursos de tus cuentas. Para obtener más información, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo Oracle Database@AWS funciona con IAM

Antes de utilizar IAM para gestionar el acceso a Oracle Database@AWS, averigüe qué funciones de IAM están disponibles para su uso con Oracle Database@.AWS

Característica de IAM	Oracle Database@AWS soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo Oracle Database@AWS funcionan otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para Oracle Database@AWS

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para Oracle Database@AWS

Para ver ejemplos de políticas basadas en la AWS identidad de Oracle Database@, consulte. Políticas de Oracle Database@AWS basadas en identidades

Políticas basadas en recursos dentro Oracle Database@AWS

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones políticas para Oracle Database@AWS

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de Oracle Database@AWS acciones, consulte Acciones definidas por Oracle Database@AWS en la Referencia de autorización de servicios.

Las acciones de política Oracle Database@AWS utilizan el siguiente prefijo antes de la acción:

```
odb
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Para ver ejemplos de políticas basadas en la AWS identidad de Oracle Database@, consulte. Políticas de Oracle Database@AWS basadas en identidades

Recursos de políticas para Oracle Database@AWS

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de Oracle Database@AWS recursos y sus tipos ARNs, consulte Recursos definidos por Oracle Database@AWS en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por Oracle Database@.AWS

Para ver ejemplos de políticas basadas en la identidad de Oracle Database@AWS , consulte. Políticas de Oracle Database@AWS basadas en identidades

Claves de condición de la política para Oracle Database@AWS

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de claves de Oracle Database@AWS condición, consulte las claves de condición de Oracle Database@AWS en la Referencia de autorización de servicios. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por Oracle Database@.AWS

Para ver ejemplos de políticas basadas en la AWS identidad de Oracle Database@, consulte. Políticas de Oracle Database@AWS basadas en identidades

ACLs in Oracle Database@AWS

ACLsSoporta: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Oracle Database@AWS

Compatibilidad con ABAC (etiquetas en las políticas): parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Utilizar credenciales temporales con Oracle Database@AWS

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Permisos principales entre servicios para Oracle Database@AWS

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos del principal que llama a un AWS servicio, combinados con los del AWS servicio solicitante para realizar solicitudes a los servicios descendentes. Para obtener información detallada sobre las políticas a la hora de realizar solicitudes de FAS, consulte Forward access sessions.

Roles de servicio para Oracle Database@AWS

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puedes crear, modificar y eliminar un rol de servicio desde IAM. Para obtener

más información, consulte Crear un rol para delegar permisos a un AWS servicio en la Guía del usuario de IAM.

> **Warning**
>
> Si se cambian los permisos de un rol de servicio, es posible que se interrumpa Oracle Database@AWS la funcionalidad. Edite las funciones de servicio solo cuando se Oracle Database@AWS proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para Oracle Database@AWS

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un servicio. AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación o la administración de funciones Oracle Database@AWS vinculadas al servicio, consulte. Uso de roles vinculados a servicios para Oracle Database@AWS

Políticas de Oracle Database@AWS basadas en identidades

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de Oracle AWS Database@. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Oracle Database@AWS, incluido el formato de cada uno de ARNs los tipos de recursos, consulte Acciones, recursos y claves de condición de Oracle Database@AWS en la Referencia de autorización de servicios.

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar los recursos de Oracle Database@ de su cuenta.AWS Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS gestionadas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder acceso a las acciones del servicio si se utilizan a través de un AWS servicio específico, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para

más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Mediante la consola de Oracle Database@AWS

Para acceder a la AWS consola Oracle Database@, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Oracle Database@AWS que tiene en su cuenta. Cuenta de AWS Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario conceder permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Permita a los usuarios aprovisionar Oracle Database@AWS recursos

Esta política permite a los usuarios un acceso total a los Oracle Database@AWS recursos de aprovisionamiento. Para configurar la resolución de DNS desde su VPC, cree un solucionador de Route 53 saliente y añada reglas para reenviar el tráfico de DNS con el nombre de dominio de OCI a la IP del receptor de DNS de 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": "*"
        }
    ]
}
```

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API o. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
```

```
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS políticas gestionadas para Oracle Database@AWS

Para añadir permisos a conjuntos de permisos y roles, es más fácil usar políticas AWS administradas que escribirlas tú mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del usuario de IAM.

Servicios de AWS mantener y actualizar las políticas AWS gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios añaden permisos adicionales a una política AWS gestionada para admitir nuevas funciones. Este tipo de actualización afecta a todas las identidades (conjuntos de permisos y roles) donde se asocia la política. Lo más probable es que los servicios actualicen una política AWS administrada cuando se lanza una nueva función o cuando hay nuevas operaciones disponibles. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no infringen los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política `ReadOnlyAccess` AWS gestionada proporciona acceso de solo lectura a todos Servicios de AWS los recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

Temas

- AWS política gestionada: Amazon ODBService RolePolicy

AWS política gestionada: Amazon ODBService RolePolicy

No puede asociar la política `AmazonODBServiceRolePolicy` a sus entidades de IAM. Esta política está asociada a un rol vinculado al servicio que le permite Oracle Database@AWS realizar acciones en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios para Oracle Database@AWS.

Para ver más detalles sobre la política, incluida la última versión del documento de política de JSON, consulta Amazon ODBService RolePolicy en la Guía de referencia de políticas AWS gestionadas.

Oracle Database@AWS autenticación y autorización en OCI

Cuando utiliza AWS APIs para crear recursos Oracle Database@AWS, esos recursos residen lógicamente en su arrendamiento vinculado de Oracle Cloud Infrastructure (OCI). Para implementar estos recursos, AWS comuníquese con OCI APIs en su nombre. Para mitigar el confuso problema de los diputados, Oracle Database@AWS utilice OCI AWS STS como entidad de confianza y reenvíe las sesiones de acceso para autorizar su intención de utilizar OCI APIs en su arrendamiento vinculado. En consecuencia, los eventos se registran para la `sts:getCallerIdentity` API desde el espacio IP de la OCI en su historial de AWS CloudTrail rutas y eventos. Espere estos eventos cuando la utilice Oracle Database@AWS APIs.

Solución de problemas Oracle Database@AWS de identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con Oracle Database@AWS e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en Oracle Database@AWS

- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis Oracle Database@AWS recursos

No estoy autorizado a realizar ninguna acción en Oracle Database@AWS

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `odb:`*`GetWidget`*.

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

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `odb:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no está autorizado a realizar la `iam:PassRole` acción, sus políticas deben actualizarse para que pueda transferir una función a Oracle AWS Database@.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir la función al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Oracle AWS Database@. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir la función al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis Oracle Database@AWS recursos

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que respaldan las políticas basadas en recursos o las listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si Oracle Database@AWS admite estas funciones, consulte. ¿Cómo Oracle Database@AWS funciona con IAM
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad en la Cuenta de AWS Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Validación de conformidad para Oracle Database@AWS

Su responsabilidad de conformidad al utilizar Oracle Database@AWS viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. La documentación de Oracle sobre el cumplimiento en la nube está disponible en el sitio web de Oracle

Resiliencia en Oracle Database@AWS

La infraestructura AWS global se basa en Regiones de AWS zonas de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, Oracle Database@AWS ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de los datos.

Uso de roles vinculados a servicios para Oracle Database@AWS

Oracle Database@AWS utiliza funciones vinculadas al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. Oracle Database@AWS Las funciones vinculadas al servicio están predefinidas Oracle Database@AWS e incluyen todos los permisos que el servicio necesita para llamar a otras personas en su nombre. Servicios de AWS

Un rol vinculado a un servicio facilita su uso Oracle Database@AWS , ya que no es necesario añadir manualmente los permisos necesarios. Oracle Database@AWS define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo Oracle Database@AWS puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Las funciones se pueden eliminar únicamente después de eliminar primero sus recursos relacionados. Esto protege sus Oracle Database@AWS recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Permisos de rol vinculados al servicio para Oracle Database@AWS

Oracle Database@AWS utiliza el rol vinculado al servicio denominado AWSService RoleFor ODB para permitir realizar llamadas Servicios de AWS en nombre Oracle Database@AWS de sus recursos.

El rol vinculado al servicio de AWSService RoleFor ODB confía en los siguientes servicios para asumir el rol:

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

Este rol vinculado al servicio tiene una política de permisos adjunta llamada `AmazonODBServiceRolePolicy` que le otorga permisos para operar en su cuenta. Para obtener más información, consulte AWS política gestionada: Amazon ODBService RolePolicy.

> **Note**
>
> Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o función) crear, editar o eliminar la descripción de una función vinculada a un servicio. Si aparece el siguiente mensaje de error:
> Unable to create the resource. Compruebe que tiene permiso para crear un rol vinculado al servicio. Otherwise wait and try again later.
> Asegúrese de que tiene habilitados los permisos siguientes:
>
> ```
> {
>     "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 obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Crear un rol vinculado a un servicio para Oracle Database@AWS

No necesita crear manualmente un rol vinculado a servicios. Al crear una base de datos de Exadata, Oracle Database@AWS crea automáticamente el rol vinculado al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear una base de datos de Exadata, vuelve a Oracle Database@AWS crear el rol vinculado al servicio para usted.

Edición de un rol vinculado a un servicio para Oracle Database@AWS

Oracle Database@AWS no permite editar el rol vinculado al servicio de AWSService RoleFor ODB. Después de crear un rol vinculado a un servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al mismo. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Edición de un rol vinculado a un servicio en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para Oracle Database@AWS

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe eliminar todos los recursos para poder eliminar el rol vinculado al servicio.

Limpiar un rol vinculado a un servicio para Oracle Database@AWS

Antes de poder utilizar IAM para eliminar un rol vinculado a un servicio, primero debe confirmar que dicho rol no tiene sesiones activas y eliminar los recursos que utiliza.

Para comprobar si el rol vinculado a un servicio tiene una sesión activa en la consola de IAM

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en. https://console.aws.amazon.com/iam/
2. En el panel de navegación de la consola de IAM, elija Roles. A continuación, seleccione el nombre (no la casilla de verificación) de la función AWSService RoleFor ODB.
3. En la página Summary (Resumen) del rol seleccionado, elija la pestaña Access Advisor (Acceso a Advisor).
4. En la pestaña Access Advisor, revise la actividad reciente del rol vinculado al servicio.

> **Note**
>
> Si no está seguro de si Oracle Database@AWS está utilizando el rol de AWSService RoleFor ODB, puede intentar eliminarlo. Si el servicio utiliza la función, se produce un error al eliminarla y se puede ver Regiones de AWS dónde se utiliza la función. Si el rol se está utilizando, debe esperar que la sesión finalice para poder eliminarlo. No se puede revocar la sesión de un rol vinculado a servicios.

Si desea eliminar la función AWSService RoleFor ODB, primero debe eliminar todos los Oracle Database@AWS recursos.

Regiones compatibles para los roles vinculados Oracle Database@AWS al servicio

Oracle Database@AWS admite el uso de funciones vinculadas al servicio en todos los lugares en los que el servicio Regiones de AWS esté disponible. Para obtener más información, consulte Puntos de conexión y Regiones de AWS.

Oracle Database@AWS actualizaciones de las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS gestionadas Oracle Database@AWS desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del Oracle Database@AWS documento.

Cambio	Descripción	Fecha
Permisos de rol vinculados al servicio para Oracle Database@AWS: actualización de una política actual	Oracle Database@AWS agregó nuevos permisos al `AmazonODBServiceRolePolicy` rol `AWSServiceRoleForODB` vinculado al servicio. Estos permisos permiten Oracle Database@AWS hacer lo siguiente:	30 de junio de 2025

Cambio	Descripción	Fecha
	• Describa los archivos adjuntos de Amazon VPC Transit Gateways • Describa los EC2 archivos adjuntos de Amazon • Activar una EventBridge fuente de Amazon Para obtener más información, consulte Permisos de rol vinculados al servicio para Oracle Database@AWS.	
Permisos de rol vinculados al servicio para Oracle Database@AWS: actualización de una política actual	Oracle Database@AWS agregó nuevos permisos al `AmazonODBServiceRolePolicy` rol `AWSServiceRoleForODB` vinculado al servicio. Estos permisos permiten Oracle Database@AWS hacer lo siguiente: • Describe una EventBridge fuente de Amazon • Describe y crea un bus de eventos Para obtener más información, consulte Permisos de rol vinculados al servicio para Oracle Database@AWS.	26 de junio de 2025
AWS política gestionada: Amazon ODBService RolePolicy— Nueva política de funciones vinculadas a los servicios	Oracle Database@AWS agregó el `AmazonODB ServiceRolePolicy` para el rol vinculado al `AWSServiceRoleForODB` servicio. Para obtener más información, consulte AWS política gestionada: Amazon ODBService RolePolicy.	2 de diciembre de 2024
Oracle Database@AWS comenzó a rastrear los cambios	Oracle Database@AWS comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	2 de diciembre de 2024

Supervisión de Oracle Database@AWS

El monitoreo es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de Oracle Database@AWS sus demás AWS soluciones. AWS proporciona las siguientes herramientas de monitoreo para observar Oracle Database@AWS, informar cuando algo anda mal y tomar medidas automáticas cuando sea apropiado:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puedes CloudWatch hacer un seguimiento del uso de la CPU u otras métricas de tus EC2 instancias de Amazon y lanzar automáticamente nuevas instancias cuando sea necesario. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.
- Amazon CloudWatch Logs le permite supervisar, almacenar y acceder a sus archivos de registro desde EC2 instancias de Amazon y otras fuentes. CloudTrail CloudWatch Los registros pueden monitorear la información de los archivos de registro y notificarle cuando se alcanzan ciertos umbrales. También se pueden archivar los datos del registro en un almacenamiento de larga duración. Para obtener más información, consulta la Guía del usuario CloudWatch de Amazon Logs.
- Amazon se EventBridge puede utilizar para automatizar sus AWS servicios y responder automáticamente a los eventos del sistema, como los problemas de disponibilidad de las aplicaciones o los cambios de recursos. Los eventos de AWS los servicios se entregan EventBridge prácticamente en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Para obtener más información, consulta la Guía EventBridge del usuario de Amazon.
- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Monitorización Oracle Database@AWS con Amazon CloudWatch

Puede monitorizar el Oracle Database@AWS uso CloudWatch, que recopila datos sin procesar y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Estas estadísticas se mantienen durante 15 meses, de forma que pueda obtener acceso a información histórica y disponer de una mejor perspectiva sobre el desempeño de su aplicación web o servicio. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

CloudWatch Métricas de Amazon para Oracle Database@AWS

El Oracle Database@AWS servicio informa de las métricas a Amazon CloudWatch en el espacio de `AWS/ODB` nombres de los clústeres de máquinas virtuales, las bases de datos de contenedores y las bases de datos conectables.

Temas

- Métricas para clústeres de máquinas virtuales en la nube
- Métricas para bases de datos de contenedores
- Métricas para bases de datos conectables

Métricas para clústeres de máquinas virtuales en la nube

El Oracle Database@AWS servicio informa de las siguientes métricas en el espacio de `AWS/ODB` nombres de los clústeres de máquinas virtuales en la nube.

Métrica	Description (Descripción)	Unidades
`ASMDiskgroupUtilization`	El porcentaje de espacio utilizable utilizado en un grupo de discos. El espacio utilizable es el espacio disponible para el crecimiento. El grupo de discos de datos almacena nuestros archivos de base de datos Oracle. El grupo de discos RECO contiene	Porcentaje

Métrica	Description (Descripción)	Unidades
	archivos de bases de datos para su recuperación, como archivos y registros retrospectivos.	
`CpuUtilization`	El porcentaje de utilización de la CPU.	Porcentaje
`FilesystemUtilization`	El porcentaje de utilización del sistema de archivos aprovisionado.	Porcentaje
`LoadAverage`	La carga media del sistema es de más de 5 minutos.	Entero
`MemoryUtilization`	El porcentaje de memoria disponible para iniciar nuevas aplicaciones sin necesidad de intercambiarlas. La memoria disponible se puede obtener mediante el siguiente comando: `cat /proc/meminfo`	Porcentaje
`NodeStatus`	Indica si se puede acceder al host.	Entero
`OcpusAllocated`	El número de OCPUs asignados.	Entero
`SwapUtilization`	El porcentaje de utilización del espacio de intercambio total.	Porcentaje

Métricas para bases de datos de contenedores

El Oracle Database@AWS servicio informa de las siguientes métricas en el espacio de `AWS/ODB` nombres de las bases de datos de contenedores.

Métrica	Description (Descripción)	Unidades
`BlockChanges`	El número promedio de bloques cambiados por segundo.	Cambios por segundo
`CpuUtilization`	El uso de la CPU expresado como porcentaje, agregado en todos los grupos de consumidores. El porcentaj e de utilización se indica con respecto al número de bases CPUs de datos que se puede utilizar, que es el doble del número de OCPUs.	Porcentaje
`CurrentLogons`	El número de inicios de sesión correctos durante el intervalo seleccionado.	Recuento
`ExecuteCount`	El número de llamadas de usuario y recursivas que ejecutaron sentencias SQL durante el intervalo seleccion ado.	Recuento
`ParseCount`	El número de análisis duros y suaves durante el intervalo seleccionado.	Recuento
`StorageAllocated`	Cantidad total de espacio de almacenamiento asignado a la	GB

Métrica	Description (Descripción)	Unidades
	base de datos en el momento de la recopilación.	
`StorageAllocatedByTablespace`	Cantidad total de espacio de almacenamiento asignado al espacio de tablas en el momento de la recopilación. En el caso de una base de datos contenedora, esta métrica proporciona los espacios de tabla del contenedor raíz.	GB
`StorageUsed`	Cantidad total de espacio de almacenamiento utilizado por la base de datos en el momento de la recopilación.	GB
`StorageUsedByTablespace`	Cantidad total de espacio de almacenamiento utilizado por el tablespace en el momento de la recopilación. En el caso de una base de datos contenedora, esta métrica proporciona los espacios de tabla del contenedor raíz.	GB
`StorageUtilization`	El porcentaje de la capacidad de almacenamiento aprovisionada que se utiliza actualmente. Representa el espacio total asignado para todos los espacios de tablas.	Porcentaje

Métrica	Description (Descripción)	Unidades
`StorageUtilization ByTablespace`	Indica el porcentaje de espacio de almacenamiento utilizado por el tablespace en el momento de la recopilac ión. En el caso de una base de datos contenedo ra, esta métrica proporcio na los espacios de tabla del contenedor raíz.	Porcentaje
`TransactionCount`	El número combinado de confirmaciones y anulacion es de usuarios durante el intervalo seleccionado.	Recuento
`UserCalls`	El número combinado de inicios de sesión, análisis y llamadas ejecutadas durante el intervalo seleccionado.	Recuento

Métricas para bases de datos conectables

El Oracle Database@AWS servicio informa de las siguientes métricas en el espacio de `AWS/ODB` nombres de las bases de datos conectables.

Métrica	Description (Descripción)	Unidades
`AllocatedStorageUt ilizationByTablesp ace`	El porcentaje de espacio utilizado por el tablespace, de todo el espacio asignado. En el caso de las bases de datos de contenedores, esta métrica proporciona datos para los espacios de tabla de los contenedores raíz.	Porcentaje

Métrica	Description (Descripción)	Unidades
	(Estadística: media, intervalo: 30 minutos)	
AvgGCCRBlockReceiveTime	El tiempo medio de recepción del bloque CR (lectura coherente) de la caché global. Solo para bases de datos RAC o agrupadas. (Estadística: media, intervalo: 5 minutos)	Milisegundos
AvgGCCurrentBlockReceiveTime	El tiempo medio de recepción de los bloques actuales de la caché global. La estadística indica el valor medio. Solo para bases de datos de Real Application Cluster (RAC). (Estadística: media, intervalo: 5 minutos)	Milisegundos
BlockChanges	El número medio de bloques cambiados por segundo. (Estadística: media, intervalo: 1 minuto)	cambios por segundo
BlockingSessions	Sesiones de bloqueo actuales. No se aplica a las bases de datos de contenedores. (Estadística: máxima, intervalo: 15 minutos)	Recuento

Métrica	Description (Descripción)	Unidades
`CPUTimeSeconds`	La tasa media de acumulación de tiempo de CPU por parte de las sesiones en primer plano de la instancia de base de datos durante el intervalo de tiempo. El componente de tiempo de CPU del promedio de sesiones activas. (Estadística: media, intervalo: 1 minuto)	Segundos por segundo
`CpuCount`	El número de CPUs durante el intervalo seleccionado.	Recuento
`CpuUtilization`	El uso de la CPU expresado como porcentaje, agregado en todos los grupos de consumidores. El porcentaje de utilización se indica con respecto al número de bases CPUs de datos que se puede utilizar, que es el doble del número de OCPUs. (Estadística: media, intervalo: 1 minuto)	Porcentaje
`CurrentLogons`	El número de inicios de sesión correctos durante el intervalo seleccionado. (Estadísticas: suma, intervalo: 1 minuto)	Recuento

Métrica	Description (Descripción)	Unidades
DBTimeSeconds	La tasa media de acumulación de tiempo de la base de datos (CPU más espera) por las sesiones en primer plano de la instancia de base de datos durante el intervalo de tiempo. También se conoce como media de sesiones activas. (Estadística: media, intervalo: 1 minuto)	Segundos por segundo
DbmgmtJobExecutionsCount	El número de ejecuciones de trabajos de SQL en una única base de datos gestionada o en un grupo de bases de datos, y su estado. Las dimensiones de estado pueden tener los siguientes valores: «Se realizó correctamente», «No se pudo», "»InProgress. (Estadística: suma, intervalo: 1 minuto)	Recuento
ExecuteCount	El número de llamadas recursivas y de usuario que ejecutaron sentencias SQL durante el intervalo seleccionado. (Estadística: suma, intervalo: 1 minuto)	Recuento
FRASpaceLimit	El límite de espacio del área de recuperación del flash. No se aplica a las bases de datos conectables. (Estadística: máxima, intervalo: 15 minutos)	GB

Métrica	Description (Descripción)	Unidades
FRAUtilization	Utilización del área de recuperación del flash. No se aplica a bases de datos conectables. (Estadística: media, intervalo: 15 minutos)	Porcentaje
GCCRBlocksReceived	La caché global CR (lectura coherente) bloquea los bloques recibidos por segundo. Solo para bases de datos RAC o agrupadas. (Estadística: media, intervalo: 5 minutos)	Bloques por segundo
GCCurrentBlocksReceived	Representa los bloques actuales de la caché global recibidos por segundo. La estadística indica el valor medio. Solo para bases de datos de Real Application Cluster (RAC). (Estadística: media, intervalo: 5 minutos)	Bloques por segundo
IOPS	El número medio de operaciones de entrada y salida por segundo. (Estadística: media, intervalo: 1 minuto)	Operaciones por segundo
IOThroughputMB	El rendimiento medio en MB por segundo. (Estadística: media, intervalo: 1 minuto)	MB por segundo

Métrica	Description (Descripción)	Unidades
`InterconnectTraffi cMB`	La velocidad media de transferencia de datos entre los entrenudos. Solo para bases de datos RAC o agrupadas. (Estadística: media, intervalo: 5 minutos)	MB por segundo
`InvalidObjects`	Recuento de objetos de base de datos no válido. No se aplica a las bases de datos contenedoras. (Estadística: máxima, intervalo: 24 horas)	Recuento
`LogicalBlocksRead`	El número promedio de bloques leídos SGA/Memory (caché del búfer) por segundo. (Estadística: media, intervalo: 1 minuto)	Lecturas por segundo
`MaxTablespaceSize`	El tamaño máximo posible del espacio de tablas. En el caso de las bases de datos de contenedores, esta métrica proporciona datos para los espacios de tabla de los contenedores raíz. (Estadíst ica: máxima, intervalo: 30 minutos)	GB
`MemoryUsage`	Tamaño total del pool de memoria en MB. (Estadística: media, intervalo: 15 minutos)	MB

Métrica	Description (Descripción)	Unidades
MonitoringStatus	El estado de supervisión del recurso. Si se produce un error en la recopilación de métricas, la información de error se captura en esta métrica. (Estadística: media, intervalo: 5 minutos)	No aplicable
NonReclaimableFRA	El área de recuperación rápida no recuperable. No se aplica a bases de datos conectables. (Estadística: media, intervalo: 15 minutos)	Porcentaje
OcpusAllocated	El número real de OCPUs recursos asignados por el servicio durante el intervalo de tiempo seleccionado. (Estadística: recuento, intervalo: 1 minuto)	Entero
ParseCount	El número de análisis duros y suaves durante el intervalo seleccionado. (Estadística: suma, intervalo: 1 minuto)	Recuento
ParsesByType	El número de análisis duros o suaves por segundo. (Estadística: media, intervalo: 1 minuto)	Análisis por segundo
ProblematicScheduledDBMSJobs	Los trabajos problemáticos programados de la base de datos cuentan. No se aplica a las bases de datos de contenedores. (Estadística: máxima, intervalo: 15 minutos)	Recuento

Métrica	Description (Descripción)	Unidades
`ProcessLimitUtilization`	El proceso limita la utilización. No se aplica a las bases de datos conectables. (Estadística: media, intervalo: 1 minuto)	Porcentaje
`Processes`	Los procesos de la base de datos cuentan. No se aplica a las bases de datos conectables. (Estadística: máxima, intervalo: 1 minuto)	Recuento
`ReclaimableFRA`	El área de recuperación rápida recuperable. No se aplica a bases de datos conectables. (Estadística: media, intervalo: 15 minutos)	Porcentaje
`ReclaimableFRASpace`	El espacio recuperable del área de recuperación de flash. No se aplica a bases de datos conectables. (Estadística: media, intervalo: 15 minutos)	GB
`RedoSizeMB`	La cantidad media de repeticiones generadas, en MB por segundo. (Estadística: media, intervalo: 1 minuto)	MB por segundo
`SessionLimitUtilization`	El límite de utilización de la sesión. No se aplica a las bases de datos conectables. (Estadística: media, intervalo: 1 minuto)	Porcentaje

Métrica	Description (Descripción)	Unidades
`Sessions`	El número de sesiones de la base de datos. (Estadística: media, intervalo: 1 minuto)	Recuento
`StorageAllocated`	La cantidad máxima de espacio asignada por el tablespace durante el intervalo . En el caso de las bases de datos de contenedores, esta métrica proporciona datos para los espacios de tabla de los contenedores raíz. (Estadística: máxima, intervalo : 30 minutos)	GB
`StorageAllocatedBy Tablespace`	La cantidad máxima de espacio asignada por el tablespace durante el intervalo . En el caso de las bases de datos de contenedores, esta métrica proporciona datos para los espacios de tabla de los contenedores raíz. (Estadística: máxima, intervalo : 30 minutos)	GB
`StorageUsed`	La cantidad máxima de espacio utilizada durante el intervalo. (Estadística: máxima, intervalo: 30 minutos)	GB

Métrica	Description (Descripción)	Unidades
`StorageUsedByTablespace`	La cantidad máxima de espacio utilizada por el tablespace durante el intervalo. En el caso de las bases de datos de contenedores, esta métrica proporciona datos para los espacios de tabla de los contenedores raíz. (Estadística: máxima, intervalo: 30 minutos)	GB
`StorageUtilization`	El porcentaje de la capacidad de almacenamiento aprovisionada que se utiliza actualmente. Representa el espacio total asignado para todos los espacios de tablas. (Estadística: media, intervalo: 30 minutos)	Porcentaje
`StorageUtilizationByTablespace`	El porcentaje del espacio utilizado, por espacio de tabla. En el caso de las bases de datos de contenedores, esta métrica proporciona datos para los espacios de tabla del contenedor raíz. (Estadística: media, intervalo: 30 minutos)	Porcentaje
`TransactionCount`	El número combinado de confirmaciones y anulaciones de usuarios durante el intervalo seleccionado. (Estadística: suma, intervalo: 1 minuto)	Recuento

Métrica	Description (Descripción)	Unidades
`TransactionsByStatus`	El número de transacciones confirmadas o anuladas por segundo. (Estadística: media, intervalo: 1 minuto)	Transacciones por segundo
`UnusableIndexes`	Los índices inutilizables cuentan en el esquema de la base de datos. No se aplica a las bases de datos de contenedores. (Estadística: máxima, intervalo: 24 horas)	Recuento
`UsableFRA`	El área de recuperación rápida utilizable. No se aplica a bases de datos conectables. (Estadística: media, intervalo: 15 minutos)	Porcentaje
`UsedFRASpace`	El uso del espacio del área de recuperación de flash. No se aplica a bases de datos conectables. (Estadística: máxima, intervalo: 15 minutos)	GB
`UserCalls`	El número combinado de inicios de sesión, análisis y llamadas ejecutadas durante el intervalo seleccionado. (Estadística: suma, intervalo: 1 minuto)	Recuento

Métrica	Description (Descripción)	Unidades
`WaitTimeSeconds`	La tasa media de acumulación de tiempo de espera no inactivo por parte de las sesiones en primer plano de la instancia de base de datos durante el intervalo de tiempo. El componente de tiempo de espera del promedio de sesiones activas. (Estadística: media, intervalo: 5 minutos)	Segundos por segundo

CloudWatch Dimensiones de Amazon para Oracle Database@AWS

Puede filtrar los datos de Oracle Database@AWS las métricas mediante cualquier dimensión de la siguiente tabla.

Dimensión	Filtrar los datos solicitados por…
`cloudVmClusterId`	El identificador de un clúster de máquinas virtuales.
`cloudExadataInfrastructureId`	El identificador de la infraestructura de Exadata.
`collectionName`	El nombre de una colección.
`deploymentType`	El tipo de infraestructura.
`diskgroupName`	El nombre de un grupo de discos
`errorCode`	Un código de error.
`errorSeverity`	La gravedad de un error.
`filesystemName`	El nombre de un sistema de archivos.
`hostName`	El nombre de la máquina host.

Dimensión	Filtrar los datos solicitados por…
instanceName	El nombre de una instancia de base de datos.
instanceNumber	El número de instancia de una instancia de base de datos.
ioType	Un tipo de I/O operación.
jobId	Un identificador único para un trabajo.
managedDatabaseGroupId	El identificador de unManaged Database Group.
managedDatabaseId	El identificador de unManaged Database.
memoryPool	Un tipo de pool de memoria.
memoryType	Un tipo de memoria.
ociCloudVmClusterId	El identificador OCI de un clúster de máquinas virtuales.
ociCloudExadataInfrastructureId	El identificador OCI de la infraestructura de Exadata.
parseType	Un tipo de análisis.
resourceId	El identificador de un recurso.
resourceId_Database	El identificador de una base de datos.
resourceId_DbNode	El identificador de un nodo de base de datos.
resourceName	El nombre de un recurso .
resourceName_Database	El nombre de una base de datos.
resourceName_DbNode	El nombre de un nodo de base de datos.
resourceType	Tipo de base de datos.

Dimensión	Filtrar los datos solicitados por…
`schemaName`	El nombre de un esquema.
`status`	El estado de una base de datos.
`tablespaceContents`	El contenido de un espacio de tablas.
`tablespaceName`	El nombre de un tablespace.
`tablespaceType`	Un tipo de espacio de tablas.
`transactionStatus`	El estado de una transacción.
`waitClass`	Una clase de evento de espera.

Supervisión de Oracle Database@AWS eventos en Amazon EventBridge

Puede monitorear Oracle Database@AWS los eventos en EventBridge, lo que proporciona un flujo de datos en tiempo real desde las aplicaciones y AWS los servicios. EventBridge dirige estos datos a destinos como AWS Lambda Amazon Simple Notification Service.

> **Note**
>
> EventBridge anteriormente se llamaba Amazon CloudWatch Events. Para obtener más información, consulta EventBridge la evolución de Amazon CloudWatch Events en la Guía del EventBridge usuario de Amazon.

Descripción general de Oracle Database@AWS los eventos

Oracle Database@AWS los eventos son mensajes estructurados que indican cambios en los ciclos de vida de los recursos. Un bus de eventos es un router que recibe eventos y los envía a cero o más destinos u objetivos. Oracle Database@AWS los eventos se pueden generar a partir de las siguientes fuentes:

Eventos de AWS

Estos eventos se generan Oracle Database@AWS APIs de forma AWS lateral y se envían al bus de eventos predeterminado de su Cuenta de AWS.

Eventos de OCI

Estos eventos se generan directamente desde la OCI, como los relacionados con la infraestructura de Oracle Exadata o los clústeres de máquinas virtuales. Cuando se suscribe Oracle Database@AWS, se crea un bus de eventos con un prefijo `aws.partner/odb/` Cuenta de AWS para recibir los eventos de OCI.

Oracle Database@AWS eventos de AWS

Oracle Database@AWS entre los eventos se AWS incluyen los cambios en el ciclo de vida relacionados con la red ODB durante la creación y la eliminación. Estos eventos se envían al bus de eventos predeterminado de su Cuenta de AWS. El tipo de entrega es el mejor esfuerzo.

Eventos de la red ODB

Event	ID de evento	Mensaje
Creación	ODB-EVENT-0001	La red ODB se creó correctamente ODBnet_ID
Error de creación	ODB-EVENT-0011	No se pudo crear la red ODB ODBnet_ID
Eliminación	ODB-EVENT-0002	Se ha eliminado correctamente la red ODB ODBnet_ID
Error de eliminación.	ODB-EVENT-0012	No se pudo eliminar la red ODB ODBnet_ID

Ejemplo: evento de creación de red ODB

El siguiente ejemplo muestra un evento para una creación correcta de una red 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 de OCI

La mayoría de los eventos se generan directamente desde OCI. Oracle Database@AWS crea un bus de eventos con su prefijo `aws.partner/odb/` Cuenta de AWS para recibir eventos de OCI. Le recomendamos que no elimine este bus de eventos.

OCI proporciona tipos de eventos completos, incluidos los siguientes:

- Infraestructura Oracle Exadata
- Eventos de clústeres de máquinas virtuales
- Eventos de CDB
- Eventos de PDB

Para obtener más información sobre los tipos de eventos específicos y los detalles que admite OCI, consulte Oracle Exadata Database Service sobre eventos de infraestructura dedicada y eventos para Autonomous Database sobre infraestructura Exadata dedicada.

Filtrar eventos Oracle Database@AWS

Puedes seguir las prácticas EventBridge recomendadas sobre la configuración de los autobuses de eventos en los autobuses de eventos de Amazon EventBridge. En función de tus casos de uso, puedes configurar EventBridge reglas para filtrar los eventos y los objetivos para recibirlos y usarlos.

Filtrar eventos de red ODB desde AWS

Para los eventos de red ODB procedentes de AWS, puede filtrarlos mediante el siguiente patrón de eventos:

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

Puede aplicar este patrón mediante la EventBridge `put-rule` API con el bus de eventos predeterminado. Para obtener más información, consulta PutRulela referencia de la EventBridge API de Amazon.

Filtrar Oracle Database@AWS eventos de OCI

Para Oracle Database@AWS los eventos de OCI, puede configurar una regla mediante un comando similar al ejemplo de la Amazon EventBridge API Reference. PutRule Tenga en cuenta las siguientes pautas:

- Utilice un patrón de eventos personalizado en función de los tipos de eventos que desee filtrar.
- EventBusNameEstablézcalo con el nombre del autobús que lo Oracle Database@AWS creó.

Para obtener más información sobre cómo filtrar eventos y configurar EventBridge objetivos en todas las cuentas, consulta Enviar y recibir eventos entre Cuentas de AWS Amazon EventBridge.

Solución de problemas de Oracle Database@AWS eventos

Si tiene algún problema con la entrega o el contenido del evento, haga lo siguiente:

- Para eventos de la red ODB, póngase en contacto con AWS Support.
- Para Oracle Database@AWS eventos distintos de los eventos de la red ODB, póngase en contacto con Oracle Cloud Support.

Para obtener más información, consulte Obtener soporte para Oracle Database@AWS.

Registrar las llamadas a Oracle Database@AWS la API mediante AWS CloudTrail

Oracle Database@AWS está integrado con AWS CloudTrailun servicio que proporciona un registro de las acciones realizadas por un usuario, rol o un Servicio de AWS. CloudTrail captura todas las llamadas a la API Oracle Database@AWS como eventos. Las llamadas capturadas incluyen

llamadas desde la Oracle Database@AWS consola y llamadas en código a las operaciones de la Oracle Database@AWS API. Con la información recopilada por CloudTrail, puede determinar a qué solicitud se realizó Oracle Database@AWS, la dirección IP desde la que se realizó la solicitud, cuándo se realizó y detalles adicionales.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó en nombre de un usuario de IAM Identity Center.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

> **Note**
>
> Oracle Database@AWS registra las llamadas a la `GetCallerIdentity` API desde AWS Security Token Service (STS) en sus CloudTrail registros. Estas llamadas a la API de STS verifican la identidad de Oracle Database@AWS cuando interactúan con OCI en su nombre. Son una parte normal y segura de AWS las operaciones y no exponen información confidencial.

CloudTrail está activa en tu cuenta Cuenta de AWS al crear la cuenta y automáticamente tienes acceso al historial de CloudTrail eventos. El historial de CloudTrail eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de eventos de gestión registrados en un. Región de AWSPara obtener más información, consulte Uso del historial de CloudTrail eventos en la Guía del usuario.AWS CloudTrail La visualización del historial de eventos no conlleva ningún CloudTrail cargo.

Para tener un registro continuo de los eventos de Cuenta de AWS los últimos 90 días, crea un almacén de datos de eventos de senderos o CloudTraillagos.

CloudTrail senderos

Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Todos los senderos creados con él Consola de administración de AWS son multirregionales. Puede crear un registro de seguimiento de una sola región o multirregionales mediante la AWS CLI.

Se recomienda crear un sendero multirregional, ya que puedes capturar toda la actividad de tu Regiones de AWS cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS y Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail .

Puede enviar una copia de sus eventos de administración en curso a su bucket de Amazon S3 sin coste alguno CloudTrail mediante la creación de una ruta; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL en sus eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato Apache ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información sobre CloudTrail Lake, consulte Cómo trabajar con AWS CloudTrail Lake en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos y las consultas sobre eventos de Lake conllevan costes. Cuando crea un almacén de datos de eventos, debe elegir la opción de precios que desee utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el período de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

Oracle Database@AWS eventos de gestión en CloudTrail

Los eventos de administración proporcionan información sobre las operaciones de administración que se llevan a cabo en los recursos de su empresa Cuenta de AWS. Se denominan también operaciones del plano de control. De forma predeterminada, CloudTrail registra los eventos de administración.

Oracle Database@AWS registra todas las operaciones del plano de Oracle Database@AWS control como eventos de administración.

Oracle Database@AWS ejemplos de eventos

Un evento representa una solicitud única de cualquier fuente e incluye información sobre la operación de API solicitada, la fecha y la hora de la operación, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que los eventos no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra un CloudTrail evento que demuestra la `CreateOdbNetwork` operación.


```
{
    "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 obtener información sobre el contenido de los CloudTrail registros, consulte el contenido de los CloudTrail registros en la Guía del AWS CloudTrail usuario.

Solución de problemas de Oracle Database@AWS

Utilice las siguientes secciones para ayudar a solucionar los problemas de red que pueda surgir. Oracle Database@AWS

Temas

Se produce un error al crear la red ODB

Cuando no puede crear una red ODB, las causas más comunes son las siguientes:

Rangos de CIDR restringidos

La red ODB utiliza rangos de CIDR específicos para las subredes de cliente y de respaldo. Asegúrese de que los rangos de CIDR que ha elegido para estas subredes no se superpongan con ningún rango de direcciones IP restringido o reservado.

Los siguientes rangos de CIDR están reservados y no se pueden usar para la red ODB:

- Rango reservado de Oracle Cloud: 169.254.0.0/16
- Clase D reservada: 224.0.0.0 - 239.255.255.255
- Clase E reservada: 240.0.0.0 - 255.255.255
- Uso futuro de OCI: 100.105.0.0/16

Siga las EC2 reglas para los rangos de CIDR tal como se describe en la documentación de la VPC. Para obtener más información, consulta las restricciones de asociación de bloques del CIDR.

Además, evite la superposición entre los rangos de CIDR específicos y los que se utilizan para la conectividad de la VPC a la red ODB.

CIDR de VPC superpuesto

El rango de CIDR que especificó para la red ODB no debe superponerse con los rangos de CIDR utilizados por ninguno de los que ya tiene. VPCs La superposición de los rangos de CIDR puede

provocar conflictos de enrutamiento e impedir la creación correcta de la red ODB. Compruebe los rangos CIDR del emparejamiento ODB VPCs y asegúrese de que el CIDR de la red ODB sea único y no se superponga.

Propiedad de VPCs

La red ODB y la VPC a la que se está conectando deben pertenecer a la AWS misma cuenta. Si intentas conectar la red ODB a una VPC propiedad de otra cuenta, se producirá un error en la creación. Compruebe que la red ODB y la VPC pertenezcan a la AWS misma cuenta.

Falta de una puerta de enlace de tránsito

Si agrega un rango de CIDR a la lista de CIDR emparejados de la red ODB sin adjuntar una puerta de enlace de tránsito a la VPC, se produce un error en la operación de creación o actualización. No hay ningún requisito en cuanto a los rangos de CIDR para los que se utiliza el adjunto.

Problemas de conectividad entre la red de VPC y ODB o los clústeres de máquinas virtuales

Cuando no puedes conectarte desde tu VPC a la red ODB o a los clústeres de máquinas virtuales que contiene, las siguientes son las causas más comunes:

- Verificación de la configuración de la VPC: en Oracle Database@AWS la consola, localice la VPC que está emparejada con la red ODB. Confirme que el ID de VPC coincide con el que se muestra en los detalles de la red ODB.
- Inspeccionar las tablas de enrutamiento: en la consola de Amazon VPC, busque la tabla de enrutamiento adjunta a la subred en la que se ejecuta la aplicación. Compruebe si hay una ruta con un CIDR de destino que coincida con el CIDR de la subred del cliente de la red ODB. Confirme que esta ruta apunta al ARN de la red ODB correcto. Si falta la ruta, añada una nueva al CIDR de la subred de clientes de la red ODB.
- Validación entre pares CIDRs: consulte la `Peered CIDRs` sección de detalles de la red ODB. Confirme que todos los bloques CIDR relevantes de su VPC estén en la lista. Si falta un CIDR obligatorio, actualice el IDR emparejado. CIDRs
- Comprobación de las reglas de los grupos de seguridad: en la EC2 consola de Amazon, localice los grupos de seguridad de los recursos de su VPC. Revise las reglas de entrada y salida y actualícelas según sea necesario para permitir el tráfico necesario.

- Confirmación de las zonas de disponibilidad: en la consola de Amazon VPC, identifique la zona de disponibilidad (AZ) de la subred. Compruebe que la red ODB también esté desplegada en la misma zona de disponibilidad que su subred.
- Evitar múltiples conexiones de emparejamiento de red ODB: compruebe las conexiones de emparejamiento de VPC en la consola. Oracle Database@AWS Asegúrese de tener solo una conexión activa a una red ODB. Si ve más de una red ODB interconectada, elimine las adicionales.

Nombres de host o nombres de escaneo irresolubles de clústeres de máquinas virtuales de VPC

Si los nombres de host o los nombres de escaneo de los clústeres de máquinas virtuales no se pueden resolver desde la VPC, configure el reenvío de DNS en la VPC y los siguientes recursos para resolver los registros de DNS alojados en la red ODB:

- Un punto final de salida para enviar consultas de DNS a la red ODB. Para obtener más información, consulte Configurar un punto final de salida en una red ODB en Oracle Database@AWS.
- Una regla de resolución para especificar el nombre de dominio de las consultas de DNS que la resolución reenvía al DNS para la red ODB. Para obtener más información, consulte Configurar una regla de resolución en Oracle Database@AWS.

Obtener soporte para Oracle Database@AWS

Descubra cómo obtener información y soporte para Oracle Database@AWS.

Alcance del soporte e información de contacto de Oracle

Oracle Cloud Support es la primera línea de soporte para todas las preguntas sobre Oracle Database@AWS . Para ponerse en contacto con el servicio de asistencia, inicie sesión en la consola de Oracle Cloud Infrastructure (OCI) y, a continuación, seleccione el icono de la balsa salvavidas. Si no tiene una cuenta de My Oracle Cloud Support, consulteCuentas y acceso a My Oracle Cloud Support.

Entre los ejemplos de problemas con los que Oracle Support puede ayudarlo se incluyen los siguientes:

- Problemas de conexión a la base de datos (Oracle TNS)

- Problemas de rendimiento de la base de datos Oracle
- Resolución de errores de Oracle Database
- Problemas de red relacionados con las comunicaciones con el arrendamiento de la OCI asociado al servicio
- La cuota (límites) aumenta para recibir más capacidad (para obtener más información, consulte Solicitar un aumento del límite para los recursos de la base de datos)
- Ampliación para añadir más capacidad de cómputo y almacenamiento a su infraestructura de bases de datos Oracle
- Actualizaciones de hardware de nueva generación
- Problemas de facturación relacionados con sus AWS Marketplace cargos

Si necesita ponerse en contacto con Oracle Support fuera de la consola OCI, dígale a su agente de Oracle Support que su problema está relacionado con Oracle AWS Database@. Esto se debe a que las solicitudes de este servicio las gestiona un equipo de soporte de OCI especializado en estas implementaciones.

Contactar con el soporte de Oracle por teléfono

1. Llame al 1-800-223-1711. Si se encuentra fuera de los Estados Unidos, visite el directorio global de contactos de soporte de Oracle para encontrar la información de contacto de su país o región.
2. Seleccione la opción «2" para abrir una nueva solicitud de servicio (SR).
3. Elija la opción «4" para «no estoy seguro».
4. Informe al agente de que tiene un problema con su sistema multinube y dígale el nombre del producto. Se abrirá una solicitud de servicio interna en su nombre y un ingeniero de soporte de OCI se pondrá en contacto con usted directamente.

También puede enviar una pregunta al foro Multicloud de la comunidad Cloud Customer Connect de Oracle. Esta opción está disponible para todos los clientes.

Cuentas y acceso a My Oracle Cloud Support

Para crear tickets de solicitud del servicio My Oracle Cloud Support, el administrador del AWS servicio Oracle Database@ de su organización debe aprobar su solicitud. Si es el AWS

administrador de Oracle Database@, complete las instrucciones de incorporación de My Oracle Cloud Support incluidas en el correo electrónico de activación del servicio Oracle AWS Database@.

Encontrará instrucciones para la incorporación a My Oracle Cloud Support en los siguientes temas:

- Configuración de su cuenta Oracle Support
- Creación de una solicitud de soporte

Para obtener instrucciones sobre cómo autorizar a los usuarios a abrir las solicitudes de soporte de My Oracle Cloud Support, consulte Administrator Tasks for Support.

AWS Support alcance e información de contacto

AWS Support es su primera línea de asistencia para todos los problemas y preguntas AWS relacionados. Cree un AWS Support caso para su problema, tal como lo hace con otros AWS servicios. El AWS Support equipo colabora con OCI Support según sea necesario.

Algunos ejemplos de AWS problemas de Oracle Database@ que AWS Support pueden ayudarle son los siguientes:

- Problemas relacionados con las redes virtuales, incluidos los relacionados con la traducción de direcciones de red (NAT), los firewalls, la gestión del tráfico y el DNS, y las subredes AWS
- Problemas de Bastion y máquinas virtuales (VM), como la conexión del host de la base de datos, la instalación del software, la latencia y el rendimiento del host
- Informes de métricas de clústeres de máquinas virtuales de Exadata en Amazon CloudWatch
- Problemas de facturación relacionados con los servicios AWS

Para obtener información sobre AWS Support, consulte Cómo empezar con AWS Support.

Acuerdos de nivel de servicio de Oracle

Si tiene preguntas sobre los acuerdos de nivel de AWS servicio de Oracle Database@ (SLAs) o desea solicitar créditos de servicio por incumplimiento de los SLA, póngase en contacto con su gerente de cuentas de Oracle. Consulte los acuerdos de nivel de servicio para obtener más información.

Cuotas para Oracle Database@AWS

Oracle Database@AWS es una oferta multinube. AWS no establece ni impone cuotas de Oracle Database@AWS recursos. Oracle Cloud Infrastructure (OCI) aplica las cuotas. Para obtener más información sobre las cuotas de OCI, consulte Cuotas y límites de servicio en la documentación de Oracle Cloud Infrastructure.

Historial de documentos de la Guía Oracle Database@AWS del usuario

En la siguiente tabla se describen las versiones de la documentación de Oracle Database@AWS.

Cambio	Descripción	Fecha
Oracle Database@AWS apoya la región de Asia Pacífico (Sídney) y la región de Canadá (Central)	Puede crear sus Oracle Database@AWS recursos en estas regiones. Para obtener más información, consulte Regiones compatibles para Oracle Database@AWS.	2 de febrero de 2026
Oracle Database@AWS apoya la región de Asia Pacífico (Tokio), la región EE.UU. Este (Ohio) y la región Europa (Fráncfort)	Puede crear sus Oracle Database@AWS recursos en estas regiones. Para obtener más información, consulte Regiones compatibles para Oracle Database@AWS.	22 de diciembre de 2025
Oracle Database@AWS apoya el reparto de derechos entre Cuentas de AWS	Ahora puede compartir los derechos de AWS Marketplace para Oracle Database@ Cuentas de AWS en la misma AWS organización mediante AWS License Manager. AWS Para obtener más información, consulte Distribución de derechos en Oracle Database@.AWS	19 de diciembre de 2025
Oracle Database@AWS admite la modificación de los filtros de datos de integración sin ETL	Oracle Database@AWS admite la modificación de los filtros de datos para las integraciones sin ETL	15 de octubre de 2025

	existentes con Amazon Redshift. Puede actualizar los patrones de filtro de datos para incluir o excluir esquemas y tablas específicos de la replicación de datos. Para obtener más información, consulte Administración de integraciones sin ETL.	
Oracle Database@AWS admite la administración CIDR de redes homólogas para conexiones entre pares	Puede especificar una red homóloga CIDRs al crear o actualizar las conexiones de emparejamiento ODB. Usted controla qué subredes de la VPC homóloga tienen acceso a su red ODB. Una cuenta de VPC puede actualizar los rangos de CIDR sin ser propietaria también de la red ODB. Para obtener más información, consulte Configuración del emparejamiento de ODB a una Amazon VPC en. Oracle Database@AWS	10 de octubre de 2025
Oracle Database@AWS admite la integración sin ETL con Amazon Redshift	Oracle Database@AWS ahora se integra con VPC Lattice para permitir la integración sin ETL con Amazon Redshift. Para obtener más información, consulte Integraciones de servicios para Oracle Database@.AWS	2 de julio de 2025

Actualización de permisos de roles vinculados a servicios de IAM	La `AmazonODBServiceRolePolicy` política ahora otorga permisos adicionales para describir los adjuntos de la pasarela de tránsito de la VPC, describir las EC2 subredes de Amazon y activar una fuente de Amazon. EventBridge Para obtener más información, consulte Oracle Database@AWS las actualizaciones de las políticas AWS gestionadas.	30 de junio de 2025
Actualización de permisos de roles vinculados a servicios de IAM	La `AmazonODBServiceRolePolicy` política ahora otorga permisos adicionales para describir eventos en Amazon EventBridge Scheduler y crear o describir un bus de eventos. Para obtener más información, consulte Oracle Database@AWS las actualizaciones de las políticas AWS gestionadas.	26 de junio de 2025
Oracle Database@AWS es compatible con la región EE.UU. Oeste (Oregón)	Puede crear sus Oracle Database@AWS recursos en la región EE.UU. Oeste (Oregón). Las AZ físicas compatibles IDs son `usw2-az3` y`usw2-az4`. Para obtener más información, consulte las regiones compatibles para Oracle Database@AWS.	26 de junio de 2025

Oracle Database@AWS permite el intercambio de recursos entre Cuentas de AWS	Ahora puede compartir la infraestructura y los clústeres de máquinas virtuales de Exadata con otras personas Cuentas de AWS de su organización mediante AWS Resource Access Manager ()AWS RAM. Puede aprovisionar la infraestructura una vez y compartirla entre varias cuentas, lo que reduce los costos y mantiene la separación de responsabilidades. Para obtener más información, consulte Uso compartido de recursos en Oracle Database@AWS.	26 de junio de 2025
Oracle Database@AWS apoya eventos en Amazon EventBridge	Oracle Database@AWS envía eventos a Amazon EventBridge para monitorear los cambios en el ciclo de vida de los recursos. Los eventos se generan tanto AWS a partir de fuentes OCI como de fuentes OCI, lo que le permite realizar un seguimiento de los cambios en la red ODB, la infraestructura de Exadata, los clústeres de máquinas virtuales y las bases de datos. Para obtener más información, consulta Monitorización de Oracle Database@AWS eventos en Amazon EventBridge.	26 de junio de 2025

Oracle Database@AWS admite la suscripción entre regiones	Oracle Database@AWS admite la suscripción entre regiones, lo que le permite suscribirse una vez y utilizar el servicio en todas las opciones disponibles. Regiones de AWS Para obtener más información, consulte Suscríbase a Oracle Database@AWS en varias regiones.	26 de junio de 2025
Oracle Database@AWS admite las conexiones de interconexión ODB como un recurso independiente	Las conexiones de interconexión ODB son ahora un recurso independiente dedicado APIs a crear, ver y eliminar conexiones de interconexión. Puede crear conexiones de emparejamiento entre una red ODB y una Amazon VPC en la misma cuenta o en cuentas diferentes. Para obtener más información, consulte Trabajar con conexiones de emparejamiento ODB.	26 de junio de 2025
Oracle Database@AWS integra la red ODB con Amazon S3	Oracle Database@AWS ahora se integra con VPC Lattice para permitir las copias de seguridad gestionadas por Oracle en Amazon S3 y el acceso directo a la red ODB a Amazon S3. Para obtener más información, consulte Integraciones de servicios para Oracle Database@.AWS	26 de junio de 2025

Oracle Database@AWS admite clústeres de máquinas virtuales autónomos	Ahora puede crear clústeres de máquinas virtuales autónomas en su infraestructura de Exadata. Los clústeres de máquinas virtuales autónomas son bases de datos totalmente administradas que automatizan las tareas de administración clave mediante el aprendizaje automático y la inteligencia artificial. Para obtener más información, consulte el paso 3: Crear un clúster de máquinas virtuales de Exadata o un clúster de máquinas virtuales autónomas en. Oracle Database@AWS	28 de mayo de 2025
Oracle Database@AWS admite ventanas de mantenimiento personalizables	Ahora puede configurar los períodos de mantenimiento para su infraestructura de Exadata con opciones de cronogramas gestionados por Oracle o gestionados por el cliente. También puede seleccionar los modos de aplicación de parches (continuos o no continuos) y especificar las preferencias de tiempo de mantenimiento. Para obtener más información, consulte Crear una infraestructura de Oracle Exadata en. Oracle Database@AWS	1 de mayo de 2025

Oracle Database@AWS admite una nueva zona de disponibilidad (AZ)	Ahora puede crear una red ODB en una zona de disponibilidad con el identificador físico `use1-az4` o `use1-az6`. Para obtener más información, consulte la infraestructura de Oracle Exadata.	26 de marzo de 2025
Oracle Database@AWS es compatible con Amazon VPC Transit Gateways	Si conecta una puerta de enlace de tránsito a una VPC que está interconectada a una red ODB, puede conectar varias VPCs a esta puerta de enlace. Las aplicaciones que se ejecutan en ellas VPCs pueden acceder a un clúster de máquinas virtuales de Exadata que se ejecute en su red ODB. Para obtener más información, consulte Configuración de Amazon VPC Transit Gateways para. Oracle Database@AWS	26 de marzo de 2025
Oracle Database@AWS admite tipos de servidores de bases de datos y almacenamiento para el Exadata X11M	Puede especificar el tipo de servidor de base de datos y el tipo de servidor de almacenamiento al crear una infraestructura con Exadata X11M. Para obtener más información, consulte Crear una infraestructura de Oracle Exadata en. Oracle Database@AWS	4 de febrero de 2025

Nueva política de funciones vinculadas al servicio	Oracle Database@AWS se agregó una nueva política `AmazonODBServiceRolePolicy` para el rol vinculado al `AWSServiceRoleForODB` servicio. Para obtener más información, consulte Actualizaciones de Oracle Database@AWS a políticas administradas de AWS.	2 de diciembre de 2024
Versión inicial	Versión inicial de la Guía del usuario Oracle Database@AWS	2 de diciembre de 2024

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.