Oracle Database@AWS Guida per l'utente

Oracle Database@AWS

Oracle Database@AWS: Oracle Database@AWS Guida per l'utente

Table of Contents

Che cos'è Oracle Database@AWS?

Oracle Database@AWS è un'offerta che consente di accedere all'infrastruttura Oracle Exadata gestita da Oracle Cloud Infrastructure (OCI) all'interno AWS dei data center. Puoi migrare i tuoi carichi di lavoro Oracle Exadata, stabilire una connettività a bassa latenza con le applicazioni in esecuzione e integrarli con i servizi. AWS AWS Riceverai un'unica fattura Marketplace AWS, che viene conteggiata ai fini AWS degli impegni e dei premi Oracle Support.

Il diagramma seguente mostra una panoramica di alto livello di una regione OCI collegata a un AWS data center che ospita l'infrastruttura Oracle Exadata. All'interno di una zona di AWS disponibilità (AZ), puoi peer di un Amazon VPC su una rete privata collegata al data center. Grazie al peering di queste reti, i server delle applicazioni nel VPC possono accedere ai database Oracle in esecuzione sull'infrastruttura Oracle Exadata.

Caratteristiche di Oracle Database@AWS

Con Oracle Database@AWS, puoi beneficiare delle seguenti funzionalità:

Migrazione dei carichi di lavoro del database Oracle Exadata a AWS

Con Oracle Database@AWS, puoi migrare facilmente i tuoi carichi di lavoro Oracle Exadata verso Oracle Exadata Database Service su Dedicated Infrastructure o Oracle Autonomous Database su Dedicated Exadata Infrastructure all'interno. AWS La migrazione offre modifiche minime, disponibilità completa delle funzionalità, compatibilità architetturale e le stesse prestazioni delle implementazioni Exadata locali. È possibile utilizzare strumenti di migrazione del database Oracle standard come Recovery Manager (RMAN), Oracle Data Guard, tablespace trasportabili, Oracle Data Pump, Oracle, AWS Database Migration GoldenGate Service e Oracle Zero Downtime Migration.

Latenza delle applicazioni ridotta

È possibile stabilire una connettività a bassa latenza tra Oracle Exadata e le applicazioni in esecuzione su. AWS La vicinanza alle applicazioni ospitate in rete AWS garantisce ritardi di rete minimi e prestazioni migliorate.

Innovazione attraverso l'unificazione dei dati

Puoi generare informazioni più approfondite e sviluppare nuove innovazioni utilizzando integrazioni zero-ETL per unificare i dati su Oracle e AWS per l'analisi, l'apprendimento

automatico e l'intelligenza artificiale generativa. Con l'integrazione zero-ETL con Amazon Redshift, puoi abilitare analisi e apprendimento automatico (ML) quasi in tempo reale sui dati transazionali archiviati in. Oracle Database@AWS

Gestione e operazioni semplificate

Puoi beneficiare di un'esperienza unificata tra Oracle e AWS di supporto, acquisti, gestione e operazioni collaborativi. L'utilizzo dei servizi di database Oracle è idoneo per AWS gli impegni esistenti e i vantaggi delle licenze Oracle, come Oracle Support Rewards. È possibile utilizzare AWS strumenti e interfacce familiari per acquistare, fornire e gestire le Oracle Database@AWS risorse. È possibile effettuare il provisioning e gestire le risorse utilizzando AWS APIs, CLI o. SDKs AWS APIs Richiama l'OCI corrispondente APIs necessario per fornire e gestire le risorse.

Integrazione perfetta con i servizi AWS

È possibile l'integrazione con altri AWS servizi e applicazioni in esecuzione nello stesso ambiente. Ad esempio, Oracle Database@AWS si integra con Amazon EC2, Amazon VPC e IAM. Puoi anche integrarti Oracle Database@AWS con AWS servizi come Amazon CloudWatch per il monitoraggio e Amazon EventBridge per la gestione degli eventi. Per i backup dei database, puoi usare Amazon S3, progettato per superare gli 119 secondi di durabilità.

Correlati Servizi AWS

Oracle Database@AWS collabora con i seguenti servizi per migliorare la disponibilità e la scalabilità delle applicazioni di database Oracle:

- Amazon EC2: fornisce server virtuali che funzionano come server di applicazioni Oracle. È possibile configurare il sistema di bilanciamento del carico per indirizzare il traffico verso i server EC2 delle applicazioni. Per ulteriori informazioni, consulta la Amazon EC2 User Guide.
- Amazon Virtual Private Cloud (VPC): consente di avviare AWS risorse in una rete virtuale logicamente isolata che hai definito. L'infrastruttura Oracle Exadata risiede in una rete speciale chiamata rete ODB che è possibile collegare a un VPC. Puoi quindi eseguire server di applicazioni nel tuo VPC e accedere ai tuoi database Exadata. Per ulteriori informazioni, consulta la Guida utente Amazon VPC.
- Amazon VPC Lattice: fornisce accesso nativo a AWS servizi come Amazon S3 e backup gestiti da Oracle dalla rete ODB. Per ulteriori informazioni, consulta la sezione Cos'è Amazon VPC Lattice? .

- Amazon CloudWatch: fornisce un servizio di monitoraggio per Oracle Database@AWS. OCI raccoglie i dati metrici sul tuo sistema Oracle Exadata e li invia a. CloudWatch Per ulteriori informazioni, consulta Monitoraggio Oracle Database@AWS con Amazon CloudWatch.
- AWS Identity and Access Management (IAM): ti aiuta a controllare in modo sicuro l'accesso alle risorse per Oracle Database@AWS i tuoi utenti. Usa IAM per controllare chi può utilizzare AWS le tue risorse (autenticazione) e quali risorse gli utenti possono utilizzare in quali modi (autorizzazione). Per ulteriori informazioni, consulta Gestione delle identità e degli accessi per Oracle Database@AWS.
- AWS servizi di analisi: offri un set ampio ed economico di servizi di analisi per aiutarti a ottenere informazioni più velocemente dal tuo database Exadata. Ogni servizio è progettato appositamente per un'ampia gamma di casi d'uso di analisi, come analisi interattiva, elaborazione di big data, data warehousing, analisi in tempo reale, analisi operative, dashboard e visualizzazioni. Per ulteriori informazioni, consulta Analytics on. AWS

Accesso Oracle Database@AWS

È possibile creare, accedere e gestire Oracle Database@AWS utilizzando Console di gestione AWS. Fornisce un'interfaccia web che è possibile utilizzare per accedere Oracle Database@AWS.

Prezzi per Oracle Database@AWS

Puoi acquistare Oracle Database@AWS offerte da Marketplace AWS. Per prima cosa contatta un rappresentante di vendita Oracle. Oracle rende quindi disponibile l'offerta in Marketplace AWS base al contratto di prezzo privato. La AWS fattura mostra gli addebiti in base all'utilizzo.

Non sono previsti costi di trasferimento dei dati quando l'applicazione Oracle e il database Oracle sono ospitati nella stessa zona di disponibilità (AZ). Le tariffe standard per il trasferimento dei dati si applicano per le comunicazioni tra AZs.

Quando si utilizzano integrazioni Oracle Database@AWS gestite come Zero-ETL, Oracle managed backup e Amazon S3, si applicano i costi di elaborazione dei dati standard per la condivisione e l'accesso alle risorse tramite VPC Lattice. Non è previsto alcun costo orario per le integrazioni gestite. Oracle Database@AWS Per ulteriori informazioni, consulta i prezzi di Amazon VPC Lattice.

Fasi successive

Ora sei pronto per iniziare a creare le tue Oracle Database@AWS risorse.

1. Scopri come Oracle Database@AWS funziona. Per ulteriori informazioni, consulta Come Oracle Database@AWS funziona.

   > **Note**
   >
   > Se conosci Oracle Exadata e vuoi iniziare subito, salta questo passaggio. AWS

2. Richiedi un'offerta privata Oracle Database@AWS tramite e poi accetta Console di gestione AWS l'offerta. Per ulteriori informazioni, consulta Richiedi un'offerta privata per Oracle Database@AWS.

   > **Note**
   >
   > Per richiedere un'offerta privata in questa anteprima, devi contattarci AWS per farla Account AWS aggiungere a un elenco consentito.

3. Crea la tua rete ODB, l'infrastruttura Oracle Exadata e i cluster di macchine virtuali Exadata utilizzando la console. AWS Crea i tuoi database Exadata utilizzando gli strumenti OCI. Per ulteriori informazioni, consulta Guida introduttiva a Oracle Database@AWS.
4. Condividi le tue risorse tra gli account con AWS Resource Access Manager ()AWS RAM. Per ulteriori informazioni, consulta Utilizzo di Oracle Database@AWS risorse condivise in un account affidabile.

Come Oracle Database@AWS funziona

Oracle Database@AWS integra Oracle Cloud Infrastructure (OCI) con. Cloud AWS Nelle sezioni seguenti, puoi conoscere i componenti chiave di questa architettura multicloud.

Oracle Exadata Database Service on Dedicated Infrastructure è un servizio OCI che fornisce Exadata Database Machine. Oracle Exadata Database Machine è una piattaforma full stack integrata, preconfigurata e pretestata da utilizzare nei data center aziendali. È possibile creare l'infrastruttura Oracle Exadata e i cluster VM in una zona di AWS disponibilità (AZ) utilizzando la console AWS , la CLI o. APIs

Dopo aver creato le risorse in AWS, si utilizza OCI APIs per creare e gestire i database Oracle Exadata. Una rete ODB, che esegui il peering su un Amazon VPC, consente ai server delle EC2 applicazioni Amazon di accedere ai tuoi database Exadata. In questo modo, i database Oracle Exadata sono integrati nell'ambiente. AWS

Il diagramma seguente mostra l'architettura. Oracle Database@AWS

Siti secondari OCI

L'infrastruttura Oracle Cloud è ospitata nelle regioni e nei domini di disponibilità OCI. Una regione OCI è costituita da domini di disponibilità OCI (ADs), che sono cluster di data center isolati all'interno di una regione OCI. Un sito figlio OCI è un data center che estende un dominio di disponibilità OCI a una zona di disponibilità (AZ) in una AWS regione. L'infrastruttura Exadata risiede logicamente in una regione OCI e risiede fisicamente in una regione. AWS

Il sito secondario OCI per risiede Oracle Database@AWS fisicamente in un AWS data center. AWS ospita l'infrastruttura Exadata e OCI fornisce e gestisce l'hardware dell'infrastruttura Exadata all'interno del data center. È possibile configurare l'infrastruttura Exadata, la rete privata e i cluster VM utilizzando la console AWS , la CLI o. APIs Puoi utilizzare AWS servizi come Amazon EC2 e Amazon VPC per consentire l'accesso delle applicazioni ai database Oracle Exadata in esecuzione sull'infrastruttura.

Infrastruttura Oracle Exadata

L'infrastruttura Oracle Exadata è l'architettura alla base dei server di database e dei server di storage che esegue i database Oracle Exadata. L'infrastruttura risiede in una zona di AWS disponibilità (AZ). Per creare cluster di macchine virtuali sull'infrastruttura Exadata, si utilizza la console AWS , la CLI o. APIs

L'infrastruttura Oracle Exadata è distribuita su macchine fisiche chiamate server di database. Questi server forniscono le risorse di elaborazione, in modo simile ai server EC2 dedicati di Amazon. Ogni server di database ospita una o più macchine virtuali (VMs) in esecuzione su un hypervisor. Per i diagrammi architettonici che illustrano queste relazioni, consulta Exadata Database Service on Dedicated Infrastructure Technical Architecture.

Quando si crea l'infrastruttura Exadata in Oracle AWS Database@, si specificano informazioni come le seguenti:

- Il numero totale di server di database
- Il numero totale di server di storage
- Il modello di sistema Exadata (X11M)
- L'AZ che ospita l'infrastruttura (vedi) Regioni supportate per Oracle Database@AWS

Per informazioni su come creare un'infrastruttura Oracle Exadata, vedi. Fase 2: Creare un'infrastruttura Oracle Exadata in Oracle Database@AWS

Rete ODB

Una rete ODB è una rete privata isolata che ospita l'infrastruttura OCI in una zona di AWS disponibilità (AZ). La rete ODB è costituita da un intervallo CIDR di indirizzi IP. La rete ODB si collega direttamente alla rete esistente all'interno del sito secondario OCI, fungendo così da mezzo di comunicazione tra e AWS OCI. È necessario specificare una rete ODB quando si creano i cluster Exadata VM (vedere). Fase 3: Creare un cluster di macchine virtuali Exadata o un cluster di macchine virtuali autonome in Oracle Database@AWS

Si forniscono risorse in una rete ODB utilizzando Oracle Database@.AWS APIs La rete ODB è gestita da AWS, ma è possibile configurare una connessione peering ODB per connettere un Amazon VPC alla rete ODB. Per ulteriori informazioni, consulta en. Peering ODB

Quando si crea una rete ODB, si specificano informazioni come le seguenti:

- Zona di disponibilità: la rete ODB è specifica di una zona AZ.

  È possibile utilizzare Oracle Database@AWS quanto segue: Regioni AWS

  Stati Uniti orientali (Virginia settentrionale)

  È possibile utilizzare il AZs con il comando fisico IDs `use1-az4` `euse1-az6`.

  Stati Uniti occidentali (Oregon)

  Puoi usarli AZs con il fisico IDs `usw2-az3` `eusw2-az4`.

  Asia Pacifico (Tokyo)

  Puoi usarli AZs con il fisico IDs `apne1-az1` `eapne1-az4`.

  Stati Uniti orientali (Ohio)

  Puoi usarli AZs con il fisico IDs `use2-az1` `euse2-az2`.

  Europa (Francoforte)

  Puoi usarli AZs con il fisico IDs `euc1-az1` `eeuc1-az2`.

  Canada (Centrale)

  È possibile utilizzare l'AZ con l'ID fisico`cac1-az4`.

  Asia Pacifico (Sydney)

  È possibile utilizzare l'AZ con l'ID fisico`apse2-az4`.

  Per trovare i nomi AZ logici nel tuo account che corrispondono alla precedente AZ fisica IDs, esegui il comando seguente.

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

- Indirizzi CIDR dei client: la rete ODB richiede una sottorete client CIDR per i cluster di macchine virtuali Exadata e i cluster di macchine virtuali autonome.

- Indirizzi CIDR di backup: la rete ODB richiede una sottorete di backup CIDR per i backup gestiti del database dei cluster di macchine virtuali. La sottorete di backup è facoltativa per i cluster VM Exadata.
- AWS integrazioni di servizi: puoi configurare un percorso di rete per integrazioni di AWS servizi come Amazon S3 e Zero-ETL con Amazon Redshift. Per ulteriori informazioni, consulta AWS integrazioni di servizi.

Per ulteriori informazioni, consulta Fase 1: Creare una rete ODB in Oracle Database@AWS.

Virtual Private Cloud (VPC)

Un Virtual Private Cloud (VPC) è una rete virtuale creata nel cloud. AWS È isolato logicamente dalle altre reti virtuali nel AWS cloud e offre il controllo completo sull'ambiente di rete virtuale, inclusa la selezione del proprio intervallo di indirizzi IP, la creazione di sottoreti e la configurazione delle tabelle di routing e dei gateway di rete. Per ulteriori informazioni, consulta Cos'è Amazon VPC?

Puoi avviare EC2 istanze Amazon nel tuo Amazon VPC. Le EC2 istanze possono ospitare server di applicazioni che comunicano con i database Oracle Exadata. Puoi gestire e avviare i server delle applicazioni proprio come qualsiasi altra EC2 istanza nel tuo VPC. Per ulteriori informazioni, consulta What is Amazon EC2?

Per impostazione predefinita, la rete ODB non dispone di connettività a VPCs. Per connettere la rete ODB all' AWS infrastruttura esistente, crea una connessione peering tra la rete ODB e un VPC. È possibile specificare il VPC quando si crea la rete ODB. Per ulteriori informazioni, consulta Fase 1: Creare una rete ODB in Oracle Database@AWS.

Peering ODB

Il peering ODB è una connessione di rete creata dall'utente che consente l'instradamento privato del traffico tra un Amazon VPC e una rete ODB. Esiste una relazione 1:1 tra un VPC e una rete ODB. Dopo il peering, un' EC2 istanza Amazon all'interno del VPC può comunicare con un database Oracle Exadata nella rete ODB come se si trovasse all'interno della stessa rete.

> **Note**
>
> Il peering ODB è diverso dal peering VPC, che è una connessione peering tra due VPCs che indirizza il traffico tra di loro.

È possibile peerizzare una rete ODB in un account e un VPC in un altro account utilizzando. AWS RAM Se condividi una rete ODB con un altro account, l'account trust può avviare direttamente il peering. L'account che avvia la connessione peering ODB possiede e gestisce la connessione.

È possibile specificare una rete peer CIDRs quando si creano o si aggiornano le connessioni peering ODB. In questo modo, puoi controllare quali sottoreti del VPC peer hanno accesso alla tua rete ODB. Un account VPC può aggiornare gli intervalli CIDR senza possedere anche la rete ODB. Per ulteriori informazioni, consulta Configurazione del peering ODB su un Amazon VPC in. Oracle Database@AWS

Le risorse in un VPC possono estendersi su zone di disponibilità (). AZs In una rete ODB, le risorse sono legate a una singola AZ. Questa AZ viene definita quando si crea la rete ODB.

Creazione di una connessione peering ODB

Una connessione peering ODB non è una caratteristica di una rete ODB ma è una risorsa indipendente con un proprio ID (con il prefisso) e un ciclo di vita. `odbpcx-` È possibile gestire una connessione peering con un set di connessioni dedicate. APIs Ad esempio, si crea una connessione peering ODB a una rete ODB esistente utilizzando la console Oracle AWS Database@ o l'API. `CreateOdbPeeringConnection` Per ulteriori informazioni, consulta Creazione di una connessione peering ODB in Oracle Database@AWS.

Quando si crea una connessione peering ODB, Oracle Database@ esegue automaticamente le seguenti azioni:AWS

1. Convalida le configurazioni di rete, inclusa la verifica della presenza di blocchi CIDR sovrapposti con Oracle VCN CIDR
2. Configura l'infrastruttura di peering di rete sottostante
3. Configura le tabelle di routing della rete ODB (non il VPC) con gli indirizzi CIDR VPC

Dopo aver creato la connessione peering ODB, aggiorna manualmente le tabelle di routing VPC utilizzando il comando Amazon. EC2 `create-route` Per ulteriori informazioni, consulta Configurazione delle tabelle di routing VPC per il peering ODB.

AWS integrazioni di servizi

Per fornire funzionalità e opzioni di connettività avanzate per i database Oracle, Oracle Database@AWS si integra con Servizi AWS Amazon VPC Lattice. Puoi configurare i percorsi di rete Servizi AWS direttamente dalla tua rete ODB senza richiedere configurazioni di rete aggiuntive o complesse. VPCs

Oracle Database@AWS supporta le seguenti integrazioni di servizi gestiti: AWS

Simple Storage Service (Amazon S3)

Puoi integrare Amazon S3 con Oracle Database@AWS nei seguenti modi:

- Backup automatici gestiti da Oracle su Amazon S3: Oracle AWS Database@ abilita automaticamente l'accesso alla rete per i backup automatici. Questa integrazione non può essere disabilitata. Se imposti Amazon S3 come destinazione di backup gestito nella console OCI, OCI carica i backup automatici in un bucket S3.
- Accesso diretto ad Amazon S3 dalla tua rete ODB: puoi abilitare l'accesso diretto alla rete ODB a S3 e quindi archiviare script, importare ed esportare file e file correlati in un bucket S3. Puoi disabilitare questo accesso. Questa impostazione è indipendente dall'accesso automatico alla rete per i backup automatici gestiti da Oracle.

Integrazione Zero-ETL con Amazon Redshift

Puoi abilitare l'integrazione zero-ETL della tua rete ODB con Amazon Redshift. Questa integrazione consente di replicare i dati su Amazon Redshift dai database Oracle in esecuzione in Oracle AWS Database@ senza il tradizionale processo di estrazione, trasformazione e caricamento (ETL). Questa integrazione consente analisi in tempo reale e carichi di lavoro AI sincronizzando automaticamente i dati Oracle con Amazon Redshift.

Oltre alle integrazioni gestite per AWS i servizi, puoi anche utilizzare VPC Lattice per accedere a servizi e risorse ospitati in VPCs altri o accedere alle istanze di rete ODB dal tuo VPC. Puoi gestire l'accesso e le risorse utilizzando la console VPC Lattice, la CLI e. APIs Per maggiori informazioni, consulta le seguenti risorse:

- Backup in Oracle Database@AWS
- Integrazione di Oracle Database@AWS Zero-ETL con Amazon Redshift
- Cos'è Amazon VPC Lattice? e VPC Lattice per Oracle Database@AWS

Instradamento del traffico proveniente da più VPCs

Per consentire VPCs a più Oracle Database@AWS risorse di accedere a una rete ODB, puoi utilizzare AWS Transit Gateway o AWS Cloud WAN.

AWS Transit Gateway

Un gateway di transito Amazon VPC è un hub di transito di rete utilizzato per interconnettere reti locali e VPCs interconnesse. Una rete ODB supporta solo il peering one-to-one diretto tra la rete ODB e un singolo VPC. È possibile peerizzare la rete ODB su un VPC e quindi collegare questo VPC a un gateway di transito. Il gateway può connettersi a più di uno. VPCs Con questa configurazione di gateway di transito, puoi instradare il traffico tra più sottoreti VPC verso una singola rete ODB.

Per ulteriori informazioni, consulta Configurazione dei gateway di transito Amazon VPC per Oracle Database@AWS.

AWS WAN cloud

AWS Cloud WAN è un servizio di rete WAN (Wide Area Networking) gestito che consente di creare, gestire e monitorare una rete globale unificata che collega le risorse negli ambienti cloud e locali. Utilizzando la dashboard centrale, puoi connettere filiali locali, data center e VPCs tutta la rete globale. AWS

Puoi peerizzare la tua rete ODB a un VPC e quindi collegare questo VPC alla rete principale Cloud WAN. Con questa configurazione, puoi utilizzare Cloud WAN per instradare il traffico tra reti multiple VPCs o locali e la tua rete ODB. Per ulteriori informazioni, consulta Configurazione di AWS Cloud WAN per Oracle Database@AWS.

Cluster VM Exadata

Un cluster Exadata VM è un insieme di Exadata strettamente accoppiati. VMs Ogni macchina virtuale dispone di un'installazione completa del database Oracle che include tutte le funzionalità di Oracle Enterprise Edition, tra cui Oracle Real Application Clusters (Oracle RAC) e Oracle Grid Infrastructure. È possibile creare uno o più database Oracle Exadata su un cluster di macchine virtuali. Per i diagrammi che mostrano l'architettura VMs e i cluster VM, consulta Exadata Database Service on Dedicated Infrastructure Technical Architecture.

Quando si crea un cluster VM, si specificano informazioni che includono quanto segue:

- Una rete ODB
- Un'infrastruttura Oracle Exadata
- I server di database su cui collocarli VMs nel cluster
- La quantità totale di storage Exadata utilizzabile

È possibile configurare i core della CPU, la memoria e lo storage locale per ogni macchina virtuale in un cluster di macchine virtuali. Per ulteriori informazioni, consulta Fase 3: Creare un cluster di macchine virtuali Exadata o un cluster di macchine virtuali autonome in Oracle Database@AWS.

Cluster VM autonomi

I cluster VM autonomi sono database completamente gestiti che automatizzano le attività di gestione chiave utilizzando l'apprendimento automatico e l'intelligenza artificiale. A differenza dei database tradizionali, i database autonomi forniscono, proteggono, aggiornano, eseguono il backup e ottimizzano automaticamente il database senza la necessità di intervento umano.

È possibile configurare il numero di core ECPU per VM, la memoria del database per CPU, lo storage del database e il numero massimo di database container autonomi. Per ulteriori informazioni, consulta Fase 3: Creare un cluster di macchine virtuali Exadata o un cluster di macchine virtuali autonome in Oracle Database@AWS.

Database Oracle Exadata

Oracle Exadata è un sistema ingegnerizzato che fornisce una piattaforma ad alte prestazioni per l'esecuzione di database Oracle. Con Oracle Database@AWS, si utilizza la AWS console per creare l'infrastruttura Oracle Exadata e i cluster VM che ospitano i database Exadata. Si utilizza quindi OCI per creare e gestire i database APIs Oracle. Per ulteriori informazioni, consulta Fase 4: Creare database Oracle Exadata nell'infrastruttura Oracle Cloud.

Onboarding su Oracle Database@AWS

Prima di iniziare a utilizzare Oracle Database@AWS, assicurati di aver effettuato la registrazione AWS e di aver creato gli utenti necessari. Quindi puoi acquistare Oracle Database@AWS da Marketplace AWS accettando un'offerta privata di Oracle.

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi Console di gestione AWScome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Accedere come utente root nella Guida per l'utente di Accedi ad AWS .

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita il Centro identità IAM.

   Per istruzioni, consulta Abilitazione del AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .

2. Nel Centro identità IAM, assegna l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere come utente del Centro identità IAM, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente del Centro identità IAM.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegnazione dell'accesso ad altri utenti

1. Nel Centro identità IAM, crea un set di autorizzazioni conforme alla best practice per l'applicazione di autorizzazioni con il privilegio minimo.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center .

Richiedi un'offerta privata per Oracle Database@AWS

La funzionalità di offerta privata per i Marketplace AWS venditori ti consente di richiedere e ricevere da Oracle Database@AWS i prezzi e i termini EULA di Oracle. Negozi prezzi e condizioni con Oracle, quindi Oracle crea un'offerta privata per la persona da te designata. Account AWS Accetti l'offerta privata e ricevi il prezzo e le condizioni d'uso negoziate. Al momento, puoi utilizzare la Oracle Database@AWS dashboard. Quando il contratto di offerta privata raggiunge la data di scadenza, si passa automaticamente alla pagina dei prezzi pubblici del prodotto oppure si annulla l'iscrizione a Oracle Database@.AWSPer ulteriori informazioni sulle offerte private, vedere Offerte private in. Marketplace AWS

Per richiedere e accettare un'offerta privata per Oracle Database@AWS

1. Accedi alla Console di gestione AWS.
2. Cerca e scegli Oracle Database@AWS.
3. Scegli Richiedi offerta privata.

> **Note**
>
> La Oracle Database@AWS dashboard è disponibile solo dopo aver accettato un'offerta privata.

4. Sul sito Oracle Cloud Infrastructure (OCI), specifica dettagli come la regione e le informazioni di contatto.
5. Attendi che un rappresentante OCI ti contatti e ti renda disponibile un'offerta privata.
6. Nel Console di gestione AWS, scegli Visualizza offerta privata.
7. Scegli l'offerta, quindi scegli Visualizza offerta.
8. Scegli Crea contratto e rispondi alle richieste successive per accettare l'offerta privata.
9. Dopo aver accettato l'offerta privata, dovrai attivare il tuo account OCI. Puoi accedere ai link di attivazione di Oracle direttamente da Console di gestione AWS.

    1. Nella console, vai alla sezione Guida introduttiva.
    2. Fai clic sul link di attivazione Oracle fornito nella console. In alternativa, puoi anche utilizzare il link di attivazione che ti è stato inviato via e-mail.
    3. Nella pagina di attivazione di Oracle, scegli se creare un nuovo account Oracle cloud o aggiungerlo a un account esistente.

4. Completa il processo di attivazione seguendo le istruzioni sullo schermo.
5. Dopo aver inviato la richiesta di attivazione, vedrai lo stato di Attivazione in corso nel pannello di controllo e la dashboard verrà temporaneamente disattivata con un motivo visualizzato. Console di gestione AWS
6. Una volta completata l'attivazione, la AWS dashboard di Oracle Database@ diventa disponibile, che consente di gestire le risorse.

10. Nella, scegli Console di gestione AWS Dashboard.

Abbonati a Oracle Database@ in più regioni AWS

Quando ti abboni Marketplace AWS e Oracle Database@AWS completi l'onboarding, sei collegato alla tua Account AWS locazione OCI. Questo collegamento, insieme alle risorse correlate, viene replicato automaticamente in tutte le AWS regioni in cui è disponibile. Oracle Database@AWS L'iscrizione e l'onboarding avvengono una sola volta anziché ripetere la procedura per ogni regione.

Per utilizzarlo Oracle Database@AWS in più regioni, procedi nel seguente modo:

1. Iscriviti Marketplace AWS e completa Oracle Database@AWS la procedura di onboarding.

   Quando ti abboni per la prima volta a Oracle Database@AWS, il tuo account viene attivato in una regione d'origine. È necessario specificare la regione di origine in Oracle Cloud Infrastructure (OCI).
2. Abilita le tue regioni preferite tramite la console OCI.

   Se non abiliti una regione in OCI e poi passi a questa regione nella Oracle Database@AWS console, ricevi un errore che indica che non sei abbonato. In questo caso, è necessario abilitare questa regione in OCI prima di poter utilizzare la Oracle Database@AWS dashboard in questa regione.
3. Accedi Oracle Database@AWS in qualsiasi AWS regione supportata senza ripetere la procedura di abbonamento.

Guida introduttiva a Oracle Database@AWS

Per iniziare a utilizzare Oracle Database@AWS, puoi creare le seguenti risorse utilizzando la Oracle Database@AWS console, la CLI o: APIs

1. Rete ODB
2. Infrastruttura Oracle Exadata
3. Cluster VM Exadata o cluster VM autonomo
4. Connessione peering ODB

Per creare database Oracle Exadata sulla tua infrastruttura, devi utilizzare la console Oracle Cloud Infrastructure (OCI) o APIs anziché la dashboard. Oracle Database@AWS Pertanto, le risorse vengono distribuite in due ambienti cloud: le risorse di rete e di infrastruttura sono presenti AWS, mentre il piano di controllo dell'amministrazione del database è in OCI. Per ulteriori informazioni, consulta Oracle Database@AWSla documentazione dell'infrastruttura Oracle Cloud.

Prerequisiti per la configurazione Oracle Database@AWS

Prima di configurare l'infrastruttura Oracle Exadata, assicurati di eseguire le seguenti operazioni:

- Segui le fasi in Onboarding su Oracle Database@AWS. È necessario aver accettato un'offerta privata per l'utilizzo. Oracle Database@AWS
- Concedi al tuo responsabile IAM le autorizzazioni relative alla policy elencate inConsenti agli utenti di fornire risorse Oracle Database@AWS. Queste autorizzazioni sono necessarie per l'uso. Oracle Database@AWS

Servizi OCI supportati su Oracle Database@AWS

Oracle Database@AWS supporta i seguenti servizi Oracle Cloud Infrastructure (OCI):

- Oracle Exadata Database Service on Dedicated Infrastructure: fornisce un ambiente Exadata dedicato e completamente gestito accessibile all'interno. AWS Per ulteriori informazioni, consulta Oracle Cloud Exadata Database Service on Dedicated Infrastructure nella documentazione OCI.
- Database autonomo su infrastruttura Exadata dedicata: fornisce un ambiente di database altamente automatizzato e completamente gestito in OCI con risorse hardware e software dedicate.

Per ulteriori informazioni, vedere Informazioni su Autonomous Database on Dedicated Exadata Infrastructure nella documentazione OCI.

Regioni supportate per Oracle Database@AWS

È possibile utilizzare Oracle Database@AWS quanto segue Regioni AWS:

Stati Uniti orientali (Virginia settentrionale)

Puoi usare il AZs con il comando fisico IDs `use1-az4` e `use1-az6`.

Stati Uniti occidentali (Oregon)

Puoi usarli AZs con il fisico IDs `usw2-az3` e `usw2-az4`.

Asia Pacifico (Tokyo)

Puoi usarli AZs con il fisico IDs `apne1-az1` e `apne1-az4`.

Stati Uniti orientali (Ohio)

Puoi usarli AZs con il fisico IDs `use2-az1` e `use2-az2`.

Europa (Francoforte)

Puoi usarli AZs con il fisico IDs `euc1-az1` e `euc1-az2`.

Canada (Centrale)

È possibile utilizzare l'AZ con l'ID fisico `cac1-az4`.

Asia Pacifico (Sydney)

È possibile utilizzare l'AZ con l'ID fisico `apse2-az4`.

Per trovare i nomi AZ logici nel tuo account che corrispondono alla precedente AZ fisica IDs, esegui il comando seguente.

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

Pianificazione dello spazio degli indirizzi IP in Oracle Database@AWS

Pianifica attentamente lo spazio degli indirizzi IP in Oracle Database@AWS. Considera il consumo di indirizzi IP in base al numero di cluster di macchine virtuali, incluso il numero di cluster VMs per cluster che puoi fornire alla rete ODB. Per ulteriori informazioni, consulta ODB Network Design nella documentazione sull'infrastruttura Oracle Cloud.

Argomenti

Restrizioni per gli indirizzi IP nella rete ODB

Tieni presente le seguenti restrizioni relative agli intervalli CIDR nella rete ODB:

- Non è possibile modificare l'intervallo CIDR del client o della sottorete di backup per la rete ODB dopo averla creata.
- Non è possibile utilizzare gli intervalli VPC CIDR nella colonna Associazioni con restrizioni nella tabella delle restrizioni delle associazioni di blocchi IPv4 CIDR.
- Per Exadata X9M, gli indirizzi IP 100.106.0.0/16 e 100.107.0.0/16 sono riservati all'interconnessione del cluster tramite l'automazione OCI, quindi non è possibile effettuare le seguenti operazioni:
  - Assegna questi intervalli all'intervallo CIDR client o di backup della rete ODB.
  - Utilizza questi intervalli per un CIDR VPC utilizzato per connettersi alla rete ODB.
- I seguenti intervalli CIDR sono riservati all'infrastruttura Oracle Cloud e non possono essere utilizzati per la rete ODB:
  - Intervallo riservato Oracle Cloud CIDR 169.254.0.0/16
  - Classe riservata D 224.0.0.0 — 239.255.255.255
  - Classe riservata E 240.0.0.0 — 255.255.255.255
- Non è possibile sovrapporre gli intervalli CIDR degli indirizzi IP per le sottoreti client e di backup.

- Non è possibile sovrapporre gli intervalli CIDR degli indirizzi IP allocati per le sottoreti client e di backup con gli intervalli CIDR VPC utilizzati per connettersi alla rete ODB.
- Non è possibile effettuare il provisioning in un cluster di macchine virtuali VMs in diverse reti ODB. La rete è una proprietà del cluster VM, il che significa che è possibile effettuare il provisioning solo di quelle VMs presenti nel cluster VM nella stessa rete ODB.

Requisiti CIDR della sottorete client per la rete ODB

Nella tabella seguente, è possibile trovare il numero di indirizzi IP utilizzati dal servizio e dall'infrastruttura per la sottorete del client CIDR. La dimensione CIDR minima per la sottorete client è /27 e la dimensione massima è /16.

Numero di indirizzi IP	Consumato da	Note
6	Oracle Database@AWS	Questi indirizzi IP sono riservati indipendentemente dal numero di cluster di VM predisposti nella rete ODB. Oracle Database@AWS consuma quanto segue: • 3 indirizzi IP riservati alle risorse di rete ODB in AWS • 3 indirizzi IP riservati al servizio di rete OCI
3	Ogni cluster di VM	Questi indirizzi IP sono riservati ai Single Client Access Names (SCANs) indipendentemente dal numero di nomi VMs presenti in ciascun cluster di macchine virtuali.
4	Ogni macchina virtuale	Questi indirizzi IP dipendono esclusivamente dal numero di utenti VMs presenti nell'infrastruttura.

Requisiti CIDR della sottorete di backup per la rete ODB

Nella tabella seguente, è possibile trovare il numero di indirizzi IP utilizzati dal servizio e dall'infrastruttura per la sottorete di backup CIDR. La dimensione CIDR minima per la sottorete di backup è /28 e la dimensione massima è /16.

Numero di indirizzi IP	Consumato da	Note
3	Oracle Database@AWS	Questi indirizzi IP sono riservati indipendentemente dal numero di cluster di VM predisposti nella rete ODB. Oracle Database@AWS consuma quanto segue: • 2 indirizzi IP all'inizio dell'intervallo CIDR • 1 indirizzo IP alla fine dell'intervallo CIDR
3	Ogni macchina virtuale	Questi indirizzi IP dipendono esclusivamente dal numero di utenti VMs presenti nell'infrastruttura.

Scenari di consumo IP per la rete ODB

Nella tabella seguente, è possibile visualizzare gli indirizzi IP utilizzati nella rete ODB per diverse configurazioni di cluster VM. Considerando che /28 è l'intervallo CIDR minimo tecnico per la sottorete client CIDR per distribuire 1 cluster di macchine virtuali con 2 VMs, si consiglia di utilizzare almeno un intervallo CIDR /27. In questo caso, l'intervallo IP non è completamente utilizzato dai cluster VM e consente l'allocazione di indirizzi IP aggiuntivi.

Configurazione	Client consumato IPs	Cliente IPs minimo	Backup IPs utilizzato	Backup IPs minimo
1 cluster VM con 2 VMs	17 (6 servizi+3 cluster + 4*2)	32 (intervallo CIDR /27)	9 (3 servizi + 3*2)	16 (intervallo CIDR /28)
1 cluster VM con 3 VMs	21 (6 servizi+3 cluster + 4*3)	32 (intervallo CIDR /27)	12 (3 servizi + 3*3)	16 (intervallo CIDR /28)
1 cluster VM con 4 VMs	25 (6 servizi+3 cluster + 4*4)	32 (intervallo CIDR /27)	15 (3 servizi + 3*4)	16 (intervallo CIDR /28)
1 cluster VM con 8 VMs	41 (6 servizi+3 cluster + 4*8)	64 (intervallo CIDR /26)	27 (3 servizi + 3*8)	32 (intervallo CIDR /27)

La tabella seguente mostra quante istanze di ciascuna configurazione sono possibili in base a uno specifico intervallo CIDR del client. Ad esempio, 1 cluster di macchine virtuali con 4 VMs utilizza 24 indirizzi IP nella sottorete client. Se l'intervallo CIDR è /25, sono disponibili 128 indirizzi IP. Pertanto, è possibile effettuare il provisioning di 5 cluster di macchine virtuali nella sottorete.

Configurazione del cluster VM	Numero con /27 (32) IPs	Numero con /26 (64) IPs	Numero con /25 (128) IPs	Numero con /24 (256) IPs	Numero quando /23 (512) IPs	Numero quando /22 (1024) IPs
1 cluster VM con 2 VMs (16) IPs	1	3	7	15	30	60
1 cluster VM con 3 VMs (20) IPs	1	3	6	12	24	48
1 cluster VM con 4 VMs (24) IPs	1	2	5	10	20	40
2 cluster VM da 2 VMs ciascuno (27) IPs	1	2	4	9	18	36
2 cluster di macchine virtuali da 3 VMs ciascuno (35) IPs	0	1	3	7	14	28
2 cluster di macchine virtuali da 4 VMs ciascuno (43) IPs	0	1	2	5	11	23

Fase 1: Creare una rete ODB in Oracle Database@AWS

Una rete ODB è una rete privata isolata che ospita l'infrastruttura OCI in una zona di disponibilità (AZ). Una rete ODB e un'infrastruttura Oracle Exadata sono i presupposti per il provisioning di cluster VM e la creazione di database Exadata. È possibile creare la rete ODB e l'infrastruttura Oracle Exadata in entrambi gli ordini. Per ulteriori informazioni, consultare Rete ODB e Peering ODB.

Questa attività presuppone che tu abbia letto. Pianificazione dello spazio degli indirizzi IP in Oracle Database@AWS Per modificare o eliminare la rete ODB in un secondo momento, vedere. Gestione di Oracle Database@AWS

Per creare una rete ODB

1. Accedi a Console di gestione AWS e apri la Oracle Database@AWS console all'indirizzo https://console.aws.amazon.com/odb/.
2. Scegli la tua AWS regione in alto a destra. Per ulteriori informazioni, consulta Regioni supportate per Oracle Database@AWS.
3. Dal riquadro di sinistra, scegli Reti ODB.
4. Scegli Crea rete ODB.
5. Per il nome della rete ODB, inserisci un nome di rete. Il nome deve contenere da 1 a 255 caratteri e iniziare con un carattere alfabetico o un carattere di sottolineatura. Non può contenere trattini consecutivi.
6. Per Zona di disponibilità, scegli un nome AZ. Per informazioni sull'assistenza AZs, consultaRegioni supportate per Oracle Database@AWS.
7. Per Client subnet CIDR, specifica un intervallo CIDR per le connessioni client. Per ulteriori informazioni, consulta Requisiti CIDR della sottorete client per la rete ODB.
8. Per Backup subnet CIDR, specificare un intervallo CIDR per le connessioni di backup. Per isolare il traffico di backup e migliorare la resilienza, si consiglia di non sovrapporre il CIDR di backup e il CIDR del client. Per ulteriori informazioni, consulta Requisiti CIDR della sottorete di backup per la rete ODB.
9. Per la configurazione DNS, scegli una delle seguenti opzioni:

   Predefinita

   Per Prefisso del nome di dominio, inserisci un nome da utilizzare come prefisso del tuo dominio. Il nome di dominio è fisso come oraclevcn.com. Ad esempio, se si immette**`myhost`**, il nome di dominio completo è myhost.oraclevcn.com.

   Nome di dominio personalizzato

   Per Nome di dominio, inserisci un nome di dominio completo. Ad esempio, puoi inserire myhost.myodb.com.
10. (Facoltativo) Per le integrazioni di servizi, seleziona un servizio da integrare con la tua rete utilizzando VPC Lattice. Oracle Database@AWS si integra con vari strumenti Servizi AWS per

fornire funzionalità e opzioni di connettività avanzate per i database Oracle. Seleziona una delle seguenti integrazioni:

Amazon S3

Abilita l'accesso diretto alla rete ODB ad Amazon S3. I tuoi database possono accedere a S3 per l'importazione/esportazione di dati o per backup personalizzati. Puoi inserire una policy JSON. Per ulteriori informazioni, consulta Backup gestiti dall'utente su Amazon S3 in Oracle Database@AWS.

Zero-ETL

Abilita l'analisi in tempo reale e l'apprendimento automatico sui dati transazionali utilizzando Amazon Redshift. Per ulteriori informazioni, consulta Integrazione di Oracle Database@AWS Zero-ETL con Amazon Redshift.

> **Note**
>
> Quando crei la tua rete ODB, Oracle Database@ preconfigura AWS automaticamente l'accesso alla rete per i backup gestiti da Oracle su Amazon S3. Non puoi abilitare o disabilitare questa integrazione. Per ulteriori informazioni, consulta AWS integrazioni di servizi.

11. (Facoltativo) Per i tag, inserisci fino a 50 tag per la rete. Un tag è una coppia chiave-valore che puoi utilizzare per organizzare e tenere traccia delle tue risorse.
12. Scegli Crea rete ODB.

Dopo aver creato una rete ODB, puoi peerizzarla su un VPC. Il peering ODB è una connessione di rete creata dall'utente che consente l'instradamento privato del traffico tra un Amazon VPC e una rete ODB. Dopo il peering, un' EC2 istanza Amazon all'interno del VPC può comunicare con le risorse della rete ODB come se si trovassero all'interno della stessa rete. Per ulteriori informazioni, consulta Configurazione del peering ODB su un Amazon VPC in Oracle Database@AWS.

Fase 2: Creare un'infrastruttura Oracle Exadata in Oracle Database@AWS

L'infrastruttura Oracle Exadata è l'architettura alla base dei server di database, dei server di storage e delle reti che eseguono i database Oracle Exadata. Scegli Exadata X9M o X11M come modello di sistema. È quindi possibile creare cluster VM sull'infrastruttura Exadata utilizzando la console. AWS

È possibile creare l'infrastruttura Oracle Exadata e la rete ODB in entrambi gli ordini. Non è necessario specificare le informazioni di rete quando si crea l'infrastruttura.

Non è possibile modificare un'infrastruttura Oracle Exadata dopo averla creata. Per eliminare un'infrastruttura Exadata, vedere. Eliminazione di un'infrastruttura Oracle Exadata in Oracle Database@AWS

Per creare un'infrastruttura Exadata

1. Accedi a Console di gestione AWS e apri la Oracle Database@AWS console all'indirizzo. https://console.aws.amazon.com/odb/
2. Dal riquadro di sinistra, scegli Infrastrutture Exadata.
3. Scegli Crea un'infrastruttura Exadata.
4. Per il nome dell'infrastruttura Exadata, inserisci un nome. Il nome deve contenere da 1 a 255 caratteri e iniziare con un carattere alfabetico o un carattere di sottolineatura. Non può contenere trattini consecutivi.
5. Per Zona di disponibilità, scegli una delle opzioni supportate. AZs Quindi scegli Successivo.
6. Per il modello di sistema Exadata, scegli Exadata.X9M o Exadata.X11M. Per Exadata.X11M, scegli anche i seguenti tipi di server:
   - Per il tipo di server di database, scegli il tipo di modello di server di database della tua infrastruttura Exadata. Attualmente, l'unica scelta è X11M.
   - Per il tipo di server di archiviazione, scegli il tipo di modello di server di archiviazione della tua infrastruttura Exadata. Attualmente, l'unica scelta è X11M-HC.
7. Per i server di database, lascia il valore predefinito di 2 o sposta il cursore per scegliere fino a 32 server. Per specificarne più di 2, richiedi un aumento del limite a OCI.

   Ogni server di database Exadata X9M supporta 126. OCPUs Ogni server di database Exadata X11M supporta 760. ECPUs Il conteggio totale delle risorse di calcolo cambia man mano che si

modifica il numero di server. Per ulteriori informazioni su OCPUs e ECPUs, consulta Compute Models in Autonomous Database nella documentazione Oracle.

8. Per i server di storage, lascia il valore predefinito di 3 o sposta il cursore per scegliere fino a 64 server. Per specificarne più di 3, richiedi un aumento del limite a OCI. Ogni server di storage X9M fornisce 64 TB. Ogni server di storage X11m fornisce 80 TB. Il totale di TB di storage cambia man mano che si modifica il numero di server. Quindi scegli Successivo.
9. Per la finestra Manutenzione, configura quando può avvenire la manutenzione del sistema:
   a. Per la preferenza Scheduling, selezionate una delle seguenti opzioni:
      - Pianificazione gestita da Oracle: Oracle determina il momento ottimale per le attività di manutenzione.
      - Pianificazione gestita dal cliente: si specifica quando possono essere eseguite le attività di manutenzione.
   b. Per la modalità Patching, selezionare una delle seguenti opzioni:
      - Rolling: gli aggiornamenti vengono applicati a un nodo alla volta, consentendo al database di rimanere disponibile durante l'applicazione delle patch.
      - Non in sequenza: gli aggiornamenti vengono applicati a tutti i nodi contemporaneamente, il che potrebbe richiedere tempi di inattività.
   c. Se hai selezionato Pianificazione gestita dal cliente, configura le seguenti impostazioni aggiuntive:
      - Per i mesi di manutenzione, seleziona i mesi in cui è possibile eseguire la manutenzione.
      - Per Settimana del mese, seleziona la settimana del mese in cui è possibile eseguire la manutenzione (prima, seconda, terza, quarta o ultima).
      - Per Giorno della settimana, seleziona il giorno in cui è possibile eseguire la manutenzione (dal lunedì alla domenica).
      - Per Ora di inizio, seleziona l'ora in cui inizia la finestra di manutenzione. L'ora è in UTC.
      - Per Tempi di consegna delle notifiche, seleziona con quanti giorni di anticipo desideri ricevere una notifica sulla manutenzione imminente.

> **Note**
>
> L'infrastruttura Oracle Cloud esegue la manutenzione del sistema durante questa finestra. Durante la manutenzione, l'infrastruttura Exadata rimane disponibile, ma potrebbero verificarsi brevi periodi di maggiore latenza.

10. (Facoltativo) Per i contatti di notifica di manutenzione OCI, inserisci fino a 10 indirizzi e-mail. AWS inoltra questi indirizzi e-mail a OCI. Quando si verificano aggiornamenti, OCI invia notifiche via e-mail agli indirizzi elencati.
11. (Facoltativo) Per i tag, inserisci fino a 50 tag per l'infrastruttura. Un tag è una coppia chiave-valore che puoi utilizzare per organizzare e tenere traccia delle tue risorse.
12. Scegli Avanti e rivedi le impostazioni dell'infrastruttura.
13. Scegli Create Exadata infrastructure.

Fase 3: Creare un cluster di macchine virtuali Exadata o un cluster di macchine virtuali autonome in Oracle Database@AWS

Un cluster Exadata VM è un set VMs su cui è possibile creare database Oracle Exadata. I cluster VM vengono creati sull'infrastruttura Exadata. È possibile implementare più cluster VM con diverse infrastrutture Oracle Exadata nella stessa rete ODB. Hai il pieno controllo amministrativo sui database che crei sui cluster VM Exadata.

Un cluster VM autonomo è un pool preallocato di risorse di calcolo e storage Oracle Exadata, virtualizzato a livello di macchina virtuale, che esegue Autonomous Databases (ADB). A differenza dei database gestiti dagli utenti creati su un cluster Exadata VM, un database Autonomous si ottimizza automaticamente, installa automaticamente le patch e viene gestito da Oracle anziché da un amministratore del database.

Considera le seguenti limitazioni quando crei cluster di macchine virtuali:

- Puoi implementare un cluster di macchine virtuali solo nella zona in cui hai creato la rete ODB e l'infrastruttura Oracle Exadata.
- Se non condividi un cluster VM tra più account, deve trovarsi nella stessa Account AWS infrastruttura Oracle Exadata. Se si utilizza AWS RAM per condividere una rete ODB e

un'infrastruttura Oracle Exadata da un AWS account con un account affidabile, l'account affidabile può creare cluster VM nel proprio account.

- È possibile distribuire solo cluster VM nella rete ODB. Non sono consentite altre risorse.
- Non è possibile modificare l'allocazione dello storage dopo aver creato un cluster di macchine virtuali.

> **Important**
>
> Il processo di creazione può richiedere più di 6 ore, a seconda delle dimensioni del cluster VM.

Exadata VM cluster

Per creare un cluster di macchine virtuali Exadata

1. Accedi a Console di gestione AWS e apri la console all' Oracle Database@AWS indirizzo. https://console.aws.amazon.com/odb/
2. Dal riquadro di sinistra, scegli Exadata VM clusters.
3. Scegli Crea cluster VM.
4. Per il nome del cluster VM, inserisci un nome. Il nome deve contenere da 1 a 255 caratteri e iniziare con un carattere alfabetico o un carattere di sottolineatura. Non può contenere trattini consecutivi.
5. (Facoltativo) Per il nome del cluster Grid Infrastructure, inserisci una versione dell'infrastruttura Grid per il tuo cluster VM che corrisponda alla versione del database Oracle che stai utilizzando. Il nome deve contenere da 1 a 11 caratteri e non può contenere trattini.
6. In Fuso orario, inserisci un fuso orario.
7. Per le opzioni di licenza, scegli Bring Your Own License (BYOL) o Licenza inclusa, quindi scegli Avanti. Questa licenza è la licenza OCI fornita da Oracle, non una licenza fornita da. AWS
8. Configura le impostazioni dell'infrastruttura Exadata come segue:

   a. Per Infrastruttura, scegli quanto segue:

      - Per il nome dell'infrastruttura Exadata, scegli l'infrastruttura da utilizzare per questo cluster di macchine virtuali.

- Per la versione Grid Infrastructure, scegli la versione da usare per questo cluster di macchine virtuali.
- Per la versione dell'immagine Exadata, scegli la versione da usare per questo cluster di macchine virtuali. Ti consigliamo di scegliere la versione mostrata, che è la versione più recente disponibile.

b. Per i server di database, seleziona uno o più server di database per ospitare il cluster di macchine virtuali.

c. Per la configurazione, procedi come segue:

- Scegli il numero di core della CPU, la memoria e lo storage locale per ogni macchina virtuale o accetta le impostazioni predefinite.
- Scegli la quantità totale di storage Exadata per il cluster VM o accetta l'impostazione predefinita.

d. (Facoltativo) Per l'allocazione dello storage, seleziona una delle seguenti opzioni:

- Abilita l'allocazione dello storage per le istantanee sparse di Exadata
- Abilita l'allocazione dello storage per i backup locali

L'allocazione dello storage utilizzabile cambia man mano che si selezionano le opzioni. Non è possibile modificare questa allocazione di archiviazione in un secondo momento. Controlla la selezione, quindi scegli Avanti.

9. Configura la connettività come segue:

a. Per la rete ODB, scegli una rete ODB esistente.

b. Per il prefisso del nome host, inserisci un prefisso per il cluster VM. Assicurati di non includere il nome di dominio. Il prefisso costituisce la prima parte del nome host del cluster Oracle Exadata VM.

> **Note**
>
> Il nome di dominio Host è fisso come oraclevcn.com.

c. Per la porta del listener SCAN (TCP/IP), immettere un numero di porta per l'accesso TCP al listener SCAN (Single Client Access Name). La porta predefinita è 1521. Oppure è possibile inserire una porta SCAN personalizzata nell'intervallo 1024-8999, esclusi

i seguenti numeri di porta: 2484, 6100, 6200, 7060, 7070, 7085 e 7879. Quindi scegli Successivo.

d. Per le coppie di chiavi SSH, inserisci la parte di chiave pubblica di una o più coppie di chiavi utilizzate per l'accesso SSH al cluster VM. Quindi scegli Successivo.

10. (Facoltativo) Scegliete la diagnostica e i tag come segue:

    a. Scegli se abilitare la raccolta diagnostica per gli eventi di diagnostica, Health monitor e i registri degli incidenti e le raccolte di tracce. Oracle può utilizzare queste informazioni diagnostiche per identificare, tracciare e risolvere i problemi.

    b. Per Tag, inserisci fino a 50 tag per il cluster VM. Un tag è una coppia chiave-valore che puoi utilizzare per organizzare e tenere traccia delle tue risorse. Quindi scegli Successivo.

11. Verificare le impostazioni. Quindi scegli Crea cluster VM.

Autonomous VM cluster

Per creare un cluster di VM autonomo

1. Accedi a Console di gestione AWS e apri la Oracle Database@AWS console all'indirizzo https://console.aws.amazon.com/odb/.
2. Dal riquadro di sinistra, scegli Cluster di macchine virtuali autonome.
3. Scegli Crea cluster VM autonomo.
4. Per il nome del cluster VM, inserisci un nome. Il nome deve contenere da 1 a 255 caratteri e iniziare con un carattere alfabetico o un carattere di sottolineatura. Non può contenere trattini consecutivi.
5. In Fuso orario, inserisci un fuso orario.
6. Per le opzioni di licenza, scegli Bring Your Own License (BYOL) o Licenza inclusa, quindi scegli Avanti. Questa licenza è la licenza OCI fornita da Oracle, non una licenza fornita da. AWS
7. Configura le impostazioni dell'infrastruttura Exadata come segue:

    a. Per il nome dell'infrastruttura Exadata, scegli l'infrastruttura da utilizzare per questo cluster di macchine virtuali autonome.

    b. Per i server di database, seleziona uno o più server di database per ospitare il tuo cluster di macchine virtuali autonome.

c. Per la configurazione, procedi come segue:

- Scegli il numero di core ECPU per macchina virtuale, la memoria del database per CPU, lo storage del database e il numero massimo di database contenitore autonomo o accetta le impostazioni predefinite.
- Scegli la quantità totale di storage Exadata per il cluster Autonomous VM o accetta l'impostazione predefinita.

8. Configura la connettività come segue:

a. Per la rete ODB, scegli una rete ODB esistente.

b. Per la porta del listener SCAN (TCP/IP), inserite un numero di porta per Porta (non TLS). La porta predefinita è 1521. Oppure puoi inserire una porta (TLS) nell'intervallo 1024—8999, esclusi i seguenti numeri di porta: 2484, 6100, 6200, 7060, 7070, 7085 e 7879. Quindi scegli Successivo.

Seleziona Abilita l'autenticazione TLS reciproca (mTLS) per consentire l'autenticazione TLS reciproca.

9. (Facoltativo) Scegliete diagnostica e tag come segue:

a. Scegli se pianificare la configurazione di modifica in base alla pianificazione gestita da Oracle o alla pianificazione gestita dal cliente. Se scegli la pianificazione gestita dal cliente, imposta i mesi di manutenzione, le settimane del mese, il giorno della settimana e l'ora di inizio (UTC).

b. Per Tag, inserisci fino a 50 tag per il cluster Autonomous VM. Un tag è una coppia chiave-valore che puoi utilizzare per organizzare e tenere traccia delle tue risorse. Quindi scegli Successivo.

10. Verificare le impostazioni. Quindi scegli Crea cluster VM autonomo.

Fase 4: Creare database Oracle Exadata nell'infrastruttura Oracle Cloud

In Oracle Database@AWS, puoi creare e gestire le seguenti risorse utilizzando la AWS console, la CLI o: APIs

- Reti ODB
- Infrastruttura Oracle Exadata

- Cluster VM Exadata e cluster VM autonomi
- Connessioni peering ODB

Per creare e gestire i database Oracle Exadata sull'infrastruttura che hai creato, devi utilizzare la console Oracle Cloud Infrastructure anziché la dashboard. Oracle Database@AWS È possibile creare un database Exadata gestito dall'utente su un cluster Exadata VM e un database autonomo su un cluster Autonomous Exadata VM. Per informazioni sulla creazione di database Oracle in OCI, consulta Exadata Database nella documentazione dell'infrastruttura Oracle Cloud.

Per creare database Oracle Exadata

1. Accedi a Console di gestione AWS e apri la Oracle Database@AWS console all'indirizzo. https://console.aws.amazon.com/odb/
2. Dal riquadro di sinistra, scegli Exadata VM clusters o Autonomous VM clusters.
3. Scegli un cluster VM per visualizzare la pagina dei dettagli.
4. Scegli Gestisci in OCI per essere reindirizzato alla console dell'infrastruttura Oracle Cloud.
5. Crea il tuo database Exadata o Autonomous Database gestito dall'utente in OCI.

Configurazione del peering ODB su un Amazon VPC in Oracle Database@AWS

Il peering ODB è una connessione di rete creata dall'utente che consente l'instradamento privato del traffico tra un Amazon VPC e una rete ODB. Esiste una one-to-one relazione tra un VPC e una rete ODB. Dopo aver creato una connessione peering utilizzando la console, la CLI o l'API, assicurati di aggiornare le tabelle di routing VPC e configurare la risoluzione DNS. Per una panoramica concettuale del peering ODB, consulta. Peering ODB

Creazione di una connessione peering ODB in Oracle Database@AWS

Con le connessioni peering ODB, puoi stabilire una connettività di rete privata tra la tua infrastruttura Oracle Exadata e le applicazioni in esecuzione su Amazon. VPCs Ogni connessione peering ODB è una risorsa separata che puoi creare, visualizzare ed eliminare indipendentemente dalla rete ODB.

Quando si crea una connessione peering ODB, è possibile specificare gli intervalli CIDR della rete peer. Questa tecnica limita l'accesso alla rete alle sottoreti richieste, riduce i potenziali bersagli di attacchi e consente una segmentazione della rete più granulare per i requisiti di conformità.

È possibile creare i seguenti tipi di connessioni peering ODB:

Peering ODB con lo stesso account

Puoi creare una connessione peering ODB tra una rete ODB e un Amazon VPC nello stesso account. AWS

Peering ODB tra account

È possibile creare una connessione peering ODB tra una rete ODB in un account e un Amazon VPC in un altro account, dopo aver condiviso la rete ODB utilizzando. AWS RAM Gli account proprietari di VPC possono gestire gli intervalli CIDR specificati nella connessione peering senza possedere anche la rete ODB.

Esiste una relazione 1:1 tra un VPC e una rete ODB. Non è possibile creare una connessione peering ODB tra un VPC e più reti ODB o tra una rete ODB e più reti. VPCs

Console

1. Accedi a Console di gestione AWS e apri la console all'indirizzo. Oracle Database@AWS https://console.aws.amazon.com/odb/
2. Nel riquadro di navigazione, scegli Connessioni peering ODB.
3. Scegli Crea connessione peering ODB.
4. (Facoltativo) Per il nome di peering ODB, inserisci un nome univoco per la connessione.
5. Per la rete ODB, scegli la rete ODB da peer.
6. Per la rete peer, scegli Amazon VPC per effettuare il peer con la tua rete ODB.
7. (Facoltativo) Per la rete peer CIDRs, specifica blocchi CIDR aggiuntivi dal VPC peer che possono accedere alla rete ODB. Se non lo specifichi CIDRs, è consentito l'accesso CIDRs a tutti i dati del VPC peer.
8. (Facoltativo) In Tag, aggiungi una coppia chiave/valore.
9. Scegli Crea connessione peering ODB.

Dopo aver creato una connessione peering ODB, configura le tabelle di routing Amazon VPC per instradare il traffico verso la rete ODB peerizzata. Per ulteriori informazioni, consulta Configurazione delle tabelle di routing VPC per il peering ODB. Tieni presente che Oracle Database@AWS configura automaticamente le tabelle di routing di rete ODB.

AWS CLI

Per creare una connessione peering ODB, utilizzare il comando. `create-odb-peering-connection`

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

Per limitare l'accesso alla rete ODB a intervalli CIDR specifici, utilizzate il parametro. `--peer-network-cidrs-to-be-added` Se non specifichi intervalli CIDR, tutti gli intervalli hanno accesso.

```
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"
```

Per elencare le connessioni peering ODB, usa il comando. `list-odb-peering-connections`

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

Per ottenere dettagli su una connessione peering ODB specifica, usa il comando. `get-odb-peering-connection`

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

Aggiornamento di una connessione peering ODB

È possibile aggiornare una connessione peering ODB esistente per aggiungere o rimuovere una rete peer. CIDRs Puoi controllare quali sottoreti del VPC peer hanno accesso alla tua rete ODB.

Console

1. Accedi a Console di gestione AWS e apri la console all'indirizzo. Oracle Database@AWS https://console.aws.amazon.com/odb/
2. Nel riquadro di navigazione, scegli Connessioni peering ODB.
3. Seleziona la connessione peering ODB che desideri aggiornare.
4. Scegli Azioni, quindi scegli Aggiorna connessione peering.
5. Nella CIDRs sezione Peer network, aggiungi o rimuovi i blocchi CIDR secondo necessità:
   - Per aggiungere CIDRs, scegli Aggiungi CIDR e inserisci il blocco CIDR.
   - Per rimuovere CIDRs, scegli la X accanto al blocco CIDR che desideri rimuovere.
6. Scegli Aggiorna connessione peering.

AWS CLI

Per aggiungere una rete peer CIDRs a una connessione peering ODB, specifica il parametro `--peer-network-cidrs-to-be-added` nel 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"
```

Per rimuovere una rete peer CIDRs da una connessione peering ODB, specificare il parametro nel comando. `--peer-network-cidrs-to-be-removed` `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"
```

Configurazione delle tabelle di routing VPC per il peering ODB

Una tabella di instradamento contiene un insieme di regole, denominato route, che consente di determinare la direzione del traffico di rete dalla sottorete o dal gateway. Il CIDR di destinazione in una tabella di routing è un intervallo di indirizzi IP a cui si desidera indirizzare il traffico. Se hai specificato un VPC per il peering ODB sulla tua rete ODB, aggiorna la tabella di routing VPC con l'intervallo IP di destinazione nella tua rete ODB. Per ulteriori informazioni sul peering ODB, consulta. Peering ODB

Per aggiornare una tabella di routing, utilizzare il AWS CLI `ec2 create-route` comando. Gli esempi seguenti aggiornano le tabelle di routing di Amazon VPC. Per ulteriori informazioni, consulta Configurazione delle tabelle di routing VPC per il peering 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
```

Le tabelle di routing di rete ODB vengono aggiornate automaticamente con il VPC. CIDRs Per consentire l'accesso alla rete ODB solo per una sottorete specifica CIDRs anziché per tutta CIDRs la rete VPC, puoi specificare la rete peer CIDRs quando crei una connessione peering ODB o aggiornare una connessione peering ODB esistente per aggiungere o rimuovere intervalli CIDR peer. Per ulteriori informazioni, consultare Creazione di una connessione peering ODB in Oracle Database@AWS e Aggiornamento di una connessione peering ODB.

Per ulteriori informazioni sulle tabelle di routing VPC, consulta Subnet route tables nella Amazon Virtual Private Cloud User Guide e ec2 create-route nel Command Reference.AWS CLI

Configurazione DNS per Oracle Database@AWS

Amazon Route 53 è un servizio Web DNS (Domain Name System) altamente disponibile e scalabile che puoi utilizzare per il routing DNS. Quando si crea una connessione peering ODB tra la rete ODB e un VPC, è necessario un meccanismo per risolvere le query DNS per le risorse di rete ODB dall'interno del VPC. Puoi utilizzare Amazon Route 53 per configurare le seguenti risorse:

- Un endpoint in uscita

  L'endpoint è necessario per inviare query DNS alla rete ODB.
- Una regola del resolver

  Questa regola specifica il nome di dominio delle query DNS che il Route 53 Resolver inoltra al DNS per la rete ODB.

Come funziona il DNS in Oracle Database@AWS

Oracle Database@AWS gestisce automaticamente la configurazione DNS (Domain Name System) per la rete ODB. Per il nome di dominio, è possibile specificare un prefisso personalizzato per il nome di dominio predefinito `oraclevcn.com` o un nome di dominio completamente personalizzato. Per ulteriori informazioni, consulta Fase 1: Creare una rete ODB in Oracle Database@AWS.

Quando effettua il Oracle Database@AWS provisioning di una rete ODB, crea le seguenti risorse:

- Una rete cloud virtuale (VCN) di Oracle Cloud Infrastructure (OCI) con gli stessi blocchi CIDR della rete ODB

  Questo VCN risiede nella locazione OCI collegata del cliente. Esiste una mappatura 1:1 tra una rete ODB e un OCI VCN. Ogni rete ODB è associata a un OCI VCN.
- Un resolver DNS privato all'interno di OCI VCN

  Questo resolver DNS gestisce le query DNS all'interno di OCI VCN. L'automazione OCI crea record per il cluster VM. Le scansioni utilizzano il nome di dominio `*.oraclevcn.com` completo (FQDN).
- Un endpoint di ascolto DNS all'interno di OCI VCN per il resolver DNS privato

  È possibile trovare l'endpoint di ascolto DNS nella pagina dei dettagli della rete ODB sulla console. Oracle Database@AWS

Configurazione di un endpoint in uscita in una rete ODB in Oracle Database@AWS

Un endpoint in uscita consente l'invio di query DNS dal tuo VPC a una rete o a un indirizzo IP. L'endpoint specifica gli indirizzi IP da cui provengono le query. Per inoltrare le query DNS dal tuo VPC alla tua rete ODB, crea un endpoint in uscita utilizzando la console Route 53. Per ulteriori informazioni, consulta Inoltro delle query DNS in uscita alla rete.

Per configurare un endpoint in uscita in una rete ODB

1. Accedi a Console di gestione AWS e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Dal riquadro di sinistra, scegli Endpoint in uscita.
3. Nella barra di navigazione, scegli la regione per il VPC in cui desideri creare l'endpoint in uscita.
4. Scegli Create outbound endpoint (Crea endpoint in uscita).
5. Completa la sezione Impostazioni generali per l'endpoint in uscita come segue:
   a. Scegli un gruppo di sicurezza che consenta la connettività TCP e UDP in uscita a quanto segue:
      - Indirizzi IP utilizzati dai resolver per le query DNS sulla rete ODB
      - Porte utilizzate dai resolver per le query DNS sulla rete ODB
   b. In Endpoint Type (Tipo di endpoint), selezionare IPv4.
   c. Per Protocolli per questo endpoint, scegli Do53.
6. In Indirizzi IP, fornisci le seguenti informazioni:
   - Specificate gli indirizzi IP o lasciate che il Route 53 Resolver scelga per voi gli indirizzi IP tra gli indirizzi disponibili nella sottorete. Scegli da un minimo di 2 a un massimo di 6 indirizzi IP per le query DNS. Ti consigliamo di scegliere gli indirizzi IP in almeno due zone di disponibilità diverse.
   - Per Subnet, scegli le sottoreti che hanno le seguenti caratteristiche:
     - Tabelle di routing che includono le rotte verso gli indirizzi IP del listener DNS sulla rete ODB
     - Liste di controllo dell'accesso alla rete (ACLs) che consentono il traffico UDP e TCP verso gli indirizzi IP e le porte utilizzate dai resolver per le query DNS sulla rete ODB
     - Rete ACLs che consente il traffico proveniente dai resolver sulla porta di destinazione nell'intervallo 1024-65535

7. (Facoltativo) Per i tag, specificare i tag per l'endpoint.
8. Seleziona Invia.

Configurazione di una regola del resolver in Oracle Database@AWS

Una regola del resolver è un insieme di criteri che determina come instradare le query DNS. Riutilizza o crea una regola che specifichi il nome di dominio delle query DNS che il resolver inoltra al DNS per la rete ODB.

Utilizzo di una regola resolver esistente

Per utilizzare una regola resolver esistente, l'azione da eseguire dipende dal tipo di regola:

Una regola per lo stesso dominio nella stessa AWS regione del VPC del tuo Account AWS

Associa la regola al tuo VPC invece di creare una nuova regola. Scegli la regola dalla dashboard delle regole e associala a quella applicabile VPCs nella AWS regione.

Una regola per lo stesso dominio nella stessa regione del tuo VPC ma in un account diverso

Usa AWS Resource Access Manager per condividere la regola dall'account remoto al tuo account. Quando condividi una regola, condividi anche l'endpoint in uscita corrispondente. Dopo aver condiviso la regola con il tuo account, scegli la regola dalla dashboard delle regole e associala VPCs a quella del tuo account. Per ulteriori informazioni, consulta Gestione delle regole di inoltro.

Creazione di una nuova regola del resolver

Se non riesci a riutilizzare una regola resolver esistente, crea una nuova regola utilizzando la console Amazon Route 53.

Per creare una nuova regola resolver

1. Accedi a Console di gestione AWS e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Dal riquadro a sinistra, scegli Regole.
3. Nella barra di navigazione, scegli la regione per il VPC in cui si trova l'endpoint in uscita.
4. Scegli Crea regola.

5. Completa la sezione Regola per il traffico in uscita come segue:

   a. Per Tipo di regola, scegli Inoltra regola.

   b. Per Nome di dominio, specifica il nome di dominio completo dalla rete ODB.

   c. A tal VPCs fine, utilizza questa regola, associala al VPC da cui le query DNS vengono inoltrate alla rete ODB.

   d. Per Endpoint in uscita, scegli l'endpoint in uscita in cui hai creato. Configurazione di un endpoint in uscita in una rete ODB in Oracle Database@AWS

   > **Note**
   >
   > Il VPC associato a questa regola non deve necessariamente essere lo stesso VPC in cui è stato creato l'endpoint in uscita.

6. Completa la sezione Indirizzi IP di destinazione come segue:

   a. Per l'indirizzo IP, specificate l'indirizzo IP dell'IP del listener DNS sulla rete ODB.

   b. Per Porta, specificare 53. Questa è la porta utilizzata dal resolver per le query DNS.

   > **Note**
   >
   > Il Route 53 Resolver inoltra le query DNS che corrispondono a questa regola e provengono da un VPC associato a questa regola all'endpoint in uscita di riferimento. Queste query vengono inoltrate agli indirizzi IP di destinazione specificati negli indirizzi IP di destinazione.

   c. Per Protocollo di trasmissione, scegli Do53.

7. (Facoltativo) Per i tag, specificate i tag per la regola.

8. Seleziona Invia.

Verifica della configurazione DNS in Oracle Database@AWS

Dopo aver creato la regola dell'endpoint e del resolver in uscita, verifica che il DNS si risolva correttamente. Utilizzando un' EC2 istanza Amazon nel VPC dell'applicazione, esegui una risoluzione DNS come segue:

Per Linux o macOS

Usa un comando del modulo`dig` *`record-name record-type`*.

Per Windows

Usa un comando del modulo`nslookup -type=`*`record-name record-type`*.

Configurazione dei gateway di transito Amazon VPC per Oracle Database@AWS

Amazon VPC Transit Gateways è un hub di transito di rete che interconnette cloud privati virtuali (VPCs) e reti locali. Ogni VPC dell' hub-and-spokearchitettura può connettersi al gateway di transito per accedere ad altri VPC connessi. VPCs AWS Transit Gateway supporta il traffico per entrambi IPv4 e IPv6.

Nel Oracle Database@AWS, una rete ODB supporta una connessione peering a un solo VPC. Se connetti un gateway di transito a un VPC collegato a una rete ODB, puoi connetterne più VPCs di uno a questo gateway. Le applicazioni in esecuzione su questi diversi sistemi VPCs possono accedere a un cluster di macchine virtuali Exadata in esecuzione nella rete ODB.

Il diagramma seguente mostra un gateway di transito connesso a due VPCs e una rete locale.

Nel diagramma precedente, un VPC viene collegato a una rete ODB. In questa configurazione, la rete ODB può indirizzare il traffico verso tutti gli VPCs utenti collegati al gateway di transito. La tabella delle rotte per ogni VPC include sia la route locale che le route che inviano il traffico destinato alla rete ODB al gateway di transito.

In AWS Transit Gateway, ti viene addebitato il numero di connessioni orarie che effettui verso il gateway di transito e la quantità di traffico che attraversa. AWS Transit Gateway Per informazioni sui costi, consulta la pagina AWS Transit Gateway dei prezzi.

Requisiti

Assicurati che il tuo Oracle Database@AWS ambiente soddisfi i seguenti requisiti:

- Il VPC collegato tramite peering alla rete ODB deve trovarsi nello stesso. Account AWS Se il VPC peered si trova in un account diverso dalla rete ODB, gli allegati del gateway di transito falliscono indipendentemente dalle configurazioni di condivisione.

- Il VPC collegato alla rete ODB deve disporre di un gateway di transito collegato.

> **Note**
>
> Se il gateway di transito è configurato per la condivisione, può risiedere in qualsiasi account. Pertanto, non è necessario che il gateway stesso si trovi nello stesso account della rete VPC e ODB.

- L'allegato del gateway di transito deve trovarsi nella stessa zona di disponibilità (AZ) della rete ODB.

Limitazioni

Tieni presente le seguenti limitazioni di Amazon VPC Transit Gateway per: Oracle Database@AWS

- Amazon VPC Transit Gateways non offre l'integrazione nativa per utilizzare una rete ODB come allegato. Pertanto, le funzionalità VPC come le seguenti non sono disponibili:
  - Risoluzione di nomi host DNS pubblici in indirizzi IP privati
  - Notifica degli eventi per le modifiche alla topologia della rete ODB, al routing e allo stato della connessione
- Il traffico multicast verso la rete ODB non è supportato.

Impostazione e configurazione di un gateway di transito

Puoi creare e configurare un gateway di transito utilizzando la console o `aws ec2` i comandi Amazon VPC. La procedura seguente presuppone che tu non abbia una rete ODB collegata a un VPC nel tuo. Account AWS Se nel tuo account sono già presenti una rete ODB e un VPC, salta i passaggi 1—3.

> **Note**
>
> Se colleghi o ricolleghi gli allegati sul tuo VPC, assicurati di reinserire gli intervalli CIDR nella rete ODB ODB.

Per impostare e configurare un gateway di transito per Oracle Database@AWS

1. Creare una rete ODB. Per ulteriori informazioni, consulta Fase 1: Creare una rete ODB in Oracle Database@AWS.
2. Crea un VPC, utilizzando lo stesso account che contiene la rete ODB. Per ulteriori informazioni, consulta Create a VPC nella Amazon VPC User Guide.
3. Crea una connessione peering ODB tra la tua rete ODB e il tuo VPC. Per ulteriori informazioni, consulta Configurazione del peering ODB su un Amazon VPC in Oracle Database@AWS.
4. Configura un gateway di transito seguendo la procedura descritta in Introduzione all'uso di Amazon VPC Transit Gateways. Il gateway deve appartenere alla rete ODB e al VPC o essere condiviso da un altro account. Account AWS

   > **Important**
   >
   > Crea l'allegato del gateway di transito nella stessa AZ della rete ODB.

5. Aggiungi gli intervalli CIDR alla tua rete ODB per le reti locali VPCs e le reti locali che intendi collegare alla tua rete principale. Per ulteriori informazioni, consulta Aggiornamento di una rete ODB in Oracle Database@AWS.

   Se utilizzi la CLI, esegui il comando `update-odb-network` con `--peered-cidrs-to-be-added` and. `--peered-cidrs-to-be-removed` Per ulteriori informazioni, consulta la sezione relativa alle informazioni di riferimento ai comandi di AWS CLI.

Configurazione di AWS Cloud WAN per Oracle Database@AWS

AWS Cloud WAN è un servizio di rete WAN (Wide Area Networking) gestito. Puoi utilizzare AWS Cloud WAN per creare, gestire e monitorare una rete globale unificata che collega le risorse in esecuzione negli ambienti cloud e locali.

In AWS Cloud WAN, una rete globale è un'unica rete privata che funge da contenitore di alto livello per gli oggetti di rete. Una rete centrale è la parte della rete globale gestita da AWS.

AWS Il cloud WAN offre i seguenti vantaggi chiave:

- Gestione centralizzata della rete che semplifica le operazioni mantenendo la sicurezza in più regioni
- Reti principali con segmentazione integrata per isolare il traffico attraverso più domini di routing

- Support per policy per automatizzare la gestione della rete e definire configurazioni coerenti in tutta la rete globale

In Oracle Database@AWS, una rete ODB supporta il peering su un solo VPC. Se connetti una rete centrale AWS Cloud WAN a un VPC peered, abilita il routing globale del traffico. Le applicazioni collegate in più VPCs regioni possono accedere ai cluster VM Exadata nella rete ODB. È possibile isolare il traffico di rete ODB nel proprio segmento o abilitare l'accesso ad altri segmenti.

Il diagramma seguente mostra una rete centrale AWS Cloud WAN connessa a tre VPCs e una rete locale.

AWS Cloud WAN non offre l'integrazione nativa per utilizzare una rete ODB come allegato. Pertanto, le funzionalità VPC come le seguenti non sono disponibili:

- Risoluzione di nomi host DNS pubblici in indirizzi IP privati
- Notifica degli eventi per le modifiche alla topologia della rete ODB, al routing e allo stato della connessione

In AWS Cloud WAN, ti viene addebitato ogni ora quanto segue:

- Numero di regioni (periferie della rete principale)
- Numero di allegati alla rete principale
- La quantità di traffico che fluisce attraverso la rete principale attraverso gli allegati

Per informazioni dettagliate sui prezzi, consulta i prezzi di AWS Cloud WAN.

Per configurare una rete principale per Oracle Database@AWS

1. Aggiungi intervalli CIDR alla tua rete ODB per le reti locali VPCs e per le reti locali che intendi collegare alla tua rete principale. Per ulteriori informazioni, consulta Aggiornamento di una rete ODB in Oracle Database@AWS.

   > **Note**
   >
   > Se colleghi o ricolleghi gli allegati sul tuo VPC, assicurati di reinserire gli intervalli CIDR nella rete ODB ODB.

2. Segui i passaggi descritti in Creare una rete globale e una rete principale AWS Cloud WAN.

Condivisione dei diritti in Oracle Database@AWS

Con Oracle Database@AWS, puoi condividere le autorizzazioni AWS Marketplace per Oracle AWS Database@ all'interno della stessa organizzazione. Account AWS AWS Ciò consente ad altri account di fornire la propria infrastruttura Oracle Exadata e le risorse di rete ODB utilizzando l'abbonamento dell'utente.

Metodi di condivisione

Oracle Database@AWS supporta due metodi di condivisione:

Condivisione dei diritti con License Manager AWS

- Concedi ad altri account la possibilità di fornire la propria infrastruttura Oracle Exadata e le risorse di rete ODB
- Ogni account opera in modo indipendente con il controllo completo del ciclo di vita delle risorse
- Ideale per abilitare il provisioning self-service tra team o unità aziendali

Condivisione delle risorse con AWS Resource Access Manager ()AWS RAM

- Condividi l'infrastruttura Oracle Exadata e le risorse di rete ODB già predisposte
- Centralizza la gestione dell'infrastruttura consentendo al contempo agli account dei destinatari di creare cluster di macchine virtuali
- Ottimizza i costi facendo in modo che più account utilizzino la stessa infrastruttura

Puoi utilizzare entrambi i metodi di condivisione contemporaneamente in base alle tue esigenze organizzative.

Limitazioni per la condivisione dei diritti d'uso di Oracle Database@AWS

Quando condividi le AWS autorizzazioni Oracle Database@, tieni presenti le seguenti limitazioni:

- Puoi condividere solo con l'interno della tua organizzazione Account AWS AWS

- Non è possibile condividere con un'intera unità organizzativa (OU) o con l'intera organizzazione
- Un account può ricevere diritti da un solo account acquirente (da un'offerta privata)
- Un account acquirente non può condividere i diritti con un altro account acquirente
- Gli account dei destinatari devono inizializzare il AWS servizio Oracle Database@ prima di poter utilizzare l'autorizzazione condivisa
- Le operazioni di concessione delle autorizzazioni possono essere eseguite solo dalla regione Stati Uniti orientali (Virginia settentrionale)

Condivisione delle autorizzazioni Oracle Database@AWS tra account

Per favorire la collaborazione ottimizzando al contempo i costi, condividi le AWS autorizzazioni di Oracle Database@ con altri membri della stessa organizzazione. Account AWS AWS Questo argomento spiega come condividere le autorizzazioni utilizzando AWS License Manager.

Prerequisiti per la condivisione dei diritti

Prima di condividere i permessi Oracle Database@,AWS assicurati di disporre dei seguenti requisiti:

- Un AWS abbonamento attivo a Oracle Database@ (devi essere l'account acquirente che ha accettato l'offerta privata tramite) Marketplace AWS
- Gli AWS account IDs dell'organizzazione con cui desideri condividere i diritti
- Autorizzazioni necessarie per consentire al concedente e al beneficiario di utilizzare le risorse e le operazioni di AWS License Manager (per ulteriori informazioni, vedere Gestione delle identità e degli accessi per License Manager nella Guida per l'utente di License Manager AWS)
- Autorizzazioni elencate di seguito per l'utente (concedente) e per il beneficiario del diritto (beneficiario)

Autorizzazioni necessarie per la condivisione dei diritti

Oltre alle autorizzazioni di AWS License Manager, Oracle Database@AWS richiede le seguenti autorizzazioni:

Autorizzazioni Concedente o

- `odb:CreateGrantShare`

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

Autorizzazioni concesse

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

Condivisione dei AWS diritti Oracle Database@ con un altro account utilizzando License Manager AWS

Per condividere i diritti con un altro AWS account, è necessario creare una sovvenzione utilizzando AWS License Manager. Per ulteriori informazioni, consulta Distribute License Manager entitlements nella AWS License Manager User Guide.

Dopo aver creato la concessione, il destinatario (beneficiario) deve:

- Accettare e attivare la sovvenzione. Per ulteriori informazioni, vedere Accettazione e attivazione della concessione in License Manager nella Guida per l'utente di AWS License Manager.
- Segui le istruzioni di inizializzazione per Oracle AWS Database@.

Una volta completata l'inizializzazione, il beneficiario può effettuare il provisioning delle risorse Oracle Database@ utilizzando l'autorizzazione condivisa.AWS

Condivisione delle risorse in Oracle Database@AWS

Con Oracle Database@AWS, puoi condividere l'infrastruttura Exadata e la tua rete ODB tra più utenti della stessa organizzazione. Account AWS AWS Ciò consente di effettuare il provisioning dell'infrastruttura una sola volta e di riutilizzarla tra account affidabili, riducendo i costi e separando le responsabilità.

Quando condividi risorse:

- L'account proprietario della risorsa (account proprietario) mantiene il controllo sul ciclo di vita della risorsa.
- Gli account che ricevono l'accesso a risorse condivise (account affidabili) possono visualizzare e utilizzare tali risorse in base alle autorizzazioni concesse.
- Gli account affidabili possono creare le proprie risorse sull'infrastruttura condivisa ma non possono eliminare le risorse condivise sottostanti.

Integrazione di Oracle Database@ con AWSAWS RAM

Oracle Database@AWS utilizza AWS Resource Access Manager (AWS RAM) per consentire la condivisione sicura e controllata delle risorse tra gli account. Con AWS RAM, puoi condividere in modo sicuro le tue AWS risorse Oracle Database@ tra più account all'interno della stessa organizzazione. AWS AWS AWS RAM semplifica la condivisione delle risorse, riduce il sovraccarico operativo e fornisce sicurezza e visibilità nelle risorse Oracle Database@ condivise.AWS

Con AWS RAM, condividi le risorse di tua proprietà creando una condivisione di risorse. Una condivisione di risorse specifica le risorse da condividere e Account AWS con chi condividerle.

Vantaggi della condivisione delle risorse in Oracle Database@AWS

La condivisione delle AWS risorse Oracle Database@ tra account offre i seguenti vantaggi:

- Ottimizzazione dei costi: esegui il provisioning della costosa infrastruttura Exadata una sola volta tramite un account amministrativo e condividila con più account, riducendo i costi complessivi.
- Separazione delle responsabilità: mantieni confini chiari tra gli amministratori dell'infrastruttura e gli utenti del database, favorendo al contempo la collaborazione.

- Gestione semplificata: centralizza il provisioning e la gestione dell'infrastruttura, abilitando al contempo le operazioni di database distribuite.
- Governance coerente: applica politiche e controlli coerenti tra le risorse condivise.

Ad esempio, un amministratore può fornire l'infrastruttura Oracle Exadata e la rete ODB al proprio interno Account AWS e condividerle con gli account degli sviluppatori. Gli sviluppatori possono quindi creare cluster di macchine virtuali su questa infrastruttura condivisa senza dover fornire il proprio costoso hardware. Questo approccio riduce in modo significativo i costi mantenendo al contempo un'adeguata separazione delle responsabilità tra gli account.

Come funziona la condivisione delle risorse in Oracle Database@AWS

È possibile condividere le seguenti risorse Oracle Database@:AWS

- Infrastruttura Oracle Exadata
- Rete ODB

Oracle Database@AWS condivide le risorse precedenti tramite il seguente processo:

1. L'account acquirente (l'account che accetta l'offerta AWS privata Oracle Database@ tramite AWS Marketplace) fornisce AWS risorse Oracle Database@, come l'infrastruttura Exadata e una rete ODB.
2. L'account acquirente crea una condivisione di risorse utilizzando AWS RAM, specificando le risorse da condividere e gli account affidabili con cui condividerle.
3. Le condivisioni di risorse per gli account fidati all'interno della stessa organizzazione vengono accettate automaticamente.
4. Prima di utilizzare risorse condivise, gli account affidabili devono inizializzare il AWS servizio Oracle Database@ nel proprio account utilizzando il `aws odb initialize-service` comando o selezionando Attiva account nella console Oracle Database@.AWS
5. Dopo l'inizializzazione, gli account affidabili possono creare le proprie risorse sull'infrastruttura condivisa, ad esempio i cluster di macchine virtuali sull'infrastruttura Exadata condivisa e sulla rete ODB.

Autorizzazioni su risorse condivise per account affidabili

Quando si condividono risorse, Oracle Database@ seleziona AWS automaticamente azioni specifiche (autorizzazioni gestite) per ogni tipo di risorsa:

Per l'infrastruttura Exadata

Oracle Database@AWS concede le seguenti autorizzazioni agli account affidabili:

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

Per la rete ODB

Le seguenti autorizzazioni sono concesse agli account attendibili:

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

La condivisione delle risorse rispetta la natura gerarchica delle risorse Oracle Database@.AWS Ad esempio, se condividi l'infrastruttura Exadata, gli account affidabili possono creare cluster di VM su questa infrastruttura, ma non possono modificare o eliminare l'infrastruttura Exadata stessa.

Quando una risorsa non è condivisa, gli account affidabili perdono la capacità di creare nuove risorse sull'infrastruttura condivisa. Tuttavia, tutte le risorse che hanno già creato rimangono accessibili e funzionali.

Limitazioni per la condivisione delle risorse Oracle Database@AWS

Prima di condividere le risorse, tieni presenti le seguenti limitazioni.

Limitazioni per la condivisione delle risorse

Quando condividi le AWS risorse Oracle Database@, tieni presente le seguenti limitazioni:

- È possibile condividere risorse solo con. Account AWS IDs
- È possibile condividere risorse solo all' Account AWS interno della stessa AWS organizzazione.
- Le risorse vengono condivise all'interno di una AWS regione specifica. Per condividere risorse tra regioni, è necessario creare condivisioni di risorse separate in ciascuna regione.
- Quando crei una condivisione di risorse, le azioni (autorizzazioni gestite) per ogni tipo di risorsa vengono selezionate automaticamente e non possono essere modificate.
- Non è possibile utilizzare Oracle Database@AWS come risorsa e condividerla con altri. Account AWS
- Un account affidabile può utilizzare risorse condivise provenienti da un solo account acquirente (da un'offerta privata). Pertanto, due account acquirente non possono condividere risorse con lo stesso account affidabile.
- Un account acquirente non può condividere risorse con un altro account acquirente.
- Le risorse condivise con un account affidabile devono essere condivise prima dall'account acquirente nella regione di residenza dell'acquirente.
- Quando annulli la condivisione di una risorsa, ti consigliamo di attendere circa 15 minuti prima di ricondividere la stessa risorsa con lo stesso account affidabile.

Limitazioni per la creazione e l'utilizzo di risorse condivise

Durante la creazione o l'utilizzo di AWS risorse Oracle Database@, tieni presente le seguenti limitazioni:

- Solo l'account acquirente può creare l'infrastruttura Exadata e le risorse di rete ODB. L'account acquirente è quello che accetta l'offerta privata di Oracle AWS Database@.
- Gli account affidabili possono creare risorse solo sull'infrastruttura Exadata condivisa dall'account acquirente.

- Gli account affidabili devono inizializzare il AWS servizio Oracle Database@ nel proprio account prima di poter utilizzare risorse condivise.

Limitazioni per l'eliminazione di risorse condivise

- Non è possibile eliminare l'infrastruttura Exadata con cluster di macchine virtuali creati da account attendibili finché tali cluster di macchine virtuali non vengono rimossi.
- Non è possibile eliminare una rete ODB con una connessione peering ODB creata da un account fidato finché la connessione peering ODB non è stata rimossa.
- L'account acquirente non può eliminare le risorse Oracle AWS Database@ create da account affidabili.
- Gli account affidabili possono visualizzare le risorse condivise ma non possono modificare o eliminare le AWS risorse Oracle Database@ di proprietà dell'account acquirente.

Condivisione di Oracle Database@AWS risorse tra account

Per favorire la collaborazione ottimizzando al contempo i costi, condividi le AWS risorse di Oracle Database@ con altre persone Account AWS all'interno della stessa organizzazione. AWS Questo argomento spiega come condividere le risorse utilizzando (). AWS Resource Access Manager AWS RAM

Argomenti

Prerequisiti per la condivisione delle risorse

Prima di condividere le AWS risorse di Oracle Database@, assicurati di disporre di quanto segue:

- Un AWS abbonamento attivo a Oracle Database@ (devi essere l'account acquirente che ha accettato l'offerta privata tramite) Marketplace AWS
- I nomi IDs o le risorse che desideri condividere, come l'infrastruttura Exadata o le reti ODB

- Gli AWS account IDs dell'organizzazione con cui desideri condividere le risorse
- Autorizzazioni necessarie per creare condivisioni di risorse in AWS RAM
- La possibilità di condividere risorse AWS Organizations tramite l'utilizzo AWS RAM (per ulteriori informazioni, consulta Abilitare la condivisione delle risorse AWS Organizations all'interno della Guida per l'AWS Resource Access Manager utente)

Condivisione delle AWS risorse Oracle Database@ con un altro account utilizzando AWS RAM

Per condividere un'infrastruttura Exadata o una rete ODB con un altro AWS account, si crea una condivisione di risorse utilizzando. AWS RAM Ciò consente all'account affidabile di creare cluster VM sulla tua infrastruttura Exadata.

Console

1. Apri la console all'indirizzo. AWS RAM https://console.aws.amazon.com/ram/
2. Seleziona Crea condivisione risorse.
3. In Nome, inserisci un nome descrittivo per la condivisione delle risorse.
4. In Seleziona il tipo di risorsa, una delle seguenti risorse:
   - Oracle Database@ rete ODB AWS
   - Infrastruttura Oracle Database@ Exadata AWS
5. Seleziona le risorse dell'infrastruttura Exadata che desideri condividere. Scegli Avanti fino a quando non arrivi a Garantire l'accesso ai principali.
6. In Principali, scegli Account AWS, quindi inserisci l' AWS account con IDs cui desideri condividere.
7. In Autorizzazioni gestite, seleziona le seguenti autorizzazioni per consentire all'account fidato di creare cluster VM sull'infrastruttura Exadata condivisa:
   - AWSRAMDefaultAutorizzazioneODBNetwork
   - AWSRAMDefaultAutorizzazioneODBCloudExadataInfrastructure
8. Seleziona Crea condivisione risorse.

AWS CLI

Per condividere risorse utilizzando il, usa il comando. AWS CLI`aws ram create-resource-share` L'esempio seguente crea una condivisione di risorse denominata `ExadataInfraShare` che condivide l'infrastruttura Exadata specificata con l'account 222222222222, consentendo a questo account di creare cluster di macchine virtuali sull'infrastruttura condivisa.

```
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
```

Visualizzazione delle condivisioni di risorse

Per visualizzare le risorse che hai condiviso e gli account con cui le hai condivise:

Console

1. Apri la AWS RAM console all'indirizzo https://console.aws.amazon.com/ram/.
2. Scegli Risorse condivise per visualizzare le risorse che hai condiviso con altri account.
3. Seleziona una condivisione di risorse per visualizzarne i dettagli, incluse le risorse condivise e i principali con cui sono condivise.

AWS CLI

Per visualizzare le tue condivisioni di risorse utilizzando AWS CLI, usa il `get-resource-shares` comando:

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

Per visualizzare le risorse in una condivisione di risorse specifica, usa il `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
```

Per visualizzare i principali (account) con cui è condivisa una condivisione di risorse, usa il `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
```

Aggiornamento o eliminazione delle condivisioni di risorse utilizzando AWS RAM

Per interrompere la condivisione di una risorsa con un account fidato utilizzando AWS RAM, intraprendi una delle seguenti azioni:

- Rimuovi la risorsa dalla condivisione delle risorse.
- Rimuovi l'account fidato dalla condivisione delle risorse.
- Eliminare la condivisione di risorse.

Prima di revocare l'accesso o eliminare una risorsa condivisa, considera le seguenti implicazioni:

- Gli account affidabili non possono più creare nuove risorse sull'infrastruttura non condivisa.
- Le risorse esistenti create da account fidati sull'infrastruttura condivisa Exadata continuano a funzionare e rimangono accessibili a tali utenti. Account AWS
- Non è possibile eliminare l'infrastruttura Exadata con cluster VM creati da account fidati finché tali cluster di VM non vengono rimossi.

Prima di annullare la condivisione delle risorse, ti consigliamo di coordinarti con gli account affidabili per garantire una transizione senza intoppi.

Per ulteriori informazioni, consulta Aggiornare una condivisione di risorse AWS RAM e Eliminare una condivisione di risorse AWS RAM nella Guida per l'AWS Resource Access Manager utente.

Inizializzazione Oracle Database@AWS in un account affidabile

Un account affidabile è un account Account AWS che dichiari idoneo a ricevere condivisioni di risorse. Deve essere un'altra persona Account AWS dell' AWS organizzazione. Prima di poter utilizzare le AWS risorse Oracle Database@ condivise in un account affidabile, è necessario inizializzare il servizio. L'inizializzazione crea i metadati necessari e stabilisce la connessione tra l'infrastruttura Oracle Cloud dell'utente e Oracle Cloud. Account AWS

Argomenti

Cos'è l'inizializzazione di Oracle Database@?AWS

Dopo che una risorsa è stata condivisa con l'account, è necessario inizializzare il AWS servizio Oracle Database@ prima di poter accedere o utilizzare la risorsa condivisa. Se si tenta di utilizzare Oracle Database@AWS APIs senza prima inizializzare il servizio, viene visualizzato un errore.

L'inizializzazione è un processo che si effettua una sola volta. Crea i metadati necessari e stabilisce una connessione tra la tua infrastruttura Account AWS e Oracle Cloud.

È possibile inizializzare il servizio utilizzando la console di AWS gestione o il. AWS CLI

Console

1. Aprire la console Oracle Database@AWS all'indirizzo. https://console.aws.amazon.com/odb/
2. Se è la prima volta che accedi alla AWS console Oracle Database@ con questo account, viene visualizzata una pagina di benvenuto.
3. Scegli Attiva account.
4. Inizia il processo di inizializzazione del servizio. Il completamento di questo processo potrebbe richiedere alcuni minuti.
5. Aggiorna periodicamente la pagina di benvenuto finché il pulsante Attiva account non diventa il pulsante Dashboard.
6. Scegli Dashboard per iniziare a utilizzare Oracle Database@AWS.

AWS CLI

Per inizializzare Oracle Database@AWS nel tuo account di fiducia utilizzando il, usa il comando. AWS CLI`initialize-service`

```
aws odb initialize-service
```

Per verificare lo stato di inizializzazione, utilizzare il comando. `get-oci-onboarding-status`

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

Una volta completata l'inizializzazione, l'output mostra uno stato di`ACTIVE_LIMITED`, a indicare che il tuo account può accedere a risorse condivise ma non può creare una nuova infrastruttura Exadata o una nuova rete ODB.

Fasi successive

Dopo aver inizializzato Oracle Database@AWS nel proprio account fidato, è possibile effettuare le seguenti operazioni:

- Visualizza le risorse condivise utilizzando i `get` comandi `list` and o nella console. AWS
- Crea cluster di VM e cluster di VM autonomi su un'infrastruttura Exadata condivisa e una rete ODB.
- Crea una connessione peering ODB su una rete ODB condivisa.

Per ulteriori informazioni sull'utilizzo di risorse condivise, vedere. Utilizzo di Oracle Database@AWS risorse condivise in un account affidabile

Utilizzo di Oracle Database@AWS risorse condivise in un account affidabile

Dopo aver condiviso una risorsa con il proprio account di fiducia e aver inizializzato il AWS servizio Oracle Database@, è possibile visualizzare e utilizzare la risorsa condivisa. Questo argomento spiega come utilizzare le risorse condivise in un account affidabile.

Argomenti

- Limitazioni per le risorse condivise in un account affidabile
- Creazione di cluster VM su un'infrastruttura Exadata condivisa
- Visualizzazione delle risorse condivise in un account affidabile
- Configurazione del peering ODB con reti ODB condivise

Limitazioni per le risorse condivise in un account affidabile

Quando lavori con AWS risorse Oracle Database@ condivise, tieni presente le seguenti limitazioni:

- La condivisione delle risorse è supportata solo all'interno della stessa organizzazione. AWS
- Solo l'account acquirente (l'account che accetta l'offerta AWS privata Oracle Database@) può creare l'infrastruttura Exadata e le risorse di rete ODB.
- È possibile creare risorse solo su un'infrastruttura condivisa e solo se si dispone delle autorizzazioni necessarie.
- Le azioni specifiche (autorizzazioni gestite) per ogni tipo di risorsa vengono selezionate automaticamente durante la creazione della condivisione di risorse e non possono essere modificate.
- Non puoi modificare o eliminare le risorse di proprietà di un altro account.
- Le risorse create sull'infrastruttura condivisa sono di proprietà dell'account e vengono conteggiate ai fini delle quote OCI. Lo stesso vale per le risorse principali.
- Se l'account proprietario annulla la condivisione di una risorsa, non è più possibile creare nuove risorse su questa infrastruttura condivisa. Tuttavia, le risorse esistenti continuano a funzionare.
- La condivisione di risorse tra regioni non è supportata. Puoi condividere risorse solo all'interno della stessa AWS regione.
- Le risorse dell'account attendibile vengono fatturate all'acquirente dell'abbonamento Oracle Database@AWS .
- Quando utilizzi una risorsa condivisa, devi fornire l'Amazon Resource Name (ARN).

Creazione di cluster VM su un'infrastruttura Exadata condivisa

Se il tuo account fidato ha accesso a un'infrastruttura Exadata condivisa e a una rete ODB, puoi creare cluster di VM Exadata, cluster di VM autonomi o peering ODB su questa infrastruttura.

> **Note**
>
> Quando utilizzi una risorsa condivisa con te, invece di specificare solo l'ID della risorsa, devi specificare l'Amazon Resource Name (ARN).

Console

1. Apri la console Oracle AWS Database@ all'indirizzo. https://console.aws.amazon.com/odb/
2. Nel pannello di navigazione, scegli Exadata VM clusters o Autonomous VM clusters.
3. Scegli Crea cluster VM o Crea cluster VM autonomo.

4. Per l'infrastruttura Exadata, seleziona l'infrastruttura Exadata condivisa su cui desideri creare il cluster VM.
5. Completa i campi rimanenti come richiesto per la configurazione del cluster VM.
6. Scegli Crea cluster VM o Crea cluster VM autonomo.

AWS CLI

Per creare un cluster VM sull'infrastruttura Exadata condivisa utilizzando, usa il AWS CLI comando: `create-cloud-vm-cluster`

```
aws odb create-cloud-vm-cluster --region us-east-1 \
    --cloud-exadata-infrastructure-id arn:aws:odb:us-east-1:111111111111:cloud-exadata-infrastructure/exa_aaaaaaaaaa \
    --odb-network-id arn:aws:odb:us-east-1:111111111111:odb-network/odbnet_aaaaaaaaaa \
    --cpu-core-count 4 \
    --display-name "Shared-VMC-1" \
    --gi-version "19.0.0.0" \
    --hostname "vmchost" \
    --ssh-public-keys "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQ..." \
```

Per creare un cluster di VM autonomo su un'infrastruttura Exadata condivisa utilizzando il, usa il comando: AWS CLI`create-cloud-vm-cluster`

```
aws odb create-cloud-autonomous-vm-cluster --region us-east-1  \
    --cloud-exadata-infrastructure-id arn:aws:odb:us-east-1:111111111111:cloud-exadata-infrastructure/exa_aaaaaaaaaa \
    --odb-network-id arn:aws:odb:us-east-1:111111111111:odb-network/odbnet_aaaaaaaaaa\
    --display-name "Shared-AVMC-1" \
    --autonomous-data-storage-size-in-tbs 8 \
    --cpu-core-count-per-node 16
```

Il cluster VM viene creato sull'infrastruttura Exadata condivisa specificata ed è di proprietà del tuo account fidato.

Visualizzazione delle risorse condivise in un account affidabile

Puoi visualizzare le risorse che sono state condivise con il tuo account utilizzando la Console di AWS gestione o il AWS CLI.

Console

1. Aprire la console Oracle Database@ all'indirizzo AWS . https://console.aws.amazon.com/odb/
2. Nel pannello di navigazione, scegli il tipo di risorsa che desideri visualizzare: infrastruttura Exadata o rete ODB.
3. La console mostra le risorse condivise con te.
4. Seleziona una risorsa condivisa per visualizzarne i dettagli.

AWS CLI

Per visualizzare le risorse condivise utilizzando il AWS CLI, utilizzare il `list` comando appropriato per il tipo di risorsa. Ad esempio, per elencare l'infrastruttura Exadata:

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

La risposta mostra le risorse condivise con te.

Per ottenere informazioni dettagliate su una risorsa condivisa specifica, usa il `get` comando appropriato con l'ID della risorsa:

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

Configurazione del peering ODB con reti ODB condivise

Per abilitare la comunicazione tra le applicazioni e i database su reti ODB condivise, puoi configurare il peering ODB tra il tuo VPC e la rete ODB condivisa. Per ulteriori informazioni sul peering ODB, vedere. Creazione di una connessione peering ODB in Oracle Database@AWS

Console

1. Aprire la console Oracle Database@AWS all'indirizzo. https://console.aws.amazon.com/odb/
2. Nel riquadro di navigazione, scegli ODB peering.
3. Scegli Crea peering di rete ODB.
4. Per la rete ODB, seleziona la rete ODB condivisa con cui desideri eseguire il peering.
5. Per la rete Peer, seleziona il tuo VPC.
6. Scegli Crea peering di rete ODB.

AWS CLI

Per creare una connessione peering di rete tra il tuo VPC e una rete ODB condivisa utilizzando, usa AWS CLI il comando. `create-odb-peering-connection`

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

Dopo aver creato la connessione peering, aggiorna le tabelle di routing per abilitare il traffico tra le reti peering.

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

Gestione di Oracle Database@AWS

È possibile modificare ed eliminare alcune Oracle Database@AWS risorse dopo averle create.

Aggiornamento di una rete ODB in Oracle Database@AWS

È possibile aggiornare le seguenti risorse di rete ODB:

- Il nome della rete ODB
- Amazon VPC da utilizzare per stabilire una connessione peering ODB alla rete ODB
- Gli intervalli VPC CIDR che possono accedere alle risorse Exadata nella rete ODB

> **Note**
>
> Specificando gli intervalli CIDR, si limita la connettività alle sottoreti VPC necessarie anziché rendere l'intero VPC disponibile per la rete ODB.

Questa sezione presuppone che tu abbia già creato una rete ODB in. Fase 1: Creare una rete ODB in Oracle Database@AWS

Per aggiornare una rete ODB

1. Accedi a Console di gestione AWS e apri la Oracle Database@AWS console all'indirizzo https://console.aws.amazon.com/odb/.
2. Dal riquadro di sinistra, scegli Reti ODB.
3. Seleziona la rete che desideri modificare.
4. Scegli Modifica.
5. (Facoltativo) Per il nome di rete ODB, inserite un nuovo nome di rete. Il nome deve contenere da 1 a 255 caratteri e iniziare con un carattere alfabetico o un carattere di sottolineatura. Non può contenere trattini consecutivi.
6. (Facoltativo) Per Peered CIDRs, specifica gli intervalli CIDR del VPC peered che necessitano di connettività alla rete ODB. Per limitare l'accesso, si consiglia di specificare gli intervalli CIDR minimi richiesti.
7. (Facoltativo) Per configurare le integrazioni dei servizi, seleziona o deseleziona Amazon S3 o Zero-ETL.

8. Scegli Continua, quindi scegli Modifica.

Eliminazione di una rete ODB in Oracle Database@AWS

È possibile eliminare una rete ODB. Questa sezione presuppone che tu abbia già creato una rete ODB in. Fase 1: Creare una rete ODB in Oracle Database@AWS Non è possibile eliminare una rete ODB attualmente utilizzata da un cluster di macchine virtuali.

Per eliminare una rete ODB

1. Accedi a Console di gestione AWS e apri la Oracle Database@AWS console all'indirizzo https://console.aws.amazon.com/odb/.
2. Dal riquadro di sinistra, scegli Reti ODB.
3. Seleziona la rete che desideri eliminare.
4. Scegli Elimina.
5. (Facoltativo) Scegliete Elimina risorse OCI associate per eliminare le risorse OCI create insieme alla rete ODB.
6. Immetti **`delete me`** nella casella di testo.
7. Scegli Elimina.

Eliminazione di un cluster di macchine virtuali in Oracle Database@AWS

È possibile eliminare un cluster di macchine virtuali Exadata o un cluster di macchine virtuali autonome. Questa sezione presuppone che tu abbia già creato un cluster VM in. Fase 3: Creare un cluster di macchine virtuali Exadata o un cluster di macchine virtuali autonome in Oracle Database@AWS

Per eliminare un cluster di macchine virtuali

1. Accedi a Console di gestione AWS e apri la Oracle Database@AWS console all'indirizzo https://console.aws.amazon.com/odb/.
2. Dal riquadro di sinistra, scegli Exadata VM clusters o Autonomous VM clusters.
3. Scegli un cluster di VM da eliminare.

4. Scegli Elimina.
5. Quando richiesto, inserisci **`delete me`** e quindi scegli Elimina.

Eliminazione di un'infrastruttura Oracle Exadata in Oracle Database@AWS

È possibile eliminare un'infrastruttura Oracle Exadata. Questa sezione presuppone che tu abbia già creato un'infrastruttura Oracle Exadata in. Fase 2: Creare un'infrastruttura Oracle Exadata in Oracle Database@AWS Non è possibile eliminare un'infrastruttura Exadata attualmente utilizzata da un cluster di macchine virtuali.

Per eliminare un'infrastruttura Oracle Exadata

1. Accedi a Console di gestione AWS e apri la Oracle Database@AWS console all'indirizzo. https://console.aws.amazon.com/odb/
2. Dal riquadro di sinistra, scegli Infrastrutture Exadata.
3. Scegli un'infrastruttura Exadata da eliminare.
4. Scegli Elimina.
5. Quando richiesto, inserisci **`delete me`** e scegli Elimina.

Eliminazione di una connessione peering ODB

Quando non è più necessaria una connessione peering ODB, è possibile eliminarla. È necessario eliminare tutte le connessioni peering ODB prima di poter eliminare una rete ODB.

Console

1. Accedi a Console di gestione AWS e apri la console all' Oracle Database@AWS indirizzo. https://console.aws.amazon.com/odb/
2. Nel riquadro di navigazione, scegli Connessioni peering ODB.
3. Seleziona la connessione peering ODB da eliminare.
4. Scegli Elimina.
5. Per confermare l'eliminazione, inserisci **`delete me`** e scegli Elimina.

AWS CLI

Per eliminare una connessione peering ODB, usa il `delete-odb-peering-connection` comando.

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

Backup in Oracle Database@AWS

Oracle Database@AWS offre diverse opzioni di backup per proteggere i database Oracle. Puoi utilizzare backup gestiti da Oracle che si integrano perfettamente con Amazon S3 o creare backup gestiti dall'utente utilizzando Oracle Recovery Manager (RMAN).

Backup gestiti da Oracle su Amazon S3

Quando si crea una rete ODB, Oracle Database@ configura AWS automaticamente l'accesso alla rete per i backup gestiti da Oracle su Amazon S3. OCI configura le voci DNS e gli elenchi di sicurezza necessari. Queste configurazioni consentono il traffico tra OCI Virtual Cloud Network (VCN) e Amazon S3. La rete ODB non abilita o controlla i backup automatici.

I backup gestiti da Oracle sono completamente gestiti da OCI. Quando si crea il database Oracle Exadata, è possibile abilitare i backup automatici selezionando Abilita backup automatici nella console OCI. Scegli una delle seguenti destinazioni di backup:

- Amazon S3
- Archiviazione di oggetti OCI
- Servizio di ripristino autonomo

Per ulteriori informazioni, vedere Backup Exadata Database nella documentazione OCI.

Backup gestiti dall'utente su Amazon S3 in Oracle Database@AWS

Con Oracle Database@AWS, puoi creare backup del tuo database gestiti dall'utente utilizzando il servizio di database Exadata su un'infrastruttura dedicata. Esegui il backup dei dati con Oracle Recovery Manager (RMAN) e li archivia nei bucket Amazon S3. Hai il pieno controllo sulla pianificazione dei backup, sulle politiche di conservazione e sui costi di storage, mantenendo al contempo i vantaggi del servizio gestito di Oracle Database@.AWS

> **Note**
>
> Oracle Database@AWS non supporta i backup gestiti dagli utenti per Autonomous Database@ su infrastruttura dedicata.

I backup gestiti dall'utente completano le soluzioni di backup gestito fornite da Oracle AWS Database@.AWSÈ possibile utilizzare backup manuali per requisiti di conformità, disaster recovery tra regioni o integrazione con i flussi di lavoro di gestione dei backup esistenti.

È possibile utilizzare le seguenti tecniche di backup gestite dall'utente:

Oracle Secure Backup

Trasmetti i backup direttamente su Amazon S3 con prestazioni ottimali.

Storage Gateway

Utilizza Storage Gateway per backup basati su file che utilizzano una condivisione NFS.

Punto di montaggio S3

Usa un client di file per montare un bucket Amazon S3 come file system locale.

Prerequisiti per i backup gestiti dall'utente su Amazon S3 in Oracle Database@AWS

Prima di eseguire il backup dei database Oracle Exadata su Amazon S3, procedi come segue:

1. Abilita l'accesso diretto ad Amazon S3 dalla tua rete ODB.
2. Configura la connettività di rete e il routing tra Oracle Database@ e Amazon AWS S3.

Abilitazione dell'accesso dalla rete ODB ad Amazon S3

Per eseguire il backup manuale del database su Amazon S3, abilita l'accesso diretto a S3 dalla tua rete ODB. Questa tecnica consente ai tuoi database di accedere ad Amazon S3 per le tue esigenze aziendali, come l'importazione/esportazione di dati o i backup gestiti dagli utenti. Hai il pieno controllo sulla destinazione di destinazione dello storage di backup e puoi utilizzare le policy per limitare l'accesso ad Amazon S3 utilizzando VPC Lattice.

L'accesso diretto ad Amazon S3 dalla rete ODB non è abilitato per impostazione predefinita. Puoi abilitare l'accesso a S3 quando crei o modifichi la tua rete ODB.

Console

Per abilitare l'accesso diretto ad Amazon S3 dalla tua rete ODB

1. Apri la console Oracle Database@AWS all'indirizzo. https://console.aws.amazon.com/odb/
2. Nel riquadro di navigazione, scegli Reti ODB.
3. Seleziona la rete ODB per la quale desideri abilitare l'accesso ad Amazon S3.
4. Scegli Modifica.
5. Seleziona Amazon S3.
6. (Facoltativo) Configura un documento di policy di Amazon S3 per controllare l'accesso ad Amazon S3. Se non specifichi una policy, la policy predefinita garantisce l'accesso completo.
7. Scegli Continua e poi Modifica.

AWS CLI

Per abilitare l'accesso diretto ad Amazon S3 dalla tua rete ODB, usa il `update-odb-network` comando con il parametro: `s3-access`

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

Per configurare un documento di policy di Amazon S3, utilizza il `--s3-policy-document` parametro:

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

Quando l'accesso ad Amazon S3 è abilitato, puoi accedere ad Amazon S3 dalla tua rete ODB utilizzando il DNS regionale. `s3.region.amazonaws.com` OCI configura questo nome DNS per impostazione predefinita. Per utilizzare un nome DNS personalizzato, modifica il DNS VCN per garantire che il DNS personalizzato si risolva nell'indirizzo IP dell'endpoint della rete di servizio.

Configurazione della connettività di rete tra Oracle AWS Database@ e Amazon S3

Per consentire backup gestiti dagli utenti su Amazon S3, la macchina virtuale deve essere in grado di accedere all'endpoint Amazon VPC S3. Nella console OCI, puoi modificare le regole di sicurezza

in un gruppo di sicurezza di rete (NSG) per controllare il traffico in ingresso e in uscita. Per i backup gestiti dagli utenti, il traffico scorre sulla sottorete client anziché sulla sottorete di backup. Nei passaggi seguenti, si aggiorna la sottorete del client NSGs per aggiungere la regola di uscita per l'indirizzo IP dell'endpoint VPC.

Per consentire l'accesso delle macchine virtuali all'endpoint Amazon S3

1. Apri la console Oracle AWS Database@ all'indirizzo. https://console.aws.amazon.com/odb/
2. Scegli reti ODB.
3. Scegli il nome della rete ODB.
4. Scegli le risorse OCI.
5. Scegli la scheda Integrazioni di servizio.
6. In Amazon S3, prendi nota delle seguenti informazioni:
   - L' IPv4 indirizzo dell'endpoint Amazon VPC S3. Queste informazioni ti serviranno in seguito. Ad esempio, l'indirizzo IP potrebbe essere`192.168.12.223`.
   - Il nome di dominio dell'endpoint Amazon VPC S3. Queste informazioni ti serviranno in un secondo momento. Ad esempio, il nome di dominio potrebbe esseres`3.us-east-1.amazonaws.com`.
7. Nel riquadro di navigazione a sinistra, scegli Exadata VM clusters, quindi scegli il nome del tuo cluster VM.
8. Nella parte superiore della pagina, scegli la scheda Riepilogo.
9. Scegli Macchine virtuali, quindi scegli il nome della tua macchina virtuale.
10. Nota il valore in DNS Name. Questo è il nome host che specifichi quando ti connetti alla tua macchina virtuale utilizzando. `ssh`
11. In alto a destra, scegli Gestisci in OCI. Si apre la console OCI.
12. Nella pagina dell'elenco delle reti di cloud virtuale, scegli il VCN che contiene il gruppo di sicurezza di rete (NSG) per la sottorete del client di rete ODB (). `exa_static_nsg` Per ulteriori informazioni, vedere Gestione delle regole di sicurezza per un NSG nella documentazione OCI.
13. Nella pagina dei dettagli, esegui una delle seguenti azioni a seconda dell'opzione visualizzata:
    - Nella scheda Sicurezza, vai a Gruppi di sicurezza di rete.
    - In Risorse, scegli Gruppi di sicurezza di rete.
14. Scegliete l'NSG per la sottorete del client ()`exa_static_nsg`.
15. Aggiungi una regola di uscita per l'indirizzo dell'endpoint VPC che hai annotato in precedenza.

Per testare la connettività a S3 dalla tua macchina virtuale

1. Utilizzalo `ssh` per connetterti `root` alla macchina virtuale di cui hai ottenuto il nome DNS in precedenza. Quando ti connetti, specifica un `.pem` file con le tue chiavi SSH.
2. Esegui i seguenti comandi per assicurarti che la macchina virtuale possa accedere all'endpoint Amazon VPC Amazon S3. Usa il nome di dominio S3 che hai annotato in precedenza.

```
# 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
```

Backup su Amazon S3 con Oracle Secure Backup

Oracle Secure Backup funge da interfaccia SBT da utilizzare con Recovery Manager (RMAN). Puoi utilizzare RMAN con Oracle Secure Backup per eseguire il backup dei database Oracle Database@ direttamente su Amazon AWS S3. Oracle Secure Backup offre i seguenti vantaggi:

- Oracle Secure Backup ottimizza il trasferimento dei dati tra RMAN e S3.
- Non è necessaria alcuna archiviazione di backup intermedia.
- Oracle Secure Backup gestisce il ciclo di vita dei supporti di backup.

Per eseguire il backup su Amazon S3 utilizzando Oracle Secure Backup

1. Installa il modulo Oracle Secure Backup sul tuo server VM Exadata. Sostituisci i valori segnaposto con la tua chiave di accesso e la chiave di AWS accesso segreta. Per ulteriori informazioni, consulta la documentazione Oracle all'indirizzo Backup to Cloud with Oracle Secure Backup Cloud Module.

```
cd $ORACLE_HOME/lib
java -jar osbws_install.jar -AWSID aws-access-key-id -AWSKey aws-secret-access-
key -walletDir $ORACLE_HOME/dbs/osbws_wallet -location us-west-2 -useHttps -
awsEndPoint s3.us-west-2.amazonaws.com
```

2. Connect a RMAN e configura il canale di backup e il tipo di dispositivo predefinito.

```
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. Verifica la configurazione.

```
RMAN> SHOW ALL;
```

4. Esegui il backup del database.

```
RMAN> BACKUP DATABASE;
```

5. Verificare che il backup sia stato completato correttamente.

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

Backup su Amazon S3 Gateway di archiviazione AWS utilizzando su Amazon EC2

Gateway di archiviazione AWS è un servizio ibrido che collega l'ambiente locale ai Cloud AWS servizi di storage. Per i AWS backup Oracle Database@, puoi utilizzare Storage Gateway per creare un flusso di lavoro di backup basato su file che scrive direttamente su Amazon S3. A differenza della tecnica Oracle Secure Backup, gestisci il ciclo di vita dei backup.

In questa soluzione, crei un' EC2 istanza Amazon separata per la configurazione di Storage Gateway. Puoi anche aggiungere un volume Amazon EBS per memorizzare nella cache le letture e le scritture su Amazon S3.

Questa tecnica offre i seguenti vantaggi:

- Non è necessario un gestore di contenuti multimediali come Oracle Secure Backup.
- Non è necessaria alcuna archiviazione di backup intermedia.

Per implementare lo Storage Gateway e creare una condivisione di file

1. Apri Console di gestione AWS at https://console.aws.amazon.com/storagegateway/home/ e scegli la AWS regione in cui desideri creare il gateway.

2. Implementa e attiva un gateway di file Amazon S3, utilizzando un'istanza EC2 Amazon come hub. Segui le istruzioni in Deploy a Amazon EC2 host personalizzato per S3 File Gateway nella Storage Gateway User Guide.

   Quando configuri il tuo file gateway, assicurati di fare quanto segue:

   - Aggiungi almeno un volume Amazon EBS per lo storage della cache, con una dimensione di almeno 150 GiB.
   - Apri la TCP/UDP porta 2049 per l'accesso NFS nel tuo gruppo di sicurezza. Ciò consente di creare condivisioni di file NFS.
   - Apri la porta TCP 80 per il traffico in entrata per consentire l'accesso HTTP una tantum durante l'attivazione del gateway. Dopo l'attivazione, è possibile chiudere questa porta.
3. Crea un endpoint Amazon VPC per la connettività privata tra la tua rete ODB e lo Storage Gateway. Per ulteriori informazioni, consulta Accedere a un AWS servizio utilizzando un endpoint VPC di interfaccia.
4. Crea una condivisione di file per il tuo bucket Amazon S3 tramite la console Storage Gateway. Per ulteriori informazioni, consulta Creazione di una condivisione di file.

Per eseguire il backup del database su Amazon S3 utilizzando Storage Gateway

1. In un terminale, usa `ssh` per connetterti al nome DNS della macchina virtuale Exadata. Per trovare il nome DNS, vedi. Prerequisiti per i backup gestiti dall'utente su Amazon S3 in Oracle Database@AWS
2. Crea una directory sul server cluster Exadata VM per il montaggio NFS. Nell'esempio seguente viene creata la directory `/home/oracle/sgw_mount/`.

   ```
   mkdir /home/oracle/sgw_mount/
   ```
3. Monta la condivisione NFS sulla directory che hai appena creato. L'esempio seguente crea la condivisione nella directory`/home/oracle/sgw_mount/`. Sostituiscilo *`SG-IP-address`* con l'indirizzo IP dello Storage Gateway e *`your-bucket-name`* con il nome del bucket S3.

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

4. Connect a RMAN ed esegui il backup del database nella directory montata. L'esempio seguente crea il canale `rman_local_bkp` e utilizza il percorso del punto di montaggio per formattare i pezzi di backup.

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

5. Verificate che i file di backup siano creati nella directory di montaggio. L'esempio seguente mostra due parti di backup.

```
$ ls -lart /home/oracle/sgw_mount/
total 8569632
-rw-r----- 1 oracle asmdba 1112223334 Jul 10 20:51 1a2b34cd_1234_1_1
drwxrwxrwx 1 nobody nobody 0 Jul 10 20:56 .
-rw-r----- 1 oracle asmdba 5556667778 Jul 10 20:56 1a2b34cd_1235_1_1
```

Backup su Amazon S3 utilizzando un punto di montaggio S3

Puoi utilizzare il mount point di Amazon S3 per creare prima i backup localmente e poi copiarli su Amazon S3. Questa tecnica crea backup sullo storage locale e quindi li trasferisce su Amazon S3 utilizzando l'interfaccia mount point. Il tempo di backup è più lungo rispetto ad altre tecniche perché è necessario eseguire il backup dei dati due volte.

> **Note**
>
> Il backup diretto su Amazon S3 utilizzando il punto di montaggio, senza staging, non è supportato. RMAN richiede autorizzazioni specifiche per il file system che non sono compatibili con l'interfaccia del punto di montaggio di Amazon S3.

Questa tecnica non richiede la licenza di un gestore multimediale come Oracle Secure Backup. Gestisci il ciclo di vita dei tuoi backup.

Per eseguire il backup su Amazon S3 utilizzando un punto di montaggio S3

1. In un terminale, usa `ssh` per connetterti al nome DNS della macchina virtuale Exadata. Per trovare il nome DNS, vedi. Prerequisiti per i backup gestiti dall'utente su Amazon S3 in Oracle Database@AWS

2. Installa il mount point Amazon S3 sul server cluster Exadata VM. Per ulteriori informazioni sull'installazione e la configurazione, consulta Mountpoint for Amazon S3 nella Amazon S3 User Guide.

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

3. Verifica l'installazione eseguendo il comando. `mount-s3`

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

4. Creare una directory di backup intermedia sullo storage locale del server cluster Exadata VM. Eseguirai il backup del database in questa directory locale e quindi copierai il backup nel tuo bucket S3. L'esempio seguente crea una directory. `/u02/rman_bkp_local`

```
mkdir /u02/rman_bkp_local
```

5. Crea una directory per il punto di montaggio di Amazon S3. L'esempio seguente crea una directory`/home/oracle/s3mount`.

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

6. Monta il tuo bucket Amazon S3 utilizzando il punto di montaggio. L'esempio seguente monta un bucket S3 sulla directory. `/home/oracle/s3mount` *`your-s3-bucket-name`*Sostituiscilo con il nome effettivo del bucket Amazon S3.

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

7. Verifica di poter accedere ai contenuti del bucket Amazon S3.

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

8. Connect RMAN al database di destinazione ed eseguine il backup nella directory di staging locale. L'esempio seguente crea il canale `rman_local_bkp` e utilizza il percorso `/u02/rman_bkp_local/` per formattare i pezzi di backup.

```
$ rman TARGET /

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

9. Verificate che i backup siano creati nella directory locale:

```
$ 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. Copia i file di backup dalla directory di staging locale al punto di montaggio di Amazon S3.

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

11. Verifica di aver copiato correttamente i file su 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
```

Disabilitazione dell'accesso diretto ad Amazon S3

Se non hai più bisogno dell'accesso diretto ad Amazon S3 dalla tua rete ODB, puoi disabilitarlo. L'abilitazione o la disabilitazione dell'accesso diretto alla rete a S3 non influisce sull'accesso di rete ai backup gestiti da Oracle su Amazon S3.

Console

Per disabilitare l'accesso diretto ad Amazon S3

1. Apri la console Oracle Database@AWS all'indirizzo. https://console.aws.amazon.com/odb/
2. Nel riquadro di navigazione, scegli Reti ODB.
3. Seleziona la rete ODB per la quale desideri disabilitare l'accesso ad Amazon S3.
4. Scegli Modifica.
5. Deseleziona la casella di controllo Abilita l'accesso a S3.
6. Scegli Modifica rete ODB.

AWS CLI

Usa il comando `update-odb-network` con il parametro `s3-access`.

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

Risoluzione dei problemi di integrazione con Amazon S3

Se riscontri problemi con i backup gestiti da Oracle su Amazon S3 o l'accesso diretto ad Amazon S3, considera i seguenti passaggi per la risoluzione dei problemi:

Non è possibile accedere ad Amazon S3 dal tuo database

Verifica quanto segue:

- Verifica che l'accesso ad Amazon S3 sia abilitato per la tua rete ODB. Usa l'`GetOdbNetwork`azione per verificare se lo `s3Access` stato è. `Enabled`
- Assicurati di utilizzare il nome DNS regionale corretto:`s3.region.amazonaws.com`.
- Verifica che il tuo database Oracle disponga delle autorizzazioni necessarie per accedere ad Amazon S3.

I backup gestiti da Oracle non sono riusciti

Verifica quanto segue:

- I backup gestiti da Oracle su Amazon S3 sono abilitati per impostazione predefinita e non possono essere disabilitati. Se i backup falliscono, controlla i log del database Oracle per messaggi di errore specifici.
- Verifica che le risorse Amazon VPC Lattice siano configurate correttamente visualizzando le risorse di integrazione del servizio.
- Contatta Oracle Support per ricevere assistenza sui problemi relativi ai backup automatici gestiti da Oracle. Per ulteriori informazioni, consulta Ottenere supporto per Oracle Database@AWS.

Integrazione di Oracle Database@AWS Zero-ETL con Amazon Redshift

L'integrazione Zero-ETL è una soluzione completamente gestita che rende disponibili i dati transazionali e operativi in Amazon Redshift da più fonti. Con questa soluzione, puoi replicare i dati su Amazon Redshift dai tuoi database Oracle in esecuzione su Oracle Exadata o Autonomous Database su un'infrastruttura Exadata dedicata. La sincronizzazione automatica evita il tradizionale processo di estrazione, trasformazione e caricamento (ETL). Consente inoltre analisi in tempo reale e carichi di lavoro di intelligenza artificiale. Per ulteriori informazioni, consulta Integrazioni Zero-ETL nella Guida alla gestione di Amazon Redshift.

L'integrazione zero-ETL offre i seguenti vantaggi:

- Replica dei dati in tempo reale: sincronizzazione continua dei dati dai database Oracle ad Amazon Redshift con latenza minima
- Eliminazione di pipeline ETL complesse: non è necessario creare e mantenere soluzioni di integrazione dei dati personalizzate
- Sovraccarico operativo ridotto: configurazione e gestione automatizzate tramite AWS APIs
- Architettura di integrazione dei dati semplificata: perfetta integrazione tra Oracle AWS Database@ e i servizi di analisi AWS
- Sicurezza avanzata: crittografia integrata e controlli di accesso IAM AWS

Amazon Redshift non addebita costi aggiuntivi per l'integrazione Zero-ETL con Oracle Database@.AWS Paghi per le risorse Amazon Redshift esistenti utilizzate per creare ed elaborare i dati di modifica creati come parte di un'integrazione zero-ETL. Per ulteriori informazioni sui prezzi, consultare Prezzi di Amazon Redshift.

Versioni di database supportate per l'integrazione zero-ETL in Oracle Database@AWS

L'integrazione zero-ETL supporta le seguenti versioni del database Oracle:

- Oracle Exadata — Oracle Database 19c
- Database autonomo su infrastruttura dedicata: Oracle Database 19c e 23ai

Come funziona l'integrazione Zero-ETL in Oracle Database@AWS

L'integrazione zero-ETL consente a Oracle Database@ di AWS replicare i dati su Amazon Redshift. L'integrazione sfrutta Amazon VPC Lattice per creare una connettività di rete sicura. La tecnologia Change Data Capture (CDC) garantisce la sincronizzazione dei dati in tempo reale. Gestisci l'integrazione tramite. AWS Glue APIs

L'architettura di integrazione Zero-ETL include quanto segue:

- Connettività sicura: utilizza la SSL/TLS crittografia sulla porta TLS 2484 per il trasferimento dei dati
- AWS Secrets Manager: archivia le credenziali e i certificati del database in modo sicuro utilizzando il servizio di gestione AWS delle chiavi
- AWS Integrazione Glue: fornisce un'interfaccia di gestione unificata per integrazioni zero-ETL

La replica procede attraverso i seguenti passaggi:

1. Stabilire una connessione sicura al database Oracle utilizzando SSL sulla porta 2484
2. Esecuzione di un dump completo iniziale di database, schemi e tabelle selezionati
3. Configurazione dell'acquisizione dei dati di modifica (CDC) per la replica continua in tempo reale
4. Scrittura dei dati replicati nel cluster Amazon Redshift di destinazione

> **Important**
>
> L'integrazione zero-ETL non è abilitata per impostazione predefinita. È necessario configurarla utilizzando. AWS Glue APIs Non è possibile configurare l'integrazione zero-ETL direttamente utilizzando Oracle Database@.AWS APIs

Prerequisiti per l'integrazione zero-ETL in Oracle Database@AWS

Prima di configurare l'integrazione zero-ETL, assicurati di soddisfare i seguenti prerequisiti.

Prerequisiti generali

- AWS Configurazione Oracle Database@: assicurati di avere almeno un cluster di macchine virtuali fornito e in esecuzione.

- Integrazione con Zero-ETL abilitata: assicurati che il cluster VM o il cluster VM autonomo sia associato a una rete ODB con Zero-ETL abilitato.
- Versioni di Oracle Database supportate: è necessario utilizzare Oracle Database 19c (Oracle Exadata) o Oracle Database 19c/23ai (Autonomous Database on Dedicated Infrastructure).
- Stessa AWS regione: il database Oracle di origine e il cluster Amazon Redshift di destinazione devono trovarsi nella stessa AWS regione.

Prerequisiti del database Oracle

È necessario configurare il database Oracle con le seguenti impostazioni.

Configurazione utente di replica

Crea un utente di replica dedicato in ogni database collegabile (PDB) che desideri replicare:

- Per Oracle Exadata: crea un utente con una password sicura. `ODBZEROETLADMIN`
- Per un database autonomo su un'infrastruttura dedicata: utilizza l'utente esistente`GGADMIN`.

Concedi le seguenti autorizzazioni all'utente di replica.

```
-- 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";
```

Registrazione supplementare

Abilita la registrazione supplementare sul tuo database Oracle per acquisire i dati di modifica.

```
-- 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;
```

Per configurare un'integrazione zero-ETL tra Oracle Database@AWS e Amazon Redshift, devi configurare SSL.

Per i database Oracle Exadata

È necessario configurare manualmente SSL sulla porta 2484. Questa attività prevede quanto segue:

- Configurazione in `(PROTOCOL=tcps)(PORT=2484)` `listener.ora`
- Configurazione del portafoglio utilizzando `sqlnet.ora`
- Generazione e configurazione di certificati SSL (vedi Come configurare SSL/TCPS per Exadata Cloud Database (exACC/ExACS) (Doc ID 2947301.1) nella documentazione di My Oracle Support)

Per database autonomi

SSL sulla porta 2484 è abilitato per impostazione predefinita. e non sono necessarie ulteriori configurazioni.

> **Important**
>
> La porta SSL è fissa come 2484.

AWS prerequisiti del servizio

Prima di configurare l'integrazione zero-ETL, configura AWS Secrets Manager e configura le autorizzazioni IAM.

Configurare AWS Secrets Manager

Archivia le credenziali del database Oracle in AWS Secrets Manager come segue:

1. Crea una chiave gestita dal cliente (CMK) nel servizio di gestione delle AWS chiavi.
2. Memorizza le credenziali del database in AWS Secrets Manager utilizzando CMK.
3. Configura le politiche delle risorse per consentire l'accesso a Oracle Database@AWS .

Per ottenere l'ID e la password della chiave TDE, utilizzare la tecnica descritta in Metodi di crittografia supportati per l'utilizzo di Oracle come origine per il AWS Database Migration Service. Il comando seguente genera il portafoglio base64.

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

L'esempio seguente mostra un segreto per Oracle Exadata. Perché*asm_service_name*, *111.11.11.11* rappresenta l'IP virtuale per il nodo VM. È inoltre possibile registrare il listener 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"
  }
```

```
}
```

L'esempio seguente mostra un segreto per Autonomous Database on Dedicated Infrastructure.

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

Configurazione delle autorizzazioni IAM

Crea policy IAM che consentano operazioni di integrazione zero-ETL. La seguente policy di esempio consente di descrivere, creare, aggiornare ed eliminare le operazioni per un cluster di macchine virtuali Exadata. Per un cluster di macchine virtuali autonome, utilizzare il valore `cloud-autonomous-vm-cluster` anziché `cloud-vm-cluster` per la risorsa ARN.

Considerazioni sull'integrazione zero-ETL in Oracle Database@AWS

Quando configuri l'integrazione zero-ETL tra Amazon Redshift e Amazon Oracle Database@AWS Redshift, considera le seguenti linee guida:

Tempo di caricamento iniziale dei dati

Il tempo iniziale di caricamento completo dipende dalla dimensione del database. I database di grandi dimensioni potrebbero impiegare diverse ore o giorni per completare la sincronizzazione iniziale.

Prestazioni del database Oracle

L'acquisizione dei dati delle modifiche potrebbe influire sulle prestazioni del database Oracle, specialmente durante volumi di transazioni elevati. Dopo aver abilitato l'integrazione zero-ETL, monitora le prestazioni del database.

Modifiche allo schema

Le modifiche al Data Definition Language (DDL) nel database Oracle di origine potrebbero richiedere l'intervento manuale per ricreare l'integrazione. Pianifica attentamente le modifiche allo schema.

Per considerazioni generali, consulta Considerazioni sull'utilizzo di integrazioni zero-ETL con Amazon Redshift.

Limitazioni per l'integrazione zero-ETL in Oracle Database@AWS

Tieni presente le seguenti limitazioni generali:

Un singolo PDB per integrazione

Ogni integrazione zero-ETL può replicare i dati solo da un database collegabile (PDB). I filtri di dati, ad esempio, non sono supportati. `include: pdb1.*.*, include: pdb2.*.*`

Integrazione singola per Autonomous Database o Exadata Infrastructure

Ogni integrazione zero-ETL può solo replicare i dati da un database autonomo su un'infrastruttura dedicata.

Porta SSL fissa

Le connessioni SSL devono utilizzare la porta 2484.

Requisito della stessa regione

Il cluster Oracle Database@AWS VM di origine e il cluster Amazon Redshift di destinazione devono trovarsi nella stessa regione. AWS La replica tra regioni non è supportata.

Nessun supporto MTLS

Il Mutual TLS (mTLS) non è supportato. Se il database OCI ha MTL abilitato, è necessario disabilitarlo per utilizzare l'integrazione Zero-ETL.

Impostazioni di integrazione immutabili

Dopo aver creato la chiave ARN o KMS segreta associata a un'integrazione, non puoi modificarla. È necessario eliminare e ricreare l'integrazione per modificare queste impostazioni.

Crittografia TDE a livello di colonna

La crittografia trasparente dei dati (TDE) a livello di colonna non è supportata per i database Oracle Exadata. È supportato solo il TDE a livello di tablespace.

Supporto dei tipi di dati

Alcuni tipi di dati specifici di Oracle potrebbero non essere completamente supportati o potrebbero richiedere una trasformazione durante la replica. Testa a fondo i tuoi tipi di dati specifici prima di distribuire il database in produzione.

Configurazione delle AWS integrazioni Oracle Database@ con Amazon Redshift

Per configurare l'integrazione zero-ETL tra il tuo database Oracle e Amazon Redshift, completa i seguenti passaggi:

1. Abilita Zero-ETL sulla tua rete ODB.
2. Configura i prerequisiti del database Oracle.
3. Configurare AWS Secrets Manager e AWS Key Management Service.
4. Configura le autorizzazioni IAM.
5. Configura le policy relative alle risorse di Amazon Redshift.
6. Crea l'integrazione zero-ETL.
7. Crea il database di destinazione in Amazon Redshift.

Passaggio 1: abilita Zero-ETL per la tua rete ODB

È possibile abilitare l'integrazione zero-ETL per la rete ODB associata al cluster VM di origine. Per impostazione predefinita, questa integrazione è disabilitata.

Console

Per abilitare l'integrazione zero-ETL

1. Aprire la console Oracle AWS Database@ all'indirizzo. https://console.aws.amazon.com/odb/
2. Nel riquadro di navigazione, scegli Reti ODB.
3. Seleziona la rete ODB per la quale desideri abilitare l'integrazione zero-ETL.

4. Scegli Modifica.
5. Seleziona zero-ETL.
6. Scegli Continua e poi Modifica.

AWS CLI

Per abilitare l'integrazione zero-ETL, utilizzate il `update-odb-network` comando con il parametro: `--zero-etl-access`

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

Per abilitare l'integrazione zero-ETL per la rete ODB associata al cluster VM di origine, utilizzare il comando. `update-odb-network` Questo comando configura l'infrastruttura di rete richiesta per l'integrazione zero-ETL.

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

Fase 2: Configurazione del database Oracle

Completa la configurazione del database Oracle come descritto nei Prerequisiti:

- Creare utenti di replica e concedere le autorizzazioni necessarie.
- Abilita i redo log archiviati.
- Configura SSL (solo Oracle Exadata).
- Configura gli utenti ASM, se applicabile (solo Oracle Exadata).

Fase 3: Configurare AWS Secrets Manager e AWS Key Management Service

Crea una chiave gestita dal cliente (CMK) e archivia le credenziali del database.

1. Crea una CMK nel servizio di gestione delle AWS chiavi utilizzando il comando. `create-key`

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

2. Archivia le credenziali del database in AWS Secrets Manager.

```
aws secretsmanager create-secret \
  --name "ODBZeroETLCredentials" \
  --description "Credentials for Oracle Database@AWS Zero-ETL integration" \
  --kms-key-id your-cmk-key-arn \
  --secret-string file://secret-content.json
```

3. Allega una policy relativa alle risorse al segreto per consentire l'accesso a Oracle Database@AWS .

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

Nel comando precedente, `secret-resource-policy.json` contiene il seguente codice JSON.

JSON

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

```
}
```

4. Allega una politica delle risorse alla CMK. La politica delle risorse CMK deve includere le autorizzazioni sia per il principale del servizio Oracle Database@ che per il principale del AWS servizio Amazon Redshift per supportare l'integrazione zero-ETL crittografata.

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

Il file deve includere le seguenti dichiarazioni politiche. `cmk-resource-policy.json` La prima istruzione consente l'accesso al AWS servizio Oracle Database@ e la seconda istruzione consente ad Amazon Redshift di creare concessioni sulla chiave KMS per operazioni di dati crittografati.

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"
          ]
        }
      }
    }
  ]
}
```

Fase 4: Configurazione delle autorizzazioni IAM

Crea e allega policy IAM che consentano operazioni di integrazione zero-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 seguente politica concede le autorizzazioni necessarie.

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": "*"
    }
  ]
}
```

Fase 5: Configurazione delle policy relative alle risorse di Amazon Redshift

Configura politiche relative alle risorse sul tuo cluster Amazon Redshift per autorizzare le integrazioni in entrata.

```
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**
>
> In alternativa, puoi utilizzare l'opzione Fix it for me nella console. AWS Questa opzione configura automaticamente le politiche Amazon Redshift richieste senza che tu debba farlo manualmente.

Passaggio 6: crea l'integrazione zero-ETL utilizzando AWS Glue

Crea l'integrazione zero-ETL utilizzando il comando. AWS Glue `create-integration` In questo comando, specifichi il cluster di macchine virtuali di origine e lo spazio dei nomi Amazon Redshift di destinazione.

L'esempio seguente crea un'integrazione con un PDB denominato in `pdb1` esecuzione in un cluster di macchine virtuali Exadata. È inoltre possibile creare un cluster di macchine virtuali autonome sostituendolo `cloud-vm-cluster` con l'`cloud-autonomous-vm-cluster`ARN di origine. La specificazione di una chiave KMS è facoltativa. Se specifichi una chiave, questa può essere diversa da quella in cui hai creato. Fase 3: Configurare AWS Secrets Manager e 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"
```

Il comando restituisce un ARN di integrazione e imposta lo stato su. `creating` È possibile monitorare lo stato dell'integrazione utilizzando il `describe-integrations` comando.

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

> **Important**
>
> È supportato un solo PDB per integrazione. Il filtro dati deve specificare un singolo PDB, ad esempio. `include: pdb1.*.*` L'origine deve trovarsi nella stessa AWS regione e nello stesso account in cui viene creata l'integrazione.

Fase 7: creare un database di destinazione in Amazon Redshift

Dopo che l'integrazione è attiva, crea un database di destinazione nel tuo cluster 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";
```

Dopo aver creato il database di destinazione, puoi interrogare i dati replicati.

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

-- Connect to the new database
\c target_database_name

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

Verifica l'integrazione Zero-ETL

Verifica che l'integrazione funzioni interrogando lo stato dell'integrazione AWS Glue e assicurandoti che le modifiche a Oracle vengano replicate su Amazon Redshift.

Per verificare che l'integrazione zero-ETL funzioni correttamente

1. Verifica lo stato dell'integrazione.

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

   Lo stato dovrebbe essere `ACTIVE` o`REPLICATING`.

2. Verifica la replica dei dati apportando modifiche al tuo database Oracle e verificando che vengano visualizzate in Amazon Redshift.
3. Monitora i parametri di replica in Amazon CloudWatch (se disponibili).

Filtraggio dei dati per integrazioni zero-ETL in Oracle Database@AWS

Oracle Database@AWS Le integrazioni zero-ETL supportano il filtraggio dei dati. È possibile utilizzarlo per controllare quali dati il database Oracle Exadata di origine replica nel data warehouse di destinazione. Invece di replicare l'intero database, puoi applicare uno o più filtri per includere o escludere selettivamente delle tabelle specifiche. Ciò consente di ottimizzare le prestazioni di archiviazione e query assicurando che vengano trasferiti solo i dati pertinenti. Il filtraggio è limitato ai livelli di database e tabella. Il filtraggio a livello di colonna e riga non è supportato.

Oracle Database e Amazon Redshift gestiscono le lettere maiuscole e minuscole del nome oggetto in modo diverso. Ciò influisce sia sulla configurazione del filtro dei dati sia sulle query di destinazione. Tenere presente quanto segue:

- Oracle Database memorizza i nomi di database, schemi e oggetti con le lettere maiuscole, a meno che non vengano esplicitamente inseriti tra virgolette nell'istruzione `CREATE`. Ad esempio, se si crea `mytable` (senza virgolette), il dizionario dei dati Oracle memorizza il nome della tabella come `MYTABLE`. Se si cita il nome dell'oggetto nella dichiarazione di creazione, il dizionario dei dati di Oracle mantiene le maiuscole e minuscole.
- I filtri dei dati Zero-ETL fanno distinzione tra maiuscole e minuscole e devono corrispondere esattamente alle maiuscole e minuscole dei nomi degli oggetti così come appaiono nel dizionario dei dati Oracle. Ad esempio, se il dizionario Oracle memorizza lo schema e il nome della tabella`REINVENT.MYTABLE`, crea un filtro utilizzando`include: ORCL.REINVENT.MYTABLE`.

- Le query di Amazon Redshift utilizzano per impostazione predefinita i nomi di oggetti in minuscolo, a meno che non vengano esplicitamente inseriti tra virgolette. Ad esempio, una query di `MYTABLE` (senza virgolette) cerca `mytable`.

Tieni presente le differenze tra maiuscole e minuscole quando crei il filtro Amazon Redshift ed esegui query sui dati. Le considerazioni sui filtri per Oracle Database@AWS sono le stesse di Amazon RDS for Oracle. Per esempi di come le maiuscole e minuscole possono influire sui filtri di dati in un database Oracle, consulta gli esempi di RDS for Oracle nella Amazon Relational Database Service User Guide.

Monitoraggio dell'integrazione zero-ETL

Il monitoraggio regolare dell'integrazione zero-ETL garantisce prestazioni ottimali e aiuta a identificare tempestivamente i problemi.

Monitoraggio dello stato di integrazione

Monitora lo stato delle tue integrazioni zero-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
```

Gli stati di integrazione includono:

- creazione: l'integrazione è in fase di configurazione
- attivo: l'integrazione consiste nell'esecuzione e nella replica dei dati
- modifica: la configurazione dell'integrazione è in fase di aggiornamento
- needs_attention — L'integrazione richiede un intervento manuale
- fallita: l'integrazione ha riscontrato un errore
- eliminazione: l'integrazione viene rimossa

Monitoraggio delle prestazioni

Monitora i seguenti aspetti delle prestazioni di integrazione zero-ETL:

- Ritardo di replica: la differenza di tempo tra il momento in cui si verifica una modifica in Oracle e il momento in cui appare in Amazon Redshift
- Throughput dei dati: il volume di dati replicati per unità di tempo
- Tassi di errore: la frequenza degli errori o degli errori di replica
- Utilizzo delle risorse: utilizzo della CPU, della memoria e della rete sui sistemi di origine e di destinazione

Usa Amazon CloudWatch per monitorare questi parametri e impostare allarmi per soglie critiche.

Gestione delle integrazioni zero-ETL in Oracle Database@AWS

Dopo aver creato un'integrazione zero-ETL, puoi eseguire varie operazioni di gestione, tra cui la modifica e l'eliminazione delle integrazioni. Questa sezione tratta la gestione continua delle integrazioni zero-ETL.

Modifica delle integrazioni Zero-ETL

È possibile modificare solo il nome, la descrizione e le opzioni di filtro dei dati per un'integrazione Zero-ETL in un data warehouse supportato. Non è possibile modificare la AWS chiave del servizio di gestione delle chiavi utilizzata per crittografare l'integrazione o i database di origine o di destinazione.

Prerequisiti per la modifica delle integrazioni

Prima di modificare un'integrazione zero-ETL, assicurati di disporre di quanto segue:

- Autorizzazioni richieste: il tuo utente o ruolo IAM deve disporre dell'`odb:UpdateOutboundIntegration`autorizzazione oltre alle autorizzazioni standard. AWS Glue
- Integrazione in stato attivo: l'integrazione deve essere in uno `ACTIVE` stato, non in`CREATING`, `MODIFYINGDELETING`, o. `FAILED`
- Sintassi valida del filtro dati: i nuovi filtri di dati devono seguire la sintassi del include/exclude modello supportata.

Modifica dei filtri di dati

È possibile modificare le tabelle o gli schemi da replicare modificando il filtro dei dati. In questo modo, è possibile aggiungere o rimuovere oggetti di database dalla replica senza ricreare l'intera integrazione.

Per modificare il filtro dati per un'integrazione, usa il `modify-integration` comando.

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

È inoltre possibile modificare contemporaneamente il nome e la descrizione dell'integrazione. Nell'esempio seguente, si modificano il nome, le descrizioni e i filtri dell'integrazione per due schemi in`pdb1`.

```
aws glue modify-integration \
  --integration-identifier integration-id \
  --data-filter "include: pdb1.schema1.*, pdb1.schema2.*" \
  --integration-name "Updated Integration Name" \
  --description "Updated integration description"
```

> **Important**
>
> Quando si modifica il filtro dati, l'integrazione entra in `modifying` uno stato ed esegue una risincronizzazione dei dati. L'integrazione interrompe la replica, applica le nuove impostazioni del filtro e riprende la replica con un'operazione reload-target. Monitora lo stato dell'integrazione per garantire che la modifica venga completata correttamente.

Considerazioni sulle modifiche del filtro dei dati alle integrazioni zero-ETL

Quando modifichi i filtri di dati, considera quanto segue:

- Limitazione PDB singola: puoi specificare un solo database collegabile (PDB) per integrazione. I filtri di dati, ad esempio, non sono supportati `include: pdb1.*.*, include: pdb2.*.*`
- Interruzione della replica: la replica dei dati si interrompe durante il processo di modifica e riprende dopo l'applicazione del nuovo filtro.

- Ricaricamento dei dati: l'integrazione esegue un ricaricamento completo dei dati che soddisfano i nuovi criteri di filtro.
- Impatto sulle prestazioni: il completamento di modifiche di grandi dimensioni al filtro dei dati potrebbe richiedere molto tempo e influire sulle prestazioni del database di origine durante il ricaricamento.

Limitazioni per le modifiche alle impostazioni di integrazione zero-ETL

Non è possibile modificare le seguenti impostazioni dopo aver creato un'integrazione zero-ETL:

- ARN segreto: il segreto di AWS Secrets Manager contenente le credenziali del database
- Chiave KMS: la chiave gestita dal cliente utilizzata per la crittografia
- ARN di origine: il cluster Oracle AWS Database@ VM
- ARN di destinazione: il cluster o lo spazio dei nomi Amazon Redshift

Per modificare queste impostazioni, elimina l'integrazione zero-ETL esistente e creane una nuova.

Eliminazione delle integrazioni Zero-ETL

Quando non è più necessaria un'integrazione zero-ETL, è possibile eliminarla per interrompere la replica e ripulire le risorse associate.

Eliminazione con AWS Glue

Eliminare un'integrazione zero-ETL utilizzando l'API AWS Glue.

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

Puoi eliminare le integrazioni nei seguenti stati:

- attiva
- necessita di attenzione
- Non riuscito
- sincronizzazione

Effetti della cancellazione

Quando eliminate un'integrazione zero-ETL, considerate i seguenti effetti:

La replica si interrompe.

Oracle Database@AWS non replica le nuove modifiche apportate da Amazon Redshift.

I dati esistenti vengono conservati.

I dati già replicati su Amazon Redshift rimangono disponibili.

Il database di destinazione rimane.

Il database Amazon Redshift creato dall'integrazione non viene eliminato automaticamente.

> **Important**
>
> L'eliminazione è irreversibile. Se è necessario riprendere la replica dopo l'eliminazione, create una nuova integrazione, che esegua un caricamento iniziale completo.

Le migliori pratiche per una gestione zero-ETL

Segui queste best practice per garantire prestazioni, sicurezza ed economicità ottimali delle tue integrazioni zero-ETL.

Best practice operative

Queste pratiche operative aiutano a mantenere integrazioni zero-ETL affidabili ed efficienti.

Monitoraggio regolare

Imposta CloudWatch allarmi per monitorare lo stato dell'integrazione e le metriche delle prestazioni.

Rotazione delle credenziali

Ruota regolarmente le password del database e aggiornale in AWS Secrets Manager.

Verifica del backup

Verifica regolarmente che i backup del database Oracle includano i componenti necessari per il disaster recovery.

Test delle prestazioni

Verifica l'impatto dell'integrazione zero-ETL sulle prestazioni del database Oracle, specialmente durante i periodi di picco di utilizzo.

Pianificazione delle modifiche allo schema

Pianifica e verifica le modifiche allo schema in un ambiente di sviluppo prima di applicarle alla produzione.

Best practice di sicurezza

Implementa queste misure di sicurezza per proteggere l'integrazione e i dati zero-ETL.

Accesso con privilegio minimo

Concedi solo le autorizzazioni minime necessarie agli utenti di replica e ai ruoli IAM. AWS

Sicurezza di rete

Utilizza i gruppi di sicurezza e NACLs limita l'accesso alla rete solo alle porte e alle fonti necessarie.

Crittografia dei dati a riposo

Assicurati che sia i database Oracle che i cluster Amazon Redshift utilizzino la crittografia a riposo.

Registrazione di controllo

Abilita la registrazione di audit sia su Oracle che su Amazon Redshift per tenere traccia dell'accesso e delle modifiche ai dati.

Gestione segreta

Usa le funzionalità di rotazione automatica di AWS Secrets Manager ove possibile.

Ottimizzazione dei costi

Applica queste strategie per ottimizzare i costi mantenendo al contempo prestazioni di integrazione zero-ETL efficaci.

Filtraggio dei dati

Utilizza filtri di dati precisi per replicare solo i dati di cui hai bisogno, riducendo i costi di storage e di elaborazione.

Ottimizzazione di Amazon Redshift

Utilizza i tipi di nodi Amazon Redshift appropriati e implementa la compressione dei dati per ottimizzare i costi.

Monitoraggio dell'utilizzo

Controlla regolarmente l'utilizzo e i costi dell'integrazione zero-ETL tramite Cost Explorer AWS .

Pulisci le integrazioni non utilizzate

Elimina le integrazioni che non sono più necessarie per evitare addebiti continui.

Risoluzione dei problemi di integrazione zero-ETL

Questa sezione fornisce indicazioni per la risoluzione di problemi comuni con l'integrazione zero-ETL.

Errori di configurazione dell'integrazione zero-ETL

Errori di autenticazione

- Verificare che l'utente di replica esista e disponga della password corretta in AWS Secrets Manager.
- Assicuratevi che tutte le autorizzazioni richieste siano state concesse all'utente di replica.
- Verifica che l'ARN segreto sia corretto e accessibile da Oracle Database@.AWS
- Verificare che la politica delle risorse CMK consenta l'accesso da parte del responsabile del servizio Oracle Database@.AWS

Eventi di connettività di rete

- Assicurati che la tua rete ODB abbia l'integrazione Zero-ETL abilitata.
- Verifica che SSL sia configurato correttamente sulla porta 2484 (solo Exadata).
- Verifica che il listener del database Oracle sia in esecuzione e accetti connessioni.
- Assicurati che la rete si raggruppi e NACLs consenta il traffico sulla porta 2484.
- Verifica che il nome del servizio nel tuo segreto corrisponda al nome di servizio Oracle effettivo.

Errori di autorizzazione

- Verifica che il tuo utente o ruolo IAM disponga delle autorizzazioni necessarie per le operazioni di AWS Glue integrazione.
- Verifica che la policy delle risorse di Amazon Redshift consenta le integrazioni in entrata dal tuo cluster di macchine virtuali.
- Assicurati che a Oracle Database@ sia AWS stato concesso l'accesso ai tuoi segreti e alla chiave del servizio di gestione delle chiavi. AWS

Problemi di replica

Errori di caricamento iniziali

- Verificare che il database Oracle disponga di risorse sufficienti per supportare l'operazione di caricamento completo.
- Assicuratevi che la registrazione supplementare sia abilitata nel database di origine.
- Verificate la presenza di eventuali blocchi o vincoli a livello di tabella che potrebbero impedire l'estrazione dei dati.

Modifica i problemi di acquisizione dei dati

- Verificate che il database Oracle disponga di spazio e conservazione adeguati per i redo log.
- Verificate che l'utente di replica abbia accesso ai redo log archiviati.
- Per i sistemi compatibili con ASM, assicuratevi che l'utente ASM sia configurato correttamente.
- Monitora le prestazioni del database Oracle per assicurarti che CDC non stia causando conflitti di risorse.

Elevato ritardo di replica

- Monitora le metriche del ritardo di replica in. CloudWatch
- Verifica la presenza di volumi di transazioni elevati o transazioni di grandi dimensioni nel database di origine.
- Verifica che il cluster Amazon Redshift abbia una capacità adeguata per gestire i dati in entrata.

Problemi di coerenza dei dati

Dati mancanti o incompleti

- Verificate che il filtro dati includa tutti gli schemi e le tabelle richiesti.

- Verifica la presenza di tipi di dati non supportati che potrebbero causare errori di replica.
- Assicurati che l'utente di replica disponga delle autorizzazioni SELECT su tutte le tabelle richieste.

Errori di conversione del tipo di dati

- Esamina le mappature dei tipi di dati supportate tra Oracle e Redshift.
- Verifica i tipi di dati specifici di Oracle che potrebbero richiedere una gestione personalizzata.
- Valuta la possibilità di modificare lo schema Oracle per utilizzare tipi di dati più compatibili.

Monitoraggio e debug

Utilizza i seguenti approcci per monitorare ed eseguire il debug dei problemi di integrazione zero-ETL:

- Monitoraggio dello stato di integrazione: verifica regolarmente lo stato dell'integrazione utilizzando. `aws glue describe-integrations`
- CloudWatch metriche: monitora le CloudWatch metriche disponibili per le prestazioni e gli errori di replica.
- Monitoraggio del database Oracle: monitora le prestazioni del database Oracle e l'utilizzo delle risorse.
- Monitoraggio Redshift: monitora le prestazioni del cluster Amazon Redshift e l'utilizzo dello storage.

Per problemi complessi che non possono essere risolti utilizzando questa guida alla risoluzione dei problemi, contatta Supporto AWS le seguenti informazioni:

- ARN di integrazione e stato attuale.
- I messaggi di errore dell'integrazione descrivono le operazioni.
- Configurazioni del database Oracle e del cluster Amazon Redshift.
- Cronologia dell'inizio del problema.

Sicurezza in Oracle Database@AWS

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS OCI e l'utente. Il modello di responsabilità condivisa lo descrive come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gira Servizi AWS nel Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi.
  Sei responsabile anche di altri fattori, tra cui la sensibilità dei tuoi dati, i requisiti della tua organizzazione e le leggi e i regolamenti applicabili.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa modello di durante l'utilizzo Oracle Database@AWS. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere Oracle Database@AWS le tue risorse.

Puoi gestire l'accesso alle tue Oracle Database@AWS risorse. Il metodo utilizzato per gestire l'accesso dipende dal tipo di attività da eseguire con Oracle Database@AWS:

- Utilizza le policy AWS Identity and Access Management (IAM) per assegnare le autorizzazioni che determinano chi è autorizzato a gestire le Oracle Database@AWS risorse. Ad esempio, puoi utilizzare IAM per determinare chi è autorizzato a creare, descrivere, modificare ed eliminare l'infrastruttura Exadata, i cluster VM o le risorse di tag.
- Utilizza le funzionalità di sicurezza del tuo motore di database Oracle per controllare chi può accedere ai database su un'istanza DB. Queste funzionalità funzionano come se il database si trovasse sulla rete locale.
- Utilizza connessioni Secure Socket Layers (SSL) o Transport Layer Security (TLS) con i database Exadata. Per ulteriori informazioni, consulta Prepare for TLS Walletless Connections.
- Oracle Database@AWS non è immediatamente accessibile da Internet e distribuito solo su sottoreti private in. AWS

- Oracle Database@AWS utilizza molte porte TCP (Transmission Control Protocol) predefinite per varie operazioni. Per l'elenco completo delle porte, consulta Assegnazioni di porte predefinite.
- Per archiviare e gestire le chiavi utilizzando Transparent Data Encryption (TDE), abilitata per impostazione predefinita, Oracle Database@AWS utilizza i vault OCI o Oracle Key Vault. Oracle Database@AWS non supporta. AWS Key Management Service
- Per impostazione predefinita, il database viene configurato utilizzando chiavi di crittografia gestite da Oracle. Il database supporta anche chiavi gestite dal cliente.
- Per migliorare la protezione dei dati, utilizza Oracle Data Safe con. Oracle Database@AWS

I seguenti argomenti mostrano come eseguire la configurazione Oracle Database@AWS per soddisfare gli obiettivi di sicurezza e conformità.

Argomenti

- Protezione dei dati in Oracle Database@AWS
- Gestione delle identità e degli accessi per Oracle Database@AWS
- Convalida della conformità per Oracle Database@AWS
- Resilienza in Oracle Database@AWS
- Utilizzo di ruoli collegati ai servizi per Oracle Database@AWS
- Oracle Database@AWS aggiornamenti alle politiche AWS gestite

Protezione dei dati in Oracle Database@AWS

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.

- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Oracle Database@AWS o altro Servizi AWS utilizzando la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Crittografia dei dati

I database Exadata utilizzano Oracle Transparent Data Encryption (TDE) per crittografare i dati. I dati sono inoltre protetti nelle tablespace temporanee, nei segmenti di annullamento, nei redo log e durante le operazioni interne del database come JOIN e SORT. Per ulteriori informazioni, consulta Data Security.

Crittografia dei dati in transito

I database Exadata utilizzano funzionalità di crittografia e integrità native di Oracle Net Services per proteggere le connessioni al database. Per ulteriori informazioni, vedere Sicurezza dei dati in transito.

Gestione delle chiavi

Transparent Data Encryption include un keystore per archiviare in modo sicuro le chiavi di crittografia principali e un framework di gestione per gestire in modo sicuro ed efficiente il keystore ed eseguire operazioni di manutenzione delle chiavi. Per ulteriori informazioni, vedere Per amministrare le chiavi di crittografia Vault.

Gestione delle identità e degli accessi per Oracle Database@AWS

AWS Identity and Access Management (IAM) è un AWS servizio che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Oracle Database@.AWS IAM è un AWS servizio che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all’amministratore se non riesci ad accedere alle funzionalità (consulta Risoluzione dei problemi di Oracle Database@AWS identità e accesso)
- Amministratore del servizio: determina l’accesso degli utenti e invia le richieste di autorizzazione (consulta Come Oracle Database@AWS funziona con IAM)
- Amministratore IAM: scrivi policy per gestire l’accesso (consulta Policy basate su identità per Oracle Database@AWS)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/

Facebook Per ulteriori informazioni sull'accesso, consulta Come accedere all' Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta Che cos'è il Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso federato degli utenti, le autorizzazioni utente IAM temporanee, l'accesso tra account, l'accesso tra servizi e le applicazioni in esecuzione su Amazon. EC2 Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e collegandole a identità o risorse. AWS Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta Politiche di controllo delle risorse (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come Oracle Database@AWS funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a Oracle Database@AWS, scopri quali funzionalità IAM sono disponibili per l'uso con Oracle Database@.AWS

Funzionalità IAM	Oracle Database@AWS supporto
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una panoramica di alto livello su come Oracle Database@AWS e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per Oracle Database@AWS

Supporta le policy basate sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che

utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Esempi di politiche basate sull'identità per Oracle Database@AWS

Per visualizzare esempi di politiche basate sull'identità di Oracle Database@AWS , vedere. Policy basate su identità per Oracle Database@AWS

Politiche basate sulle risorse all'interno Oracle Database@AWS

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per Oracle Database@AWS

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di Oracle Database@AWS azioni, vedere Actions Defined by Oracle Database@AWS nel Service Authorization Reference.

Le azioni politiche in Oracle Database@AWS uso utilizzano il seguente prefisso prima dell'azione:

```
odb
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

Per visualizzare esempi di politiche basate sull'AWS identità di Oracle Database@, vedere. Policy basate su identità per Oracle Database@AWS

Risorse politiche per Oracle Database@AWS

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di Oracle Database@AWS risorse e relativi ARNs, vedere Resources Defined by Oracle Database@AWS nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, vedere Azioni definite da Oracle Database@.AWS

Per visualizzare esempi di politiche basate sull'identità di Oracle Database@AWS , vedere. Policy basate su identità per Oracle Database@AWS

Chiavi relative alle condizioni delle policy per Oracle Database@AWS

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco di chiavi di Oracle Database@AWS condizione, consulta Condition Keys for Oracle Database@AWS nel Service Authorization Reference. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, vedere Actions Defined by Oracle Database@.AWS

Per visualizzare esempi di politiche basate sull'identità di Oracle Database@AWS , vedere. Policy basate su identità per Oracle Database@AWS

ACLs in Oracle Database@AWS

Supporti: No ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Oracle Database@AWS

Supporta ABAC (tag nelle policy): parzialmente

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Oracle Database@AWS

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono l'accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Autorizzazioni principali multiservizio per Oracle Database@AWS

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale che chiama un AWS servizio, in combinazione con il servizio richiedente per effettuare richieste ai AWS servizi a valle. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Inoltro sessioni di accesso.

Ruoli di servizio per Oracle Database@AWS

Supporta i ruoli di servizio: no

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta Creare un ruolo per delegare le autorizzazioni a un AWS servizio nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. Oracle Database@AWS Modifica i ruoli di servizio solo quando viene Oracle Database@AWS fornita una guida in tal senso.

Ruoli collegati ai servizi per Oracle Database@AWS

Supporta i ruoli collegati ai servizi: sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un servizio. AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nell'utente Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione di ruoli Oracle Database@AWS collegati ai servizi, consulta. Utilizzo di ruoli collegati ai servizi per Oracle Database@AWS

Policy basate su identità per Oracle Database@AWS

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse Oracle AWS Database@. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da Oracle Database@AWS, incluso il formato di ARNs per ogni tipo di risorsa, vedere Actions, Resources and Condition Keys for Oracle AWS Database@ nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console di Oracle Database@AWS
- Consenti agli utenti di fornire risorse Oracle Database@AWS
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse Oracle Database@ nell'account.AWS Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite un AWS servizio specifico, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consultare Best practice di sicurezza in IAM nella Guida per l'utente IAM.

Utilizzo della console di Oracle Database@AWS

Per accedere alla AWS console Oracle Database@, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentire all'utente di elencare e visualizzare i dettagli sulle risorse Oracle Database@ presenti nel computer.AWS Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime di console per gli utenti che effettuano chiamate solo verso o l'API. AWS CLI AWS Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Consenti agli utenti di fornire risorse Oracle Database@AWS

Questa politica consente agli utenti l'accesso completo alle Oracle Database@AWS risorse di fornitura. Per configurare la risoluzione DNS dal tuo VPC, crea un resolver Route 53 in uscita e aggiungi regole per inoltrare il traffico DNS con il nome di dominio OCI all'IP del listener DNS OCI.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowODBAndEC2Actions",
            "Effect": "Allow",
            "Action": [
                "odb:GetOciOnboardingStatus",
                "odb:CreateOdbNetwork",
                "odb:DeleteOdbNetwork",
                "odb:GetOdbNetwork",
                "odb:ListOdbNetworks",
                "odb:UpdateOdbNetwork",
                "odb:CreateOdbPeeringConnection",
                "odb:DeleteOdbPeeringConnection",
                "odb:GetOdbPeeringConnection",
                "odb:ListOdbPeeringConnections",
                "odb:PutResourcePolicy",
```

```
                "odb:GetResourcePolicy",
                "odb:DeleteResourcePolicy",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeVpcEndpointAssociations",
                "ec2:CreateVpcEndpoint",
                "ec2:DeleteVpcEndpoints",
                "ec2:DescribeVpcEndpoints"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowSLRActions",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "odb.amazonaws.com",
                        "vpc-lattice.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowTaggingActions",
            "Effect": "Allow",
            "Action": [
                "odb:TagResource",
                "odb:UntagResource",
                "odb:ListTagsForResource"
            ],
            "Resource": "arn:aws:odb:*:*:odb-network/*"
        },
        {
            "Sid": "AllowOdbVpcLatticeActions",
            "Effect": "Allow",
            "Action": [
                "vpc-lattice:CreateServiceNetwork",
                "vpc-lattice:DeleteServiceNetwork",
                "vpc-lattice:GetServiceNetwork",
```

```
                "vpc-lattice:CreateServiceNetworkResourceAssociation",
                "vpc-lattice:DeleteServiceNetworkResourceAssociation",
                "vpc-lattice:GetServiceNetworkResourceAssociation",
                "vpc-lattice:CreateResourceGateway",
                "vpc-lattice:DeleteResourceGateway",
                "vpc-lattice:GetResourceGateway",
                "vpc-lattice:CreateServiceNetworkVpcEndpointAssociation"
            ],
            "Resource": "*"
        }
    ]
}
```

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. 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 politiche gestite per Oracle Database@AWS

Per aggiungere autorizzazioni ai set di autorizzazioni e ai ruoli, è più semplice utilizzare le policy AWS gestite piuttosto che scrivere le policy autonomamente. La creazione di policy gestite dai clienti IAM che forniscono al team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste policy coprono i casi d'uso comuni e sono disponibili nell'account Account AWS. Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

Servizi AWS mantenere e aggiornare le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi aggiungono occasionalmente autorizzazioni aggiuntive a una policy AWS gestita per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (set di autorizzazioni e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una politica AWS gestita quando viene lanciata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non compromettono le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy `ReadOnlyAccess` AWS gestita fornisce l'accesso in sola lettura a tutte le Servizi AWS risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consultare la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

Argomenti

- AWS politica gestita: Amazon ODBService RolePolicy

AWS politica gestita: Amazon ODBService RolePolicy

Non è possibile allegare la policy `AmazonODBServiceRolePolicy` alle entità IAM. Questa politica è associata a un ruolo collegato al servizio che consente di Oracle Database@AWS eseguire azioni per tuo conto. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Oracle Database@AWS.

Per visualizzare maggiori dettagli sulla policy, inclusa l'ultima versione del documento sulla policy JSON, consulta Amazon ODBService RolePolicy nella AWS Managed Policy Reference Guide.

Oracle Database@AWS autenticazione e autorizzazione in OCI

Quando si utilizza per AWS APIs creare risorse per Oracle Database@AWS, tali risorse risiedono logicamente nella locazione collegata di Oracle Cloud Infrastructure (OCI). Per distribuire queste risorse, AWS comunica con OCI per tuo conto. APIs Per mitigare il confuso problema degli amministratori delegati, Oracle Database@AWS utilizza OCI AWS STS come entità affidabile e inoltra sessioni di accesso per autorizzare l'intenzione dell'utente di utilizzare OCI APIs nella locazione collegata. Di conseguenza, gli eventi vengono registrati per l'`sts:getCallerIdentity`API dallo spazio IP OCI nella cronologia dei AWS CloudTrail percorsi e degli eventi. Aspettatevi questi eventi quando lo utilizzate Oracle Database@AWS APIs.

Risoluzione dei problemi di Oracle Database@AWS identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Oracle AWS Database@ e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Oracle Database@AWS
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie Oracle Database@AWS risorse

Non sono autorizzato a eseguire un'azione in Oracle Database@AWS

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `odb:`*`GetWidget`* fittizie.

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

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `odb:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue policy devono essere aggiornate per consentirti di passare un ruolo a Oracle Database@AWS.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Oracle Database@.AWS Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo amministratore. AWS L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie Oracle Database@AWS risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se Oracle Database@AWS supporta queste funzionalità, vedere. Come Oracle Database@AWS funziona con IAM
- Per sapere come fornire l'accesso alle risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in Account AWS un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Convalida della conformità per Oracle Database@AWS

La responsabilità della conformità quando si utilizza Oracle Database@AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. La documentazione di Oracle sulla conformità nel cloud è disponibile sul sito Web di Oracle

Resilienza in Oracle Database@AWS

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità è possibile progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Oltre all'infrastruttura AWS globale, Oracle Database@AWS offre diverse funzionalità per supportare le esigenze di resilienza e backup dei dati.

Utilizzo di ruoli collegati ai servizi per Oracle Database@AWS

Oracle Database@AWS utilizza ruoli AWS Identity and Access Management collegati ai servizi (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. Oracle Database@AWS I ruoli collegati ai servizi sono predefiniti Oracle Database@AWS e includono tutte le autorizzazioni richieste dal servizio per chiamare altri utenti per tuo conto. Servizi AWS

Un ruolo collegato al servizio semplifica l'utilizzo Oracle Database@AWS perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Oracle Database@AWS definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. Oracle Database@AWS Le autorizzazioni definite includono la policy di trust e la policy delle autorizzazioni. Una policy delle autorizzazioni specifica non può essere collegata a un'altra entità IAM.

È possibile eliminare i ruoli solo dopo aver eliminato le risorse correlate. In questo modo proteggi Oracle Database@AWS le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Autorizzazioni di ruolo collegate al servizio per Oracle Database@AWS

Oracle Database@AWS utilizza il ruolo collegato al servizio denominato AWSService RoleFor ODB per consentire di effettuare chiamate Oracle Database@AWS Servizi AWS per conto delle risorse dell'utente.

Il ruolo collegato al servizio AWSService RoleFor ODB prevede che i seguenti servizi assumano il ruolo:

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

A questo ruolo collegato ai servizi è collegata un policy di autorizzazione denominata `AmazonODBServiceRolePolicy` che concede le autorizzazioni per operare nell'account. Per ulteriori informazioni, consulta AWS politica gestita: Amazon ODBService RolePolicy.

Note

Per consentire a un'entità IAM (ad esempio un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi, devi configurare le autorizzazioni. Se viene visualizzato il messaggio di errore seguente:
Unable to create the resource. (Impossibile creare la risorsa. Verifica di disporre dell'autorizzazione per creare un ruolo collegato al servizio. Otherwise wait and try again later. (In caso contrario, attendi e riprova più tardi.
Accertati che le seguenti autorizzazioni siano abilitate:

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

Per ulteriori informazioni, consulta le autorizzazioni dei ruoli collegati ai servizi nella Guida per l'utente IAM.

Creazione di un ruolo collegato al servizio per Oracle Database@AWS

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un database Exadata, Oracle Database@AWS crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei un database Exadata, Oracle Database@AWS crea nuovamente il ruolo collegato ai servizi per te.

Modifica di un ruolo collegato al servizio per Oracle Database@AWS

Oracle Database@AWS non consente di modificare il ruolo collegato al servizio AWSService RoleFor ODB. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché

varie entità potrebbero farvi riferimento. Tuttavia, puoi modificare la descrizione del ruolo utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente IAM.

Eliminazione di un ruolo collegato al servizio per Oracle Database@AWS

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare quel ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario eliminare tutte le risorse prima di poter eliminare il ruolo collegato al servizio.

Pulizia di un ruolo collegato al servizio per Oracle Database@AWS

Prima di utilizzare IAM per eliminare un ruolo collegato ai servizi, devi innanzitutto verificare che il ruolo non abbia sessioni attive ed eliminare tutte le risorse utilizzate dal ruolo.

Per verificare se il ruolo collegato ai servizi dispone di una sessione attiva nella console IAM

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo. https://console.aws.amazon.com/iam/
2. Nel pannello di navigazione della console IAM seleziona Ruoli. Quindi scegli il nome (non la casella di controllo) del ruolo AWSService RoleFor ODB.
3. Nella pagina Summary (Riepilogo) per il ruolo selezionato, scegli la scheda Access Advisor (Consulente accessi).
4. Nella scheda Access Advisor (Consulente accessi), esamina l'attività recente per il ruolo collegato ai servizi.

> **Note**
>
> Se non sei sicuro che Oracle Database@AWS stia utilizzando il ruolo AWSService RoleFor ODB, puoi provare a eliminare il ruolo. Se il servizio utilizza il ruolo, l'eliminazione non riesce e puoi visualizzare Regioni AWS dove viene utilizzato il ruolo. Se il ruolo è in uso, prima di poterlo eliminare dovrai attendere il termine della sessione. Non puoi revocare la sessione per un ruolo collegato al servizio.

Se desideri rimuovere il ruolo AWSService RoleFor ODB, devi prima eliminare tutte le tue Oracle Database@AWS risorse.

Regioni supportate per i ruoli collegati Oracle Database@AWS ai servizi

Oracle Database@AWS supporta l'utilizzo di ruoli collegati al servizio in tutti i paesi in Regioni AWS cui il servizio è disponibile. Per ulteriori informazioni, consulta Regioni AWS ed endpoint.

Oracle Database@AWS aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite Oracle Database@AWS da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei Oracle Database@AWS documenti.

Modifica	Descrizione	Data
Autorizzazioni di ruolo collegate al servizio per Oracle Database@AWS: aggiornamento a policy esistente	Oracle Database@AWS ha aggiunto nuove autorizzazioni al ruolo collegato al `AmazonODB ServiceRolePolicy` `AWSServic eRoleForODB` servizio. Queste autorizzazioni consentono Oracle Database@AWS di effettuare le seguenti operazioni: • Descrivi gli allegati di Amazon VPC Transit Gateways • Descrivi EC2 gli allegati Amazon • Attiva una EventBridge fonte Amazon Per ulteriori informazioni, consulta Autorizzazioni di ruolo collegate al servizio per Oracle Database@AWS.	30 giugno 2025
Autorizzazioni di ruolo collegate al servizio per Oracle Database@AWS: aggiornamento a policy esistente	Oracle Database@AWS ha aggiunto nuove autorizzazioni al ruolo `AmazonODBServiceRo lePolicy` collegato al `AWSServiceRoleFor0 DB` servizio. Queste autorizzazioni consentono Oracle Database@AWS di effettuare le seguenti operazioni:	26 giugno 2025

Modifica	Descrizione	Data
	• Descrivi una EventBridge fonte Amazon • Descrivi e crea un bus per eventi Per ulteriori informazioni, consulta Autorizzazioni di ruolo collegate al servizio per Oracle Database@AWS.	
AWS politica gestita: Amazon ODBService RolePolicy— Nuova politica relativa ai ruoli legati ai servizi	Oracle Database@AWS ha aggiunto il ruolo `AmazonODBServiceRolePolicy` per il ruolo collegato al `AWSServiceRoleForODB` servizio. Per ulteriori informazioni, consulta AWS politica gestita: Amazon ODBService RolePolicy.	2 dicembre 2024
Oracle Database@AWS ha iniziato a tenere traccia delle modifiche	Oracle Database@AWS ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	2 dicembre 2024

Monitoraggio di Oracle Database@AWS

Il monitoraggio è una parte importante del mantenimento dell'affidabilità, della disponibilità Oracle Database@AWS e delle prestazioni delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per osservare Oracle Database@AWS, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. È possibile raccogliere e tenere traccia dei parametri, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi tenere CloudWatch traccia dell'utilizzo della CPU o di altri parametri delle tue EC2 istanze Amazon e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.
- Amazon CloudWatch Logs ti consente di monitorare, archiviare e accedere ai tuoi file di registro da EC2 istanze Amazon e altre fonti. CloudTrail CloudWatch I log possono monitorare le informazioni nei file di registro e avvisarti quando vengono raggiunte determinate soglie. Puoi inoltre archiviare i dati del log in storage estremamente durevole. Per ulteriori informazioni, consulta la Amazon CloudWatch Logs User Guide.
- Amazon EventBridge può essere utilizzato per automatizzare AWS i tuoi servizi e rispondere automaticamente agli eventi di sistema, come problemi di disponibilità delle applicazioni o modifiche delle risorse. Gli eventi AWS relativi ai servizi vengono forniti quasi EventBridge in tempo reale. Puoi compilare regole semplici che indichino quali eventi sono considerati di interesse per te e quali operazioni automatizzate intraprendere quando un evento corrisponde a una regola. Per ulteriori informazioni, consulta Amazon EventBridge User Guide.
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail.

Monitoraggio Oracle Database@AWS con Amazon CloudWatch

È possibile monitorare Oracle Database@AWS l'utilizzo CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili e quasi in tempo reale. Queste statistiche vengono conservate per

un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

CloudWatch Metriche Amazon per Oracle Database@AWS

Il Oracle Database@AWS servizio riporta i parametri ad Amazon CloudWatch nello spazio dei `AWS/ODB` nomi per cluster di macchine virtuali, database container e database collegabili.

Argomenti

Metriche per i cluster di macchine virtuali cloud

Il Oracle Database@AWS servizio riporta le seguenti metriche nel `AWS/ODB` namespace per i cluster di macchine virtuali cloud.

Metrica	Description	unità
`ASMDiskgroupUtilization`	La percentuale di spazio utilizzabile utilizzato in un gruppo di dischi. Lo spazio utilizzabile è lo spazio disponibile per la crescita. Il gruppo di dischi DATA archivia i file del nostro database Oracle. Il gruppo di dischi RECO contiene file di database per il ripristino, come archivi e registri di flashback.	Percentuale
`CpuUtilization`	La percentuale di utilizzo della CPU.	Percentuale

Metrica	Description	unità
`FilesystemUtilization`	La percentuale di utilizzo del file system di cui è stato effettuato il provisioning.	Percentuale
`LoadAverage`	La media di carico del sistema nell'arco di 5 minuti.	Numero intero
`MemoryUtilization`	La percentuale di memoria disponibile per l'avvio di nuove applicazioni, senza scambio. La memoria disponibile può essere ottenuta tramite il seguente comando: `cat /proc/meminfo`	Percentuale
`NodeStatus`	Indica se l'host è raggiungibile.	Numero intero
`OcpusAllocated`	Il numero di OCPUs risorse allocate.	Numero intero
`SwapUtilization`	La percentuale di utilizzo dello spazio di swap totale.	Percentuale

Metriche per i database dei container

Il Oracle Database@AWS servizio riporta le seguenti metriche nello spazio dei `AWS/ODB` nomi per i database dei contenitori.

Metrica	Description	unità
`BlockChanges`	Il numero medio di blocchi modificati al secondo.	Modifiche al secondo
`CpuUtilization`	L'utilizzo della CPU espresso in percentuale, aggregato per tutti i gruppi di consumatori.	Percentuale

Metrica	Description	unità
	Viene riportata la percentuale di utilizzo rispetto al numero di CPUs database che è consentito utilizzare, ovvero due volte il numero di. OCPUs	
`CurrentLogons`	Il numero di accessi riusciti durante l'intervallo selezionato.	Conteggio
`ExecuteCount`	Il numero di chiamate utente e ricorsive che hanno eseguito istruzioni SQL durante l'interva llo selezionato.	Conteggio
`ParseCount`	Il numero di analisi rigide e software durante l'intervallo selezionato.	Conteggio
`StorageAllocated`	Quantità totale di spazio di archiviazione allocato al database al momento della raccolta.	GB
`StorageAllocatedBy Tablespace`	Quantità totale di spazio di archiviazione allocato alla tablespace al momento della raccolta. Nel caso del database contenitore, questa metrica fornisce i tablespace del contenitore principale.	GB
`StorageUsed`	Quantità totale di spazio di archiviazione utilizzato dal database al momento della raccolta.	GB

Metrica	Description	unità
`StorageUsedByTablespace`	Quantità totale di spazio di archiviazione utilizzato da tablespace al momento della raccolta. Nel caso del database contenitore, questa metrica fornisce i tablespace del contenitore principale.	GB
`StorageUtilization`	La percentuale della capacità di storage assegnata attualmente in uso. Rappresenta lo spazio totale allocato per tutte le tablespace.	Percentuale
`StorageUtilizationByTablespace`	Indica la percentuale di spazio di archiviazione utilizzata dal tablespace al momento della raccolta. Nel caso del database contenitore, questa metrica fornisce i tablespace del contenitore principale.	Percentuale
`TransactionCount`	Il numero combinato di commit e rollback degli utenti durante l'intervallo selezionato.	Conteggio
`UserCalls`	Il numero combinato di accessi, analisi ed esecuzione di chiamate durante l'intervallo selezionato.	Conteggio

Metriche per database collegabili

Il Oracle Database@AWS servizio riporta le seguenti metriche nello spazio dei `AWS/ODB` nomi per i database collegabili.

Metrica	Description	unità
`AllocatedStorageUtilizationByTablespace`	La percentuale di spazio utilizzata dal tablespace, rispetto a tutto lo spazio allocato. Per i database container, questa metrica fornisce i dati per i tablespace del contenitore principale. (Statistica: media, intervallo: 30 minuti)	Percentuale
`AvgGCCRBlockReceiveTime`	Il tempo medio di ricezione del blocco CR (consistent-read) della cache globale. Solo per database RAC/cluster. (Statistica: media, intervallo: 5 minuti)	Millisecondi
`AvgGCCurrentBlockReceiveTime`	Il tempo medio di ricezione dei blocchi correnti della cache globale. La statistica riporta il valore medio. Solo per database Real Application Cluster (RAC). (Statistica: media, intervallo: 5 minuti)	Millisecondi
`BlockChanges`	Il numero medio di blocchi modificati al secondo. (Statistica: media, intervallo: 1 minuto)	modifiche al secondo
`BlockingSessions`	Sessioni di blocco correnti. Non applicabile ai database dei contenitori. (Statistica: massimo, intervallo: 15 minuti)	Conteggio
`CPUTimeSeconds`	Il tasso medio di accumulo del tempo di CPU per sessioni in primo piano nell'istanza	Secondi al secondo

Metrica	Description	unità
	del database nell'intervallo di tempo. Il componente del tempo di CPU di Average Active Sessions. (Statistica: media, intervallo: 1 minuto)	
`CpuCount`	Il numero di CPUs durante l'intervallo selezionato.	Conteggio
`CpuUtilization`	L'utilizzo della CPU espresso in percentuale, aggregato tra tutti i gruppi di consumatori. Viene riportata la percentuale di utilizzo rispetto al numero di CPUs database che è consentito utilizzare, ovvero due volte il numero di. OCPUs (Statistica: media, intervallo: 1 minuto)	Percentuale
`CurrentLogons`	Il numero di accessi riusciti durante l'intervallo selezionato. (Statistiche: somma, intervallo: 1 minuto)	Conteggio
`DBTimeSeconds`	Il tasso medio di accumulo del tempo del database (CPU + attesa) per sessioni in primo piano nell'istanza del database nell'intervallo di tempo. Conosciute anche come sessioni attive medie. (Statistica: media, intervallo: 1 minuto)	Secondi al secondo

Metrica	Description	unità
`DbmgmtJobExecutionsCount`	Il numero di esecuzioni di job SQL su un singolo database gestito o su un gruppo di database e il relativo stato. Le dimensioni dello stato possono essere i seguenti valori: «Riuscito», «Non riuscito» , "InProgress».» (Statistica: somma, intervallo: 1 minuto)	Conteggio
`ExecuteCount`	Il numero di chiamate utente e ricorsive che hanno eseguito istruzioni SQL durante l'intervallo selezionato. (Statistica: somma, intervallo: 1 minuto)	Conteggio
`FRASpaceLimit`	Il limite di spazio nell'area di ripristino flash. Non applicabile ai database collegabili. (Statistica: massimo, intervallo: 15 minuti)	GB
`FRAUtilization`	L'utilizzo dell'area di ripristino flash. Non applicabile ai database collegabili. (Statistica: media, intervallo: 15 minuti)	Percentuale
`GCCRBlocksReceived`	I blocchi CR (consistent-read) della cache globale ricevuti al secondo. Solo per database RAC/cluster. (Statistica: media, intervallo: 5 minuti)	Blocchi al secondo

Metrica	Description	unità
`GCCurrentBlocksReceived`	Rappresenta i blocchi correnti della cache globale ricevuti al secondo. La statistica riporta il valore medio. Solo per database Real Application Cluster (RAC). (Statistica: media, intervallo: 5 minuti)	Blocchi al secondo
`IOPS`	Il numero medio di operazioni di input-output al secondo. (Statistica: media, intervallo: 1 minuto)	Operazioni al secondo
`IOThroughputMB`	La velocità media in MB al secondo. (Statistica: media, intervallo: 1 minuto)	MB al secondo
`InterconnectTrafficMB`	La velocità media di trasferimento dati tra nodi. Solo per database RAC/cluster. (Statistica: media, intervallo: 5 minuti)	MB al secondo
`InvalidObjects`	Numero di oggetti di database non validi. Non applicabile ai database container. (Statistica: massimo, intervallo: 24 ore)	Conteggio
`LogicalBlocksRead`	Il numero medio di blocchi letti da SGA/Memory (buffer cache) al secondo. (Statistica: media, intervallo: 1 minuto)	Letture al secondo

Metrica	Description	unità
`MaxTablespaceSize`	La dimensione massima possibile del tablespace. Per i database container, questa metrica fornisce i dati per i tablespace del contenito re principale. (Statistica: massimo, intervallo: 30 minuti)	GB
`MemoryUsage`	Dimensione totale del pool di memoria in MB. (Statistica: media, intervallo: 15 minuti)	MB
`MonitoringStatus`	Lo stato di monitoraggio della risorsa. Se una raccolta di metriche fallisce, le informazi oni sull'errore vengono acquisite in questa metrica. (Statistica: media, intervallo: 5 minuti)	Non applicabile
`NonReclaimableFRA`	L'area di recupero rapido non recuperabile. Non applicabi le ai database collegabili. (Statistica: media, intervallo: 15 minuti)	Percentuale
`OcpusAllocated`	Il numero effettivo di OCPUs risorse allocate dal servizio durante l'intervallo di tempo selezionato. (Statistica: conteggio, intervallo: 1 minuto)	Numero intero
`ParseCount`	Il numero di analisi rigide e morbide durante l'interva llo selezionato. (Statistica: somma, intervallo: 1 minuto)	Conteggio

Metrica	Description	unità
ParsesByType	Il numero di analisi rigide o morbide al secondo. (Statistica: media, intervallo: 1 minuto)	Analisi al secondo
ProblematicScheduledDBMSJobs	I job pianificati problematici del database contano. Non applicabile ai database container. (Statistica: massimo, intervallo: 15 minuti)	Conteggio
ProcessLimitUtilization	Il processo limita l'utilizzo. Non applicabile ai database collegabili. (Statistica: media, intervallo: 1 minuto)	Percentuale
Processes	I processi del database contano. Non applicabile ai database collegabili. (Statistica: massimo, intervallo: 1 minuto)	Conteggio
ReclaimableFRA	L'area di recupero rapido recuperabile. Non applicabile ai database collegabili. (Statistica: media, intervallo: 15 minuti)	Percentuale
ReclaimableFRASpace	Spazio recuperabile dell'area di ripristino flash. Non applicabile ai database collegabili. (Statistica: media, intervallo: 15 minuti)	GB

Metrica	Description	unità
`RedoSizeMB`	La quantità media di ripristino generata, in MB al secondo. (Statistica: media, intervallo: 1 minuto)	MB al secondo
`SessionLimitUtilization`	L'utilizzo del limite di sessione. Non applicabile ai database collegabili. (Statistica: media, intervallo: 1 minuto)	Percentuale
`Sessions`	Il numero di sessioni nel database. (Statistica: media, intervallo: 1 minuto)	Conteggio
`StorageAllocated`	La quantità massima di spazio allocata dal tablespace durante l'intervallo. Per i database container, questa metrica fornisce i dati per i tablespace del contenitore principale. (Statistica: massimo, intervallo: 30 minuti)	GB
`StorageAllocatedByTablespace`	La quantità massima di spazio allocata per tablespace durante l'intervallo. Per i database container, questa metrica fornisce i dati per i tablespace del contenitore principale. (Statistica: massimo, intervallo: 30 minuti)	GB
`StorageUsed`	La quantità massima di spazio utilizzata durante l'intervallo. (Statistica: massimo, intervallo: 30 minuti)	GB

Metrica	Description	unità
`StorageUsedByTablespace`	La quantità massima di spazio utilizzata dal tablespace durante l'intervallo. Per i database container, questa metrica fornisce i dati per i tablespace del contenitore principale. (Statistica: massimo, intervallo: 30 minuti)	GB
`StorageUtilization`	La percentuale di capacità di storage assegnata attualmente in uso. Rappresenta lo spazio totale allocato per tutte le tablespace. (Statistica: media, intervallo: 30 minuti)	Percentuale
`StorageUtilizationByTablespace`	La percentuale di spazio utilizzato, per tablespace. Per i database container, questa metrica fornisce i dati per i tablespace container root. (Statistica: media, intervallo: 30 minuti)	Percentuale
`TransactionCount`	Il numero combinato di commit e rollback degli utenti durante l'intervallo selezionato. (Statistica: somma, intervallo: 1 minuto)	Conteggio
`TransactionsByStatus`	Il numero di transazioni confermate o ripristinate al secondo. (Statistica: media, intervallo: 1 minuto)	Transazioni al secondo

Metrica	Description	unità
`UnusableIndexes`	Gli indici inutilizzabili contano nello schema del database. Non applicabile ai database container. (Statistica: massimo, intervallo: 24 ore)	Conteggio
`UsableFRA`	L'area di recupero rapido utilizzabile. Non applicabi le ai database collegabili. (Statistica: media, intervallo: 15 minuti)	Percentuale
`UsedFRASpace`	L'utilizzo dello spazio nell'area di ripristino flash. Non applicabile ai database collegabili. (Statistica: massimo, intervallo: 15 minuti)	GB
`UserCalls`	Il numero combinato di accessi, analisi ed esecuzion e di chiamate durante l'interva llo selezionato. (Statistica: somma, intervallo: 1 minuto)	Conteggio
`WaitTimeSeconds`	Il tasso medio di accumulo del tempo di attesa non inattivo per sessioni in primo piano nell'istanza del database nell'intervallo di tempo. Il componente del tempo di attesa di Average Active Sessions. (Statistica: media, intervallo: 5 minuti)	Secondi al secondo

CloudWatch Dimensioni Amazon per Oracle Database@AWS

Puoi filtrare i dati Oracle Database@AWS delle metriche utilizzando qualsiasi dimensione nella tabella seguente.

Dimensione	Filtra i dati richiesti per...
`cloudVmClusterId`	L'identificatore di un cluster di macchine virtuali.
`cloudExadataInfrastructureId`	L'identificatore dell'infrastruttura Exadata.
`collectionName`	Il nome di una collezione.
`deploymentType`	Il tipo di infrastruttura.
`diskgroupName`	Il nome di un gruppo di dischi
`errorCode`	Un codice di errore.
`errorSeverity`	La gravità di un errore.
`filesystemName`	Il nome di un file system.
`hostName`	Il nome del computer host.
`instanceName`	Il nome di un'istanza di database.
`instanceNumber`	Il numero di istanza di un'istanza di database.
`ioType`	Un tipo di I/O operazione.
`jobId`	Un identificatore univoco per un lavoro.
`managedDatabaseGroupId`	L'identificatore di un. Managed Database Group
`managedDatabaseId`	L'identificatore di un. Managed Database
`memoryPool`	Un tipo di pool di memoria.

Dimensione	Filtra i dati richiesti per...
memoryType	Un tipo di memoria.
ociCloudVmClusterId	L'identificatore OCI di un cluster VM.
ociCloudExadataInfrastructureId	L'identificatore OCI dell'infrastruttura Exadata.
parseType	Un tipo di analisi.
resourceId	L'identificatore di una risorsa.
resourceId_Database	L'identificatore di un database.
resourceId_DbNode	L'identificatore di un nodo del database.
resourceName	Il nome di una risorsa.
resourceName_Database	Il nome di un database.
resourceName_DbNode	Il nome di un nodo del database.
resourceType	Un tipo di database.
schemaName	Il nome di uno schema.
status	Lo stato di un database.
tablespaceContents	Il contenuto di un tablespace.
tablespaceName	Il nome di un tablespace.
tablespaceType	Un tipo di tablespace.
transactionStatus	Lo stato di una transazione.
waitClass	Una classe di eventi di attesa.

Monitoraggio Oracle Database@AWS degli eventi in Amazon EventBridge

È possibile monitorare Oracle Database@AWS gli eventi in EventBridge, che fornisce un flusso di dati in tempo reale da applicazioni e AWS servizi. EventBridge indirizza questi dati verso obiettivi come Amazon AWS Lambda Simple Notification Service.

> **Note**
>
> EventBridge in precedenza si chiamava Amazon CloudWatch Events. Per ulteriori informazioni, EventBridge consulta l'evoluzione di Amazon CloudWatch Events nella Amazon EventBridge User Guide.

Panoramica degli Oracle Database@AWS eventi

Oracle Database@AWS gli eventi sono messaggi strutturati che indicano cambiamenti nei cicli di vita delle risorse. Un bus di eventi è un router che riceve eventi e li consegna a zero o più destinazioni o destinazioni. Oracle Database@AWS gli eventi possono essere generati dalle seguenti fonti:

Eventi da AWS

: Questi eventi vengono Oracle Database@AWS APIs generati AWS lateralmente e vengono inviati al bus eventi predefinito del tuo Account AWS.

Eventi di OCI

: Questi eventi vengono generati direttamente da OCI, come gli eventi relativi all'infrastruttura Oracle Exadata o ai cluster VM. Quando ti iscrivi Oracle Database@AWS, `aws.partner/odb/` viene creato un bus di eventi con prefisso Account AWS per ricevere eventi da OCI.

Oracle Database@AWS eventi da AWS

Oracle Database@AWS gli eventi di AWS includono le modifiche al ciclo di vita relative alla rete ODB durante la creazione e l'eliminazione. Questi eventi vengono inviati al bus eventi predefinito di. Account AWS Il tipo di consegna è la soluzione migliore.

Eventi di rete ODB

Event	ID evento	Messaggio
Creazione	ODB-EVENT-0001	Rete ODB ODBnet_ID creata con successo
Creazione non riuscita	ODB-EVENT-0011	Impossibile creare la rete ODB ODBnet_ID
Eliminazione	ODB-EVENT-0002	Rete ODB ODBnet_ID eliminata con successo
Eliminazione non riuscita	ODB-EVENT-0012	Impossibile eliminare ODBnet_ID dalla rete ODB

Esempio: evento di creazione della rete ODB

L'esempio seguente mostra un evento relativo alla corretta creazione di una rete 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 eventi di OCI

La maggior parte degli eventi viene generata direttamente da OCI. Oracle Database@AWS crea un bus di eventi con prefisso `aws.partner/odb/` nel tuo Account AWS per ricevere eventi da OCI. Si consiglia di non eliminare questo bus di eventi.

OCI offre tipi di eventi completi, inclusi i seguenti:

- Infrastruttura Oracle Exadata
- Eventi del cluster VM
- Eventi CDB
- Eventi PDB

Per ulteriori informazioni sui tipi di eventi specifici e sui dettagli supportati da OCI, vedere Oracle Exadata Database Service on Dedicated Infrastructure Events and Events for Autonomous Database on Dedicated Exadata Infrastructure.

Filtraggio degli eventi Oracle Database@AWS

Puoi seguire le best practice EventBridge suggerite per la configurazione del bus degli eventi su Event bus in Amazon EventBridge. A seconda dei casi d'uso, puoi impostare EventBridge regole per filtrare eventi e obiettivi per ricevere e utilizzare gli eventi.

Filtraggio degli eventi di rete ODB da AWS

Per gli eventi di rete ODB da AWS, è possibile filtrare utilizzando il seguente schema di eventi:

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

È possibile applicare questo modello utilizzando l' EventBridge `put-rule`API con il bus di eventi predefinito. Per ulteriori informazioni, PutRuleconsulta Amazon EventBridge API Reference.

Filtraggio Oracle Database@AWS degli eventi da OCI

Per Oracle Database@AWS gli eventi di OCI, puoi configurare una regola utilizzando un comando simile all'esempio PutRulein Amazon EventBridge API Reference. Tieni presente le seguenti linee guida:

- Utilizza uno schema di eventi personalizzato a seconda dei tipi di eventi che desideri filtrare.
- EventBusNameImposta sul nome del bus che Oracle Database@AWS ha creato.

Per ulteriori informazioni su come filtrare gli eventi e impostare gli EventBridge obiettivi tra gli account, consulta Invio e ricezione di eventi tra Account AWS Amazon EventBridge.

Risoluzione dei problemi Oracle Database@AWS degli eventi

Se riscontri un problema con la consegna o il contenuto dell'evento, procedi come segue:

- Per gli eventi della rete ODB, contatta Supporto AWS.
- Per Oracle Database@AWS eventi diversi dagli eventi di rete ODB, contatta Oracle Cloud Support.

Per ulteriori informazioni, consulta Ottenere supporto per Oracle Database@AWS.

Registrazione delle chiamate Oracle Database@AWS API utilizzando AWS CloudTrail

Oracle Database@AWS è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o un Servizio AWS. CloudTrail acquisisce tutte le chiamate API Oracle Database@AWS come eventi. Le chiamate acquisite includono chiamate dalla Oracle Database@AWS console e chiamate di codice alle operazioni Oracle Database@AWS API. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare a quale richiesta è stata effettuata Oracle Database@AWS, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e ulteriori dettagli.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente.
- Se la richiesta è stata effettuata per conto di un utente del Centro identità IAM.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

> **Note**
>
> Oracle Database@AWS registra le chiamate `GetCallerIdentity` API da AWS Security Token Service (STS) nei tuoi CloudTrail log. Queste chiamate API STS verificano l'identità di Oracle Database@AWS quando interagisci con OCI per tuo conto. Sono una parte normale e sicura delle AWS operazioni e non espongono informazioni sensibili.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWSPer ulteriori informazioni, consulta Lavorare con la cronologia degli CloudTrail eventi nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi CloudTrailLake.

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il Console di gestione AWS sono multiregionali. È possibile creare un trail per una singola Regione o per più Regioni tramite AWS CLI. La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio Regioni AWS account. Se si crea un trail per una singola Regione, è possibile visualizzare solo gli eventi registrati nella Regione AWS del trail. Per ulteriori informazioni sui trail, consulta Creating a trail for your Account AWS e Creating a trail for an organization nella Guida per l'utente di AWS CloudTrail .

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail Per informazioni sui prezzi di Amazon S3, consulta Prezzi di Amazon S3.

CloudTrail Archivi di dati sugli eventi di Lake

CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi eventi. CloudTrail Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC. ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i selettori di eventi avanzati. I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su CloudTrail Lake, consulta Working with AWS CloudTrail Lake nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di

conservazione predefinito e quello massimo per il datastore di eventi. Per ulteriori informazioni sui CloudTrail prezzi, consulta Prezzi.AWS CloudTrail

Oracle Database@AWS eventi gestionali in CloudTrail

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse di Account AWS. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

Oracle Database@AWS registra tutte le operazioni Oracle Database@AWS del piano di controllo come eventi di gestione.

Oracle Database@AWS esempi di eventi

Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'operazione API richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi gli eventi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra un CloudTrail evento che dimostra l'`CreateOdbNetwork`operazione.


```
{
    "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"
    }
}
```


Per informazioni sul contenuto dei CloudTrail record, consultate il contenuto dei CloudTrail record nella Guida per l'AWS CloudTrail utente.

Risoluzione dei problemi con Oracle Database@AWS

Utilizza le seguenti sezioni per aiutarti a risolvere i problemi di rete che potresti riscontrare. Oracle Database@AWS

Argomenti

La creazione della rete ODB non riesce

Quando non è possibile creare una rete ODB, le cause più comuni sono le seguenti:

Intervalli CIDR limitati

La rete ODB utilizza intervalli CIDR specifici per le sottoreti client e di backup. Assicurati che gli intervalli CIDR che hai scelto per queste sottoreti non si sovrappongano a intervalli di indirizzi IP riservati o riservati.

I seguenti intervalli CIDR sono riservati e non possono essere utilizzati per la rete ODB:

- Intervallo riservato Oracle Cloud: 169.254.0.0/16
- Classe riservata D: 224.0.0.0 - 239.255.255.255
- Classe riservata E: 240.0.0.0 - 255.255.255.255
- Uso futuro dell'OCI: 100.105.0.0/16

Segui le EC2 regole per gli intervalli CIDR come indicato nella documentazione VPC. Per ulteriori informazioni, consulta Restrizioni CIDR sulle associazioni di blocchi.

Inoltre, evita la sovrapposizione tra gli intervalli CIDR specificati e quelli utilizzati per la connettività VPC alla rete ODB.

VPC CIDR sovrapposto

L'intervallo CIDR che hai specificato per la rete ODB non deve sovrapporsi agli intervalli CIDR utilizzati da nessuno dei tuoi esistenti. VPCs La sovrapposizione degli intervalli CIDR può causare

conflitti di routing e impedire la corretta creazione della rete ODB. Controlla gli intervalli CIDR del peering ODB VPCs e assicurati che il CIDR della rete ODB sia unico e non si sovrapponga.

Proprietà di VPCs

La rete ODB e il VPC a cui ti stai connettendo devono appartenere allo AWS stesso account. Se stai cercando di collegare la rete ODB a un VPC di proprietà di un altro account, la creazione avrà esito negativo. Verifica che la rete ODB e il VPC siano entrambi di proprietà dello stesso account. AWS

Mancanza di un gateway di transito

Se aggiungi un intervallo CIDR all'elenco CIDR peered della rete ODB senza collegare un gateway di transito al VPC, l'operazione di creazione o aggiornamento non riesce. Non vi è alcun requisito sugli intervalli CIDR per cui viene utilizzato l'allegato.

Problemi di connettività tra la rete VPC e ODB o i cluster VM

Quando non riesci a connetterti dal tuo VPC alla rete ODB o ai cluster di VM al suo interno, le seguenti sono le cause più comuni:

- Verifica della configurazione del VPC: nella Oracle Database@AWS console, individua il VPC collegato alla rete ODB. Verifica che l'ID VPC corrisponda a quello mostrato nei dettagli della rete ODB.
- Ispezione delle tabelle di routing: nella console Amazon VPC, trova la tabella di routing collegata alla sottorete in cui è in esecuzione l'applicazione. Verifica la presenza di una route con un CIDR di destinazione che corrisponda alla sottorete client CIDR della rete ODB. Verifica che questo percorso punti all'ARN della rete ODB corretto. Se manca la route, aggiungine una nuova alla sottorete client CIDR della rete ODB.
- Convalida peered CIDRs: consulta la `Peered CIDRs` sezione nei dettagli della rete ODB. Verifica che tutti i blocchi CIDR pertinenti del tuo VPC siano elencati. Se manca un CIDR richiesto, aggiorna il file peered. CIDRs
- Verifica delle regole dei gruppi di sicurezza: nella EC2 console Amazon, individua i gruppi di sicurezza per le risorse nel tuo VPC. Rivedi le regole in entrata e in uscita, aggiornandole se necessario per consentire il traffico necessario.
- Conferma delle zone di disponibilità: nella console Amazon VPC, identifica la zona di disponibilità (AZ) della tua sottorete. Verifica che anche la rete ODB sia distribuita nella stessa zona di distribuzione della sottorete.

- Evitare più connessioni peering di rete ODB: controlla le connessioni peering VPC nella console. Oracle Database@AWS Assicurati di avere solo una connessione attiva a una rete ODB. Se vedi più di un peering di rete ODB, rimuovi quelli aggiuntivi.

Nomi host o nomi di scansione irrisolvibili di cluster VM da VPC

Se i nomi host o i nomi di scansione dei cluster VM non sono risolvibili dal tuo VPC, configura l'inoltro DNS sul VPC e le seguenti risorse per risolvere i record DNS ospitati sulla rete ODB:

- Un endpoint in uscita per inviare query DNS alla rete ODB. Per ulteriori informazioni, consulta Configurazione di un endpoint in uscita in una rete ODB in Oracle Database@AWS.
- Una regola del resolver per specificare il nome di dominio delle query DNS che il resolver inoltra alla rete DNS per ODB. Per ulteriori informazioni, consulta Configurazione di una regola del resolver in Oracle Database@AWS.

Ottenere supporto per Oracle Database@AWS

Scopri come ottenere informazioni e supporto per Oracle Database@AWS.

Ambito e informazioni di contatto del supporto Oracle

Oracle Cloud Support è la prima linea di supporto per tutte le domande su Oracle Database@AWS . Per contattare l'assistenza, accedi alla console di Oracle Cloud Infrastructure (OCI), quindi seleziona l'icona della zattera di salvataggio. Se non disponi di un account My Oracle Cloud Support, consultaI miei account e accesso a Oracle Cloud Support.

Di seguito sono riportati alcuni esempi di problemi che Oracle Support può risolvere:

- Problemi di connessione al database (Oracle TNS)
- Problemi di prestazioni del database Oracle
- Risoluzione degli errori del database Oracle
- Problemi di rete relativi alle comunicazioni con la tenancy OCI associata al servizio
- La quota (limiti) aumenta per ricevere più capacità (per ulteriori informazioni, vedere Richiesta di un aumento del limite per le risorse del database)
- Scalabilità per aggiungere maggiore capacità di elaborazione e storage all'infrastruttura di database Oracle

- Aggiornamenti hardware di nuova generazione
- Problemi di fatturazione relativi agli addebiti Marketplace AWS

Se devi contattare il supporto Oracle al di fuori della console OCI, comunica all'agente di Oracle Support che il problema è correlato a Oracle Database@AWS. Questo perché le richieste di questo servizio vengono gestite da un team di supporto OCI specializzato in queste implementazioni.

Contattare l'assistenza Oracle per telefono

1. Chiama il numero 1-800-223-1711. Se non risiedi negli Stati Uniti d'America, visita l'Oracle Support Contacts Global Directory per trovare le informazioni di contatto per il tuo paese o la tua area geografica.
2. Scegli l'opzione «2" per aprire una nuova Service Request (SR).
3. Scegli l'opzione «4" per «non essere sicuro».
4. Fai sapere all'agente che hai un problema con il tuo sistema multicloud e il nome del prodotto. Verrà aperta una richiesta di assistenza interna per tuo conto e un tecnico di supporto OCI ti contatterà direttamente.

Puoi anche inviare una domanda al forum Multicloud nella community Cloud Customer Connect di Oracle. Questa opzione è disponibile per tutti i clienti.

I miei account e accesso a Oracle Cloud Support

Per creare i ticket di richiesta del servizio My Oracle Cloud Support, l'amministratore del AWS servizio Oracle Database@ dell'organizzazione deve approvare la richiesta. Se sei l'AWS amministratore di Oracle Database@, completa le istruzioni di onboarding di My Oracle Cloud Support incluse nell'e-mail di attivazione del servizio Oracle Database@.AWS

Puoi trovare le istruzioni per l'onboarding con My Oracle Cloud Support nei seguenti argomenti:

- Configurazione dell'account Oracle Support
- Creazione di una richiesta di supporto

Per istruzioni su come autorizzare gli utenti ad aprire le richieste di supporto My Oracle Cloud Support, consulta Administrator Tasks for Support.

Supporto AWS ambito e informazioni di contatto

Supporto AWS è la tua prima linea di supporto per tutti i problemi e le domande AWS correlati. Crea una Supporto AWS richiesta per il tuo problema, come fai con altri AWS servizi. Il Supporto AWS team collabora con OCI Support secondo necessità.

Di seguito sono riportati alcuni esempi di AWS problemi relativi a Oracle Database@ che Supporto AWS possono esserti utili:

- Problemi di rete virtuale, inclusi quelli riguardanti la traduzione degli indirizzi di rete (NAT), i firewall, il DNS e la gestione del traffico e le sottoreti AWS
- Problemi relativi a Bastion e alle macchine virtuali (VM), tra cui connessione all'host del database, installazione del software, latenza e prestazioni dell'host
- Reportistica dei parametri del cluster Exadata VM all'interno di Amazon CloudWatch
- Problemi di fatturazione relativi ai servizi AWS

Per informazioni su Supporto AWS, consulta Guida introduttiva a Supporto AWS.

Contratti sui livelli di servizio Oracle

Se hai domande su Oracle Database@AWS Service Level Agreements (SLAs) o desideri richiedere crediti di servizio per le violazioni degli SLA, contatta il tuo account manager Oracle. Per ulteriori informazioni, consulta i Service Level Agreement.

Quote per Oracle Database@AWS

Oracle Database@AWS è un'offerta multicloud. AWS non imposta o impone quote per le risorse. Oracle Database@AWS Le quote vengono applicate da Oracle Cloud Infrastructure (OCI). Per ulteriori informazioni sulle quote OCI, consulta Quote e limiti di servizio nella documentazione dell'infrastruttura Oracle Cloud.

Cronologia dei documenti per la Guida per Oracle Database@AWS l'utente

La tabella seguente descrive le versioni della documentazione per Oracle Database@AWS.

Modifica	Descrizione	Data
Oracle Database@AWS supporta la regione Asia Pacifico (Sydney) e la regione Canada (Centrale)	Puoi creare Oracle Database@AWS le tue risorse in queste regioni. Per ulteriori informazioni, consulta Regioni supportate per Oracle Database@AWS.	2 febbraio 2026
Oracle Database@AWS supporta la regione Asia Pacifico (Tokyo), la regione Stati Uniti orientali (Ohio), la regione Europa (Francoforte)	Puoi creare Oracle Database@AWS le tue risorse in queste regioni. Per ulteriori informazioni, consulta Regioni supportate per Oracle Database@AWS.	22 dicembre 2025
Oracle Database@AWS supporta la condivisione dei diritti tra Account AWS	Ora puoi condividere i diritti di AWS Marketplace per Oracle Database@ all'interno della stessa AWS organizzazione utilizzando Account AWS AWS License Manager. AWS Per ulteriori informazioni, vedere Entitlement sharing in Oracle Database@.AWS	19 dicembre 2025
Oracle Database@AWS supporta la modifica dei filtri di dati di integrazione zero-ETL	Oracle Database@AWS supporta la modifica dei filtri di dati per le integrazioni zero-ETL esistenti con Amazon Redshift. Puoi aggiornare i	15 ottobre 2025

	modelli di filtro dei dati per includere o escludere schemi e tabelle specifici dalla replica dei dati. Per ulteriori informazioni, consulta Gestione delle integrazioni zero-ETL.	
Oracle Database@AWS supporta la gestione CIDR della rete peer per le connessioni peering	È possibile specificare una rete peer CIDRs quando si creano o si aggiornano le connessioni peering ODB. Puoi controllare quali sottoreti del VPC peer hanno accesso alla tua rete ODB. Un account VPC può aggiornare gli intervalli CIDR senza possedere anche la rete ODB. Per ulteriori informazioni, consulta Configurazione del peering ODB su un Amazon VPC in. Oracle Database@AWS	10 ottobre 2025
Oracle Database@AWS supporta l'integrazione zero-ETL con Amazon Redshift	Oracle Database@AWS ora si integra con VPC Lattice per consentire l'integrazione zero-ETL con Amazon Redshift. Per ulteriori informazioni, consulta Integrazioni di servizi per Oracle Database@.AWS	2 luglio 2025

Aggiornamento alle autorizzazioni del ruolo collegato ai servizi di IAM	La `AmazonODBServiceRolePolicy` policy ora concede autorizzazioni aggiuntive per descrivere gli allegati del gateway di transito VPC, descrivere le sottoreti EC2 Amazon e attivare una fonte Amazon. EventBridge Per ulteriori informazioni, consulta gli aggiornamenti alle politiche gestite.Oracle Database@AWSAWS	30 giugno 2025
Aggiornamento alle autorizzazioni del ruolo collegato ai servizi di IAM	La `AmazonODBServiceRolePolicy` policy ora concede autorizzazioni aggiuntive per descrivere gli eventi in Amazon EventBridge Scheduler e creare o descrivere un bus di eventi. Per ulteriori informazioni, consulta Oracle Database@AWS gli aggiornamenti delle politiche gestite. AWS	26 giugno 2025
Oracle Database@AWS supporta la regione Stati Uniti occidentali (Oregon)	Puoi creare Oracle Database@AWS le tue risorse nella regione Stati Uniti occidentali (Oregon). Le AZ fisiche supportate IDs sono `usw2-az3` e `usw2-az4`. Per ulteriori informazioni, consulta Regioni supportate per Oracle Database@AWS.	26 giugno 2025

Oracle Database@AWS supporta la condivisione delle risorse tra Account AWS	Ora puoi condividere l'infrastruttura Exadata e i cluster VM con altri membri della tua Account AWS organizzazione utilizzando (). AWS Resource Access Manager AWS RAMÈ possibile effettuare il provisioning dell'infrastruttura una sola volta e condividerla tra più account, riducendo i costi e mantenendo la separazione delle responsabilità. Per ulteriori informazioni, vedere Condivisione delle risorse in Oracle Database@AWS.	26 giugno 2025
Oracle Database@AWS supporta eventi in Amazon EventBridge	Oracle Database@AWS fornisce eventi ad Amazon EventBridge per monitorare i cambiamenti del ciclo di vita delle risorse. Gli eventi vengono generati sia AWS da fonti OCI che da fonti OCI, consentendoti di tenere traccia delle modifiche alla rete ODB, all'infrastruttura Exadata, ai cluster di VM e ai database. Per ulteriori informazioni, consulta Monitoraggio Oracle Database@AWS degli eventi in Amazon EventBridge.	26 giugno 2025

Oracle Database@AWS supporta l'abbonamento in più regioni	Oracle Database@AWS supporta l'abbonamento interregionale, che consente di abbonarsi una sola volta e utilizzare il servizio in tutte le aree disponibili. Regioni AWS Per ulteriori informazioni, consulta Abbonarsi a Oracle Database@AWS in più regioni.	26 giugno 2025
Oracle Database@AWS supporta le connessioni peering ODB come risorsa separata	Le connessioni peering ODB sono ora una risorsa separata dedicata APIs alla creazione, visualizzazione ed eliminazione delle connessioni peering. Puoi creare connessioni peering tra una rete ODB e un Amazon VPC nello stesso account o in account diversi. Per ulteriori informazioni, consulta Working with ODB peering Connections.	26 giugno 2025
Oracle Database@AWS integra la rete ODB con Amazon S3	Oracle Database@AWS ora si integra con VPC Lattice per consentire i backup gestiti da Oracle su Amazon S3 e l'accesso diretto alla rete ODB ad Amazon S3. Per ulteriori informazioni, consulta Service integrations for Oracle Database@.AWS	26 giugno 2025

Oracle Database@AWS supporta i cluster di VM autonomi	Ora puoi creare cluster di VM autonomi sulla tua infrastruttura Exadata. I cluster VM autonomi sono database completamente gestiti che automatizzano le attività di gestione chiave utilizzando l'apprendimento automatico e l'intelligenza artificiale. Per ulteriori informazioni, consulta Fase 3: Creare un cluster di macchine virtuali Exadata o un cluster di macchine virtuali autonome in. Oracle Database@AWS	28 maggio 2025
Oracle Database@AWS supporta finestre di manutenzione personalizzabili	Ora puoi configurare le finestre di manutenzione per la tua infrastruttura Exadata con opzioni per pianificazioni gestite da Oracle o gestite dal cliente. È inoltre possibile selezionare le modalità di applicazione delle patch (Rolling o Non-Rolling) e specificare le preferenze relative ai tempi di manutenzione. Per ulteriori informazioni, consulta Creare un'infrastruttura Oracle Exadata in. Oracle Database@AWS	1 maggio 2025

Oracle Database@AWS supporta una nuova zona di disponibilità (AZ)	È ora possibile creare una rete ODB in una zona AZ con l'ID fisico `use1-az4` o `use1-az6`. Per ulteriori informazioni, consulta l'infrastruttura Oracle Exadata.	26 marzo 2025
Oracle Database@AWS supporta i gateway di transito Amazon VPC	Se colleghi un gateway di transito a un VPC collegato a una rete ODB, puoi connetter ne più VPCs di uno a questo gateway. Le applicazioni in esecuzione in questi ambienti VPCs possono accedere a un cluster di macchine virtuali Exadata in esecuzione nella rete ODB. Per ulteriori informazioni, consulta Configurazione dei gateway di transito Amazon VPC per. Oracle Database@AWS	26 marzo 2025
Oracle Database@AWS supporta tipi di server di database e storage per Exadata X11M	È possibile specificare il tipo di server di database e il tipo di server di archiviazione quando si crea un'infrastruttura utilizzando Exadata X11M. Per ulteriori informazioni, vedere Creare un'infrastruttura Oracle Exadata in. Oracle Database@AWS	4 febbraio 2025

Nuova politica relativa ai ruoli legati ai servizi	Oracle Database@AWS ha aggiunto una nuova politica `AmazonODBServiceRolePolicy` per il ruolo collegato al `AWSServiceRoleForODB` servizio. Per ulteriori informazioni, consulta l'argomento relativo agli Aggiornamenti di Oracle Database@AWS sulle policy gestite da AWS.	2 dicembre 2024
Versione iniziale	Versione iniziale della Guida per l'utente Oracle Database@AWS	2 dicembre 2024

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.