Oracle Database@AWS Guide de l'utilisateur

Oracle Database@AWS

Oracle Database@AWS: Oracle Database@AWS Guide de l'utilisateur

Table of Contents

Qu'est-ce que c'est Oracle Database@AWS ? 1
Caractéristiques 1
Services connexes 2
Accès 3
Tarification 3
Quelle est la prochaine étape ? 4
Comment ça marche 5
Sites OCI pour enfants 5
Infrastructure Oracle Exadata 6
Réseau ODB 6
Cloud privé virtuel (VPC) 8
Peering ODB 8
Création d'une connexion d'appairage ODB 9
AWS intégrations de services 10
Acheminement du trafic à partir de plusieurs VPCs 11
AWS Transit Gateway 11
AWS Réseau WAN dans le cloud 11
Clusters de machines virtuelles Exadata 12
Clusters de machines virtuelles autonomes 12
Bases de données Oracle Exadata 13
Intégration 14
Inscrivez-vous pour un Compte AWS 14
Création d’un utilisateur doté d’un accès administratif 14
Demandez une offre privée 16
Abonnez-vous dans plusieurs régions 17
Prise en main 19
Conditions préalables 19
Services OCI pris en charge 19
Régions prises en charge 20
Planification de l'espace d'adressage IP 21
Restrictions relatives aux adresses IP dans le réseau ODB 21
Exigences CIDR du sous-réseau client 22
Exigences CIDR du sous-réseau Backup 23
Scénarios de consommation IP 23

Étape 1 : Création d'un réseau ODB 25
Étape 2 : Création d'une infrastructure Oracle Exadata 27
Étape 3 : créer un cluster de machines virtuelles 30
Étape 4 : Création de bases de données Oracle Exadata 35
Peering ODB 36
Configuration du peering ODB 36
Mettre à jour le peering ODB 38
Configuration des tables de routage VPC pour le peering ODB 39
Configuration du DNS 40
Comment fonctionne le DNS dans Oracle Database@AWS 40
Configuration d'un point de terminaison sortant 41
Configuration d'une règle de résolution 42
Tester la configuration de votre DNS 44
Configuration des passerelles de transit Amazon VPC pour Oracle Database@AWS 44
Exigences 45
Limitations 45
Mise en place et configuration d'une passerelle de transit 46
Configuration du AWS Cloud WAN pour Oracle Database@AWS 47
Partage des droits 49
Méthodes de partage 49
Partage des droits avec AWS License Manager 49
Partage de ressources avec AWS Resource Access Manager (AWS RAM) 49
Limitations 49
Partage des droits entre les comptes 50
Conditions préalables au partage des droits 50
Autorisations requises pour le partage des droits 50
Partage des droits 51
Partage de ressources 52
AWS RAM intégration 52
Avantages 52
Comment fonctionne le partage des ressources 53
Autorisations sur les ressources partagées 54
Limitations 55
Limites relatives au partage des ressources 55
Limites relatives à la création et à l'utilisation de ressources partagées 56
Limitations relatives à la suppression de ressources partagées 56

Partage des ressources entre les comptes 56
Conditions préalables au partage des ressources 57
Partage de ressources 57
Afficher vos partages de ressources 58
Mettre à jour ou supprimer des partages de ressources 59
Initialisation du service 60
Qu'est-ce que l'initialisation du service ? 60
Étapes suivantes 61
Utilisation de ressources partagées dans un compte sécurisé 62
Limites d'un compte fiable 62
Création de clusters de machines virtuelles 63
Afficher les ressources partagées 64
Configuration du peering ODB avec des réseaux ODB partagés 65
Gestion 67
Mettre à jour un réseau ODB 67
Supprimer un réseau ODB 68
Supprimer un cluster de machines virtuelles 68
Suppression d'une infrastructure Exadata 69
Supprimer une connexion d'appairage ODB 69
Sauvegarde 71
Sauvegardes gérées par Oracle 71
Sauvegardes gérées par l'utilisateur 71
Conditions préalables 72
Sauvegarde sécurisée Oracle 75
Storage Gateway 76
Point de montage S3 78
Désactivation de l'accès à S3 81
Résolution des problèmes liés à l'intégration Amazon S3 81
Intégration zéro ETL avec Redshift 83
Versions de base de données compatibles 83
Comment ça marche 84
Conditions préalables 85
Prérequis généraux 85
Prérequis pour la base de données 85
Considérations 90
Limitations 90

Configuration 91
Étape 1 : Activez Zero-ETL pour votre réseau ODB 92
Étape 2 : Configuration de votre base de données Oracle 93
Étape 3 : configurer le Gestionnaire de AWS Secrets Manager et le service de gestion des AWS clés 93
Étape 4 : Configuration des autorisations IAM 96
Étape 5 : Configuration des politiques de ressources Amazon Redshift 98
Étape 6 : Créez l'intégration Zero-ETL à l'aide de AWS Glue 99
Étape 7 : créer une base de données cible dans Amazon Redshift 100
Vérifiez l'intégration Zero-ETL 101
Filtrage des données 102
Contrôle 103
Surveillance de l'état de l'intégration 103
Surveillance des performances 103
Gestion 104
Modification des intégrations zéro ETL 104
Suppression d'intégrations zéro ETL 106
Bonnes pratiques 107
Résolution des problèmes 109
Défaillances de configuration d'intégration 109
Problèmes de réplication 110
Problèmes de cohérence des données 111
Surveillance et débogage 111
Sécurité 113
Protection des données 114
Chiffrement des données 115
Chiffrement en transit 115
Gestion des clés 116
Gestion des identités et des accès 116
Public ciblé 116
Authentification par des identités 117
Gestion de l’accès à l’aide de politiques 118
Comment Oracle Database@AWS fonctionne avec IAM 120
Politiques basées sur l’identité 126
AWS politiques gérées 131
Oracle Database@AWS authentification et autorisation dans OCI 132

Résolution des problèmes 132
Validation de conformité 134
Résilience 134
Rôles liés à un service 135
Autorisations de rôle liées à un service pour Oracle Database@AWS 135
Régions prises en charge pour les rôles Oracle Database@AWS liés à un service 138
Mises à jour des politiques 138
Contrôle 140
Surveillance avec CloudWatch 141
CloudWatch métriques 141
CloudWatch dimensions 156
Surveillance des événements 158
Vue d'ensemble des événements 159
Evénements de AWS 159
Événements de l'OCI 160
Filtrage des événements 161
Oracle Database@AWS Événements de résolution des problèmes 161
CloudTrail journaux 162
Oracle Database@AWS événements de gestion dans CloudTrail 164
Oracle Database@AWS exemples d'événements 164
Résolution des problèmes 167
Impossible de créer un réseau ODB 167
Résolution des problèmes de connectivité entre votre réseau VPC et ODB ou vos clusters de machines virtuelles 168
Noms d'hôte non résolus ou noms de scan des clusters de machines virtuelles à partir d'un VPC 169
Obtenir de l'aide pour Oracle Database@AWS 169
Étendue du support Oracle et informations de contact 169
Comptes et accès My Oracle Cloud Support 170
AWS Support champ d'application et informations de contact 171
Contrats de niveau de service Oracle 171
Quotas 172
Historique de la documentation 173
..... clxxxii

Qu'est-ce que c'est Oracle Database@AWS ?

Oracle Database@AWS est une offre qui vous permet d'accéder à l'infrastructure Oracle Exadata gérée par Oracle Cloud Infrastructure (OCI) au sein AWS des centres de données. Vous pouvez migrer vos charges de travail Oracle Exadata, établir une connectivité à faible latence avec les applications qui s'exécutent AWS et intégrer des services. AWS Vous recevez une facture unique AWS Marketplace, qui est prise en compte pour les AWS engagements et les récompenses Oracle Support.

Le schéma suivant présente une vue d'ensemble détaillée d'une région OCI liée à un centre de AWS données hébergeant l'infrastructure Oracle Exadata. Au sein d'une zone de AWS disponibilité (AZ), vous pouvez associer un Amazon VPC à un réseau privé lié au centre de données. En connectant ces réseaux, les serveurs d'applications du VPC peuvent accéder aux bases de données Oracle exécutées sur l'infrastructure Oracle Exadata.

Caractéristiques de Oracle Database@AWS

Avec Oracle Database@AWS, vous bénéficiez des fonctionnalités suivantes :

Migration des charges de travail de base de données Oracle Exadata vers AWS

> Avec Oracle Database@AWS, vous pouvez facilement migrer vos charges de travail Oracle Exadata vers Oracle Exadata Database Service sur une infrastructure dédiée ou Oracle Autonomous Database sur une infrastructure Exadata dédiée au sein de l'infrastructure Exadata. AWS La migration offre des modifications minimales, une disponibilité complète des fonctionnalités, une compatibilité architecturale et les mêmes performances que les déploiements Exadata sur site. Vous pouvez utiliser les outils de migration de base de données Oracle standard tels que Recovery Manager (RMAN), Oracle Data Guard, les tablespaces transportables, Oracle Data Pump, Oracle, AWS Database Migration GoldenGate Service et Oracle Zero Downtime Migration.

Latence réduite des applications

> Vous pouvez établir une connectivité à faible latence entre Oracle Exadata et les applications qui s'y exécutent. AWS La proximité des applications hébergées dans le AWS site garantit des délais réseau minimaux et des performances améliorées.

Innovation grâce à l'unification des données

Vous pouvez obtenir des informations plus approfondies et développer de nouvelles innovations en utilisant des intégrations sans ETL pour unifier vos données au sein d'Oracle et à des AWS fins d'analyse, d'apprentissage automatique et d'IA générative. Grâce à l'intégration Zero-ETL à l'aide d'Amazon Redshift, vous pouvez activer l'analyse en temps quasi réel et l'apprentissage automatique (ML) sur les données transactionnelles stockées dans. Oracle Database@AWS

Gestion et opérations simplifiées

Vous pouvez bénéficier d'une expérience unifiée entre Oracle et AWS d'un support, d'achats, de gestion et d'opérations collaboratifs. Votre utilisation des services de base de données Oracle est éligible à vos AWS engagements existants et aux avantages des licences Oracle, tels que le programme Oracle Support Rewards. Vous pouvez utiliser AWS des outils et des interfaces familiers pour acheter, approvisionner et gérer vos Oracle Database@AWS ressources. Vous pouvez provisionner et gérer vos ressources à l'aide AWS APIs de la CLI ou SDKs. AWS APIs Appelez l'OCI correspondant APIs nécessaire pour approvisionner et gérer les ressources.

Intégration fluide avec les AWS services

Vous pouvez intégrer d'autres AWS services et applications exécutés dans le même environnement. Par exemple, Oracle Database@AWS s'intègre à Amazon EC2, Amazon VPC et IAM. Vous pouvez également intégrer Oracle Database@AWS des AWS services tels qu'Amazon CloudWatch pour la surveillance et Amazon EventBridge pour la gestion des événements. Pour les sauvegardes de base de données, vous pouvez utiliser Amazon S3, qui est conçu pour durer plus de 11 à 9 secondes.

Relié Services AWS

Oracle Database@AWS travaille avec les services suivants pour améliorer la disponibilité et l'évolutivité de vos applications de base de données Oracle :

- Amazon EC2 — Fournit des serveurs virtuels qui fonctionnent comme des serveurs d'applications Oracle. Vous pouvez configurer votre équilibreur de charge pour acheminer le trafic vers vos serveurs EC2 d'applications. Pour plus d'informations, consultez le guide de EC2 l'utilisateur Amazon.
- Amazon Virtual Private Cloud (VPC) — Vous permet de lancer AWS des ressources dans un réseau virtuel logiquement isolé que vous avez défini. L'infrastructure Oracle Exadata réside dans un réseau spécial appelé réseau ODB que vous pouvez associer à un VPC. Vous pouvez ensuite

exécuter des serveurs d'applications dans votre VPC et accéder à vos bases de données Exadata. Pour de plus amples informations, consultez le Guide de l'utilisateur Amazon VPC.

- Amazon VPC Lattice — Fournit un accès natif à des AWS services tels qu'Amazon S3 et les sauvegardes gérées par Oracle depuis le réseau ODB. Pour plus d'informations, consultez le document Qu'est-ce qu'Amazon VPC Lattice ? .
- Amazon CloudWatch — Fournit un service de surveillance pour Oracle Database@AWS. OCI collecte les données métriques relatives à votre système Oracle Exadata et les envoie à. CloudWatch Pour de plus amples informations, veuillez consulter Surveillance Oracle Database@AWS avec Amazon CloudWatch.
- Gestion des identités et des accès AWS (IAM) — Vous aide à contrôler en toute sécurité l'accès aux Oracle Database@AWS ressources pour vos utilisateurs. Utilisez IAM pour contrôler qui peut utiliser vos AWS ressources (authentification) et quelles ressources les utilisateurs peuvent utiliser et de quelle manière (autorisation). Pour de plus amples informations, veuillez consulter Gestion des identités et des accès pour Oracle Database@AWS.
- AWS services d'analyse — Fournissez un ensemble large et rentable de services d'analyse pour vous aider à obtenir des informations plus rapidement à partir de votre base de données Exadata. Chaque service est spécialement conçu pour un large éventail de cas d'utilisation analytiques tels que l'analyse interactive, le traitement des mégadonnées, l'entreposage de données, l'analyse en temps réel, l'analyse opérationnelle, les tableaux de bord et les visualisations. Pour plus d'informations, consultez Analytics sur AWS.

Accès Oracle Database@AWS

Vous pouvez créer, accéder et gérer à Oracle Database@AWS l'aide du AWS Management Console. Il fournit une interface Web à laquelle vous pouvez accéder Oracle Database@AWS.

Tarification pour Oracle Database@AWS

Vous pouvez acheter Oracle Database@AWS des offres auprès de AWS Marketplace. Vous contactez d'abord un représentant commercial Oracle. Oracle met ensuite l'offre à votre disposition sur la AWS Marketplace base de l'accord de tarification privé. Votre AWS facture indique les frais en fonction de votre consommation.

Aucuns frais de transfert de données ne sont facturés lorsque votre application Oracle et votre base de données Oracle sont hébergées dans la même zone de disponibilité (AZ). Les frais de transfert de données standard s'appliquent aux communications entre AZs.

Lorsque vous utilisez des intégrations Oracle Database@AWS gérées telles que Zero-ETL, les sauvegardes gérées par Oracle et Amazon S3, les frais de traitement des données standard pour le partage et l'accès aux ressources via VPC Lattice s'appliquent. Il n'y a aucun frais horaire pour les intégrations Oracle Database@AWS gérées. Pour plus d'informations, consultez la tarification d'Amazon VPC Lattice.

Quelle est la prochaine étape ?

Vous êtes maintenant prêt à commencer à créer vos Oracle Database@AWS ressources.

1. Découvrez comment Oracle Database@AWS cela fonctionne. Pour de plus amples informations, veuillez consulter Comment Oracle Database@AWS fonctionne.

   > **Note**
   >
   > Si vous connaissez Oracle Exadata AWS et que vous souhaitez commencer immédiatement, ignorez cette étape.

2. Demandez une offre privée Oracle Database@AWS par le biais du AWS Management Console, puis acceptez l'offre. Pour de plus amples informations, veuillez consulter Demandez une offre privée pour Oracle Database@AWS.

   > **Note**
   >
   > Pour demander une offre privée dans cet aperçu, vous devez nous contacter AWS pour être Compte AWS ajouté à une liste d'autorisation.

3. Créez votre réseau ODB, votre infrastructure Oracle Exadata et vos clusters de machines virtuelles Exadata à l'aide de la console. AWS Créez vos bases de données Exadata à l'aide des outils OCI. Pour de plus amples informations, veuillez consulter Commencer à utiliser Oracle Database@AWS.
4. Partagez vos ressources entre comptes avec AWS Resource Access Manager (AWS RAM). Pour de plus amples informations, veuillez consulter Utilisation de Oracle Database@AWS ressources partagées dans un compte sécurisé.

Comment Oracle Database@AWS fonctionne

Oracle Database@AWS intègre Oracle Cloud Infrastructure (OCI) au AWS Cloud. Dans les sections suivantes, vous découvrirez les principaux composants de cette architecture multicloud.

Le service de base de données Oracle Exadata sur une infrastructure dédiée est un service OCI qui fournit une machine de base de données Exadata. Oracle Exadata Database Machine est une plateforme complète intégrée, préconfigurée et prétestée à utiliser dans les centres de données d'entreprise. Vous pouvez créer l'infrastructure Oracle Exadata et les clusters de machines virtuelles dans une zone de AWS disponibilité (AZ) à l'aide de la AWS console, de la CLI ou APIs.

Après avoir créé vos ressources dans AWS, vous utilisez OCI APIs pour créer et gérer les bases de données Oracle Exadata. Un réseau ODB, que vous associez à un Amazon VPC, permet aux serveurs d'applications EC2 Amazon d'accéder à vos bases de données Exadata. Les bases de données Oracle Exadata sont ainsi intégrées dans l' AWS environnement.

Le schéma suivant montre l' Oracle Database@AWS architecture.

Sites OCI pour enfants

L'infrastructure Oracle Cloud est hébergée dans les régions OCI et les domaines de disponibilité. Une région OCI est composée de domaines de disponibilité OCI (ADs), qui sont des clusters de centres de données isolés au sein d'une région OCI. Un site enfant OCI est un centre de données qui étend un domaine de disponibilité OCI à une zone de disponibilité (AZ) d'une AWS région. L'infrastructure Exadata réside logiquement dans une région OCI et réside physiquement dans une région. AWS

Le site enfant OCI se trouve Oracle Database@AWS physiquement dans un centre de AWS données. AWS héberge l'infrastructure Exadata, et OCI fournit et entretient le matériel d'infrastructure Exadata au sein du centre de données. Vous pouvez configurer l'infrastructure Exadata, le réseau privé et les clusters de machines virtuelles à l'aide de la AWS console, de la CLI ou APIs. Vous pouvez utiliser AWS des services tels qu'Amazon EC2 et Amazon VPC pour permettre aux applications d'accéder aux bases de données Oracle Exadata exécutées sur l'infrastructure.

Infrastructure Oracle Exadata

L'infrastructure Oracle Exadata est l'architecture sous-jacente des serveurs de base de données et des serveurs de stockage qui exécutent les bases de données Oracle Exadata. L'infrastructure réside dans une zone de AWS disponibilité (AZ). Pour créer des clusters de machines virtuelles sur l'infrastructure Exadata, vous utilisez la AWS console, la CLI ou APIs.

L'infrastructure Oracle Exadata est distribuée sur des machines physiques appelées serveurs de base de données. Ces serveurs fournissent les ressources de calcul, comme les serveurs EC2 dédiés Amazon. Chaque serveur de base de données héberge une ou plusieurs machines virtuelles (VMs) exécutées sur un hyperviseur. Pour les diagrammes architecturaux illustrant ces relations, voir Exadata Database Service on Dedicated Infrastructure Technical Architecture.

Lorsque vous créez une infrastructure Exadata dans Oracle Database@AWS, vous spécifiez des informations telles que les suivantes :

- Nombre total de serveurs de base de données
- Nombre total de serveurs de stockage
- Le modèle du système Exadata (X11M)
- L'AZ qui héberge l'infrastructure (voirRégions prises en charge pour Oracle Database@AWS)

Pour savoir comment créer une infrastructure Oracle Exadata, voirÉtape 2 : créer une infrastructure Oracle Exadata dans Oracle Database@AWS.

Réseau ODB

Un réseau ODB est un réseau privé isolé qui héberge l'infrastructure OCI dans une zone de AWS disponibilité (AZ). Le réseau ODB se compose d'une plage d'adresses IP CIDR. Le réseau ODB correspond directement au réseau existant au sein du site enfant OCI, servant ainsi de moyen de communication entre AWS et OCI. Vous devez spécifier un réseau ODB lorsque vous créez vos clusters de machines virtuelles Exadata (voirÉtape 3 : créer un cluster de machines virtuelles Exadata ou un cluster de machines virtuelles autonome dans Oracle Database@AWS).

Vous approvisionnez des ressources dans un réseau ODB à l'aide d'Oracle AWS APIs Database@. Le réseau ODB est géré par AWS, mais vous pouvez configurer une connexion d'appairage ODB pour connecter un Amazon VPC au réseau ODB. Pour plus d'informations, voir enPeering ODB.

Lorsque vous créez un réseau ODB, vous spécifiez des informations telles que les suivantes :

- Zone de disponibilité — Le réseau ODB est spécifique à une AZ.

  Vous pouvez l'utiliser Oracle Database@AWS dans les domaines suivants Régions AWS :

  USA Est (Virginie du Nord)

  Vous pouvez utiliser le AZs avec le support physique IDs `use1-az4` et`use1-az6`.

  USA Ouest (Oregon)

  Vous pouvez utiliser le AZs avec le support physique IDs `usw2-az3` et`usw2-az4`.

  Asie-Pacifique (Tokyo)

  Vous pouvez utiliser le AZs avec le support physique IDs `apne1-az1` et`apne1-az4`.

  USA Est (Ohio)

  Vous pouvez utiliser le AZs avec le support physique IDs `use2-az1` et`use2-az2`.

  Europe (Francfort)

  Vous pouvez utiliser le AZs avec le support physique IDs `euc1-az1` et`euc1-az2`.

  Canada (Centre)

  Vous pouvez utiliser l'AZ avec l'identifiant physique`cac1-az4`.

  Asie-Pacifique (Sydney)

  Vous pouvez utiliser l'AZ avec l'identifiant physique`apse2-az4`.

  Pour trouver dans votre compte les noms de zones de zone de données logiques qui correspondent à la zone de zone de disponibilité physique précédente IDs, exécutez la commande suivante.

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

- Adresses CIDR du client : le réseau ODB nécessite un CIDR de sous-réseau client pour les clusters de machines virtuelles Exadata et les clusters de machines virtuelles autonomes.

- Adresses CIDR de sauvegarde : le réseau ODB nécessite un sous-réseau CIDR de sauvegarde pour les sauvegardes de bases de données gérées des clusters de machines virtuelles. Le sous-réseau de sauvegarde est facultatif pour les clusters de machines virtuelles Exadata.
- AWS intégrations de services — Vous pouvez configurer un chemin réseau pour les intégrations de AWS services telles qu'Amazon S3 et Zero-ETL avec Amazon Redshift. Pour de plus amples informations, veuillez consulter AWS intégrations de services.

Pour de plus amples informations, veuillez consulter Étape 1 : créer un réseau ODB dans Oracle Database@AWS.

Cloud privé virtuel (VPC)

Un Virtual Private Cloud (VPC) est un réseau virtuel que vous créez dans le cloud. AWS Il est logiquement isolé des autres réseaux virtuels dans le AWS cloud, ce qui vous permet de contrôler totalement l'environnement réseau virtuel, y compris la sélection de votre propre plage d'adresses IP, la création de sous-réseaux et la configuration des tables de routage et des passerelles réseau. Pour plus d'informations, consultez Qu'est-ce qu'Amazon VPC ?

Vous pouvez lancer des EC2 instances Amazon dans votre Amazon VPC. Les EC2 instances peuvent héberger des serveurs d'applications qui communiquent avec les bases de données Oracle Exadata. Vous pouvez gérer et lancer les serveurs d'applications comme n'importe quelle autre EC2 instance de votre VPC. Pour plus d'informations, consultez Qu'est-ce qu'Amazon EC2 ?

Par défaut, le réseau ODB n'est pas connecté à VPCs. Pour connecter le réseau ODB à votre AWS infrastructure existante, créez une connexion d'appairage entre le réseau ODB et un VPC. Vous pouvez spécifier le VPC lorsque vous créez le réseau ODB. Pour de plus amples informations, veuillez consulter Étape 1 : créer un réseau ODB dans Oracle Database@AWS.

Peering ODB

Le peering ODB est une connexion réseau créée par l'utilisateur qui permet de router le trafic de manière privée entre un Amazon VPC et un réseau ODB. Il existe une relation 1:1 entre un VPC et un réseau ODB. Après le peering, une EC2 instance Amazon au sein du VPC peut communiquer avec une base de données Oracle Exadata du réseau ODB comme si elle se trouvait dans le même réseau.

> **Note**
>
> Le peering ODB est différent du peering VPC, qui est une connexion d'appairage entre deux VPCs personnes qui achemine le trafic entre elles.

Vous pouvez associer un réseau ODB dans un compte et un VPC dans un autre compte en utilisant. AWS RAM Si vous partagez un réseau ODB avec un autre compte, le compte fiduciaire peut directement initier le peering. Le compte qui initie la connexion d'appairage ODB possède et gère la connexion.

Vous pouvez spécifier un réseau homologue CIDRs lorsque vous créez ou mettez à jour des connexions d'appairage ODB. De cette façon, vous contrôlez quels sous-réseaux du VPC homologue ont accès à votre réseau ODB. Un compte VPC peut mettre à jour les plages d'adresses CIDR sans être également propriétaire du réseau ODB. Pour plus d'informations, consultez Configuration de l'appairage ODB vers un Amazon VPC dans. Oracle Database@AWS

Les ressources d'un VPC peuvent s'étendre sur plusieurs zones de disponibilité ()AZs. Dans un réseau ODB, les ressources sont liées à une seule AZ. Vous définissez cette AZ lorsque vous créez le réseau ODB.

Création d'une connexion d'appairage ODB

Une connexion d'appairage ODB n'est pas une caractéristique d'un réseau ODB mais constitue une ressource indépendante dotée de son propre identifiant (préfixé par) et de son propre cycle de `odbpcx-` vie. Vous gérez une connexion de peering grâce à un ensemble de connexions dédiées APIs. Par exemple, vous créez une connexion d'appairage ODB vers un réseau ODB existant à l'aide de la console Oracle Database@AWS ou de l'API. `CreateOdbPeeringConnection` Pour de plus amples informations, veuillez consulter Création d'une connexion d'appairage ODB dans Oracle Database@AWS.

Lorsque vous créez une connexion d'appairage ODB, Oracle Database@AWS exécute automatiquement les actions suivantes :

1. Valide les configurations réseau, notamment en vérifiant l'absence de chevauchement des blocs d'adresse CIDR avec le code CIDR Oracle VCN
2. Configure l'infrastructure de peering du réseau sous-jacente

3. Configure les tables de routage du réseau ODB (et non le VPC) avec les adresses CIDR du VPC

Après avoir créé votre connexion d'appairage ODB, mettez à jour vos tables de routage VPC manuellement à l'aide de la commande Amazon. EC2 `create-route` Pour de plus amples informations, veuillez consulter Configuration des tables de routage VPC pour le peering ODB.

AWS intégrations de services

Pour fournir des fonctionnalités et des options de connectivité améliorées pour vos bases de données Oracle, Oracle Database@AWS s'intègre à Services AWS Amazon VPC Lattice. Vous pouvez configurer des chemins réseau Services AWS directement depuis votre réseau ODB sans avoir besoin de configurations réseau supplémentaires VPCs ou complexes.

Oracle Database@AWS prend en charge les intégrations de services AWS gérés suivantes :

Amazon S3

Vous pouvez intégrer Amazon S3 à Oracle Database@ de la AWS manière suivante :

- Oracle a géré des sauvegardes automatiques sur Amazon S3 : Oracle Database@ active AWS automatiquement l'accès au réseau pour les sauvegardes automatiques. Cette intégration ne peut pas être désactivée. Si vous définissez Amazon S3 comme cible de sauvegarde gérée dans la console OCI, OCI télécharge les sauvegardes automatiques dans un compartiment S3.
- Accès direct à Amazon S3 depuis votre réseau ODB — Vous pouvez activer l'accès direct au réseau ODB à S3, puis stocker des scripts, importer et exporter des fichiers et des fichiers associés dans un compartiment S3. Vous pouvez désactiver cet accès. Ce paramètre est indépendant de l'accès automatique au réseau pour les sauvegardes automatiques gérées par Oracle.

Intégration zéro ETL à Amazon Redshift

Vous pouvez activer l'intégration zéro ETL de votre réseau ODB avec Amazon Redshift. Cette intégration vous permet de répliquer des données vers Amazon Redshift à partir de vos bases de données Oracle exécutées dans Oracle AWS Database@ sans le processus traditionnel d'extraction, de transformation et de chargement (ETL). Cette intégration permet des analyses en temps réel et des charges de travail basées sur l'IA en synchronisant automatiquement vos données Oracle avec Amazon Redshift.

Outre les intégrations gérées pour les AWS services, vous pouvez également utiliser VPC Lattice pour accéder à des services et ressources hébergés dans VPCs d'autres, ou accéder à des instances réseau ODB depuis votre VPC. Vous pouvez gérer l'accès et les ressources à l'aide de la console VPC Lattice, de la CLI et. APIs Pour plus d'informations, consultez les ressources suivantes :

- Sauvegarde dans Oracle Database@AWS
- Intégration d'Oracle Database@AWS Zero-ETL à Amazon Redshift
- Qu'est-ce qu'Amazon VPC Lattice ? et VPC Lattice pour Oracle Database@AWS

Acheminement du trafic à partir de plusieurs VPCs

Pour permettre VPCs à plusieurs d'accéder aux Oracle Database@AWS ressources d'un même réseau ODB, vous pouvez utiliser AWS Transit Gateway AWS le Cloud WAN.

AWS Transit Gateway

Une passerelle de transit Amazon VPC est un hub de transit réseau utilisé pour interconnecter VPCs des réseaux sur site. Un réseau ODB prend uniquement en charge le peering one-to-one direct entre le réseau ODB et un seul VPC. Vous pouvez associer votre réseau ODB à un VPC, puis associer ce VPC à une passerelle de transit. La passerelle peut se connecter à plusieurs VPCs. Avec cette configuration de passerelle de transit, vous pouvez acheminer le trafic entre plusieurs sous-réseaux VPC vers un seul réseau ODB.

Pour de plus amples informations, veuillez consulter Configuration des passerelles de transit Amazon VPC pour Oracle Database@AWS.

AWS Réseau WAN dans le cloud

AWS Le cloud WAN est un service de réseau étendu (WAN) géré qui vous permet de créer, de gérer et de surveiller un réseau mondial unifié connectant les ressources de votre cloud et de vos environnements sur site. À l'aide du tableau de bord central, vous pouvez connecter les succursales sur site, les centres de données et l' VPCs ensemble du réseau AWS mondial.

Vous pouvez associer votre réseau ODB à un VPC, puis associer ce VPC au réseau principal Cloud WAN. Avec cette configuration, vous pouvez utiliser le Cloud WAN pour acheminer le trafic entre plusieurs réseaux VPCs ou des réseaux locaux et votre réseau ODB. Pour de plus amples informations, veuillez consulter Configuration du AWS Cloud WAN pour Oracle Database@AWS.

Clusters de machines virtuelles Exadata

Un cluster de machines virtuelles Exadata est un ensemble d' VMsExadata étroitement couplés. Chaque machine virtuelle dispose d'une installation de base de données Oracle complète qui inclut toutes les fonctionnalités d'Oracle Enterprise Edition, notamment Oracle Real Application Clusters (Oracle RAC) et Oracle Grid Infrastructure. Vous pouvez créer une ou plusieurs bases de données Oracle Exadata sur un cluster de machines virtuelles. Pour les diagrammes illustrant l'architecture VMs et les clusters de machines virtuelles, voir Exadata Database Service on Dedicated Infrastructure Technical Architecture.

Lorsque vous créez un cluster de machines virtuelles, vous spécifiez les informations suivantes :

- Un réseau ODB
- Une infrastructure Oracle Exadata
- Les serveurs de base de données sur lesquels placer le VMs dans le cluster
- La quantité totale de stockage Exadata utilisable

Vous pouvez configurer les cœurs de processeur, la mémoire et le stockage local pour chaque machine virtuelle d'un cluster de machines virtuelles. Pour de plus amples informations, veuillez consulter Étape 3 : créer un cluster de machines virtuelles Exadata ou un cluster de machines virtuelles autonome dans Oracle Database@AWS.

Clusters de machines virtuelles autonomes

Les clusters de machines virtuelles autonomes sont des bases de données entièrement gérées qui automatisent les tâches de gestion clés à l'aide de l'apprentissage automatique et de l'IA. Contrairement aux bases de données traditionnelles, les bases de données autonomes provisionnent, sécurisent, mettent à jour, sauvegardent et ajustent automatiquement la base de données sans intervention humaine.

Vous pouvez configurer le nombre de cœurs ECPU par machine virtuelle, la mémoire de base de données par processeur, le stockage de base de données et le nombre maximum de bases de données de conteneurs autonomes. Pour de plus amples informations, veuillez consulter Étape 3 : créer un cluster de machines virtuelles Exadata ou un cluster de machines virtuelles autonome dans Oracle Database@AWS.

Bases de données Oracle Exadata

Oracle Exadata est un système conçu qui fournit une plate-forme haute performance pour exécuter des bases de données Oracle. Avec Oracle Database@AWS, vous utilisez la AWS console pour créer l'infrastructure Oracle Exadata et les clusters de machines virtuelles qui hébergent les bases de données Exadata. Vous utilisez ensuite OCI APIs pour créer et gérer les bases de données Oracle. Pour de plus amples informations, veuillez consulter Étape 4 : Création de bases de données Oracle Exadata dans Oracle Cloud Infrastructure.

Intégration à Oracle Database@AWS

Avant de commencer à utiliser Oracle Database@AWS, assurez-vous d'être inscrit AWS et créez les utilisateurs nécessaires. Vous pouvez ensuite acheter Oracle Database@AWS auprès d'Oracle AWS Marketplace en acceptant une offre privée d'Oracle.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d’inscription, vous recevrez un appel téléphonique ou un SMS et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l’utilisateur racine a accès à l’ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l’utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

Création d’un utilisateur doté d’un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, consultez la section Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

Pour obtenir des instructions, consultez Création d’un ensemble d’autorisations dans le Guide de l’utilisateur AWS IAM Identity Center .

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l’utilisateur AWS IAM Identity Center .

Demandez une offre privée pour Oracle Database@AWS

La fonctionnalité d'offre privée du AWS Marketplace vendeur vous permet de demander et de recevoir les AWS prix Oracle Database@ et les conditions du CLUF auprès d'Oracle. Vous négociez les prix et les conditions avec Oracle, puis Oracle crée une offre privée pour celle Compte AWS que vous désignez. Vous acceptez l'offre privée et recevez le prix et les conditions d'utilisation négociés. À ce stade, vous pouvez utiliser le Oracle Database@AWS tableau de bord. Lorsque le contrat d'offre privée atteint sa date d'expiration, vous êtes soit automatiquement redirigé vers le prix public du produit, soit vous vous désinscrivez d'Oracle AWS Database@. Pour plus d'informations sur les offres privées, consultez la section Offres privées dans AWS Marketplace.

Pour demander et accepter une offre privée pour Oracle Database@AWS

1. Connectez-vous au AWS Management Console.
2. Recherchez puis choisissez Oracle Database@AWS.
3. Choisissez Demander une offre privée.

   > **Note**
   >
   > Le Oracle Database@AWS tableau de bord n'est pas disponible tant que vous n'avez pas accepté une offre privée.

4. Sur le site Oracle Cloud Infrastructure (OCI), spécifiez des détails tels que la région et vos coordonnées.
5. Attendez qu'un représentant de l'OCI vous contacte et vous propose une offre privée.
6. Dans le AWS Management Console, choisissez Afficher l'offre privée.
7. Choisissez l'offre, puis cliquez sur Afficher l'offre.

8. Choisissez Créer un contrat et répondez aux instructions suivantes pour accepter l'offre privée.
9. Après avoir accepté l'offre privée, vous devrez activer votre compte OCI. Vous pouvez accéder aux liens d'activation Oracle directement depuis AWS Management Console.
    1. Dans la console, accédez à la section Commencer.
    2. Cliquez sur le lien d'activation Oracle fourni dans la console. Vous pouvez également utiliser le lien d'activation qui vous a été envoyé par e-mail.
    3. Sur la page d'activation d'Oracle, choisissez de créer un nouveau compte cloud Oracle ou de l'ajouter à un compte existant.
    4. Terminez le processus d'activation en suivant les instructions affichées à l'écran.
    5. Après avoir soumis votre demande d'activation, vous verrez l'état de l'activation en cours dans le AWS Management Console, et le tableau de bord sera temporairement désactivé avec un motif affiché.
    6. Une fois l'activation terminée, le tableau de AWS bord Oracle Database@ devient disponible, vous permettant de gérer vos ressources.
10. Dans le AWS Management Console, choisissez Dashboard.

Abonnez-vous à Oracle Database@AWS dans plusieurs régions

Lorsque vous vous abonnez Oracle Database@AWS AWS Marketplace et que vous terminez votre inscription, votre inscription Compte AWS est liée à votre location OCI. Ce lien, ainsi que les ressources associées, sont automatiquement répliqués dans toutes les AWS régions où il Oracle Database@AWS est disponible. Vous vous abonnez et vous intégrez une seule fois au lieu de répéter le processus pour chaque région.

Pour l'utiliser Oracle Database@AWS dans plusieurs régions, effectuez les opérations suivantes :

1. Inscrivez-vous AWS Marketplace et complétez le processus d'intégration. Oracle Database@AWS

    Lorsque vous vous abonnez pour la première fois à Oracle Database@AWS, votre compte est activé dans une région d'origine. Vous spécifiez la région d'origine dans Oracle Cloud Infrastructure (OCI).
2. Activez vos régions préférées via la console OCI.

    Si vous n'activez pas de région dans OCI, puis que vous passez à cette région dans la Oracle Database@AWS console, vous recevez un message d'erreur indiquant que vous n'êtes pas

abonné. Dans ce cas, vous devez activer cette région dans OCI avant de pouvoir utiliser le Oracle Database@AWS tableau de bord dans cette région.

3. Accédez Oracle Database@AWS à n'importe quelle AWS région prise en charge sans avoir à répéter le processus d'abonnement.

Commencer à utiliser Oracle Database@AWS

Pour commencer à utiliser Oracle Database@AWS, vous pouvez créer les ressources suivantes à l'aide de la Oracle Database@AWS console, de la CLI ou APIs :

1. Réseau ODB
2. Infrastructure Oracle Exadata
3. Cluster de machines virtuelles Exadata ou cluster de machines virtuelles autonome
4. Connexion d'appairage ODB

Pour créer des bases de données Oracle Exadata sur votre infrastructure, vous devez utiliser la console Oracle Cloud Infrastructure (OCI) ou APIs plutôt le Oracle Database@AWS tableau de bord. Ainsi, vous déployez des ressources dans deux environnements cloud : les ressources du réseau et de l'infrastructure sont intégrées AWS, tandis que le plan de contrôle de l'administration de la base de données est dans OCI. Pour plus d'informations, consultez Oracle Database@AWSla documentation d'Oracle Cloud Infrastructure.

Conditions préalables à la configuration Oracle Database@AWS

Avant de configurer votre infrastructure Oracle Exadata, assurez-vous d'effectuer les opérations suivantes :

- Effectuez les étapes décrites dans la section Intégration à Oracle Database@AWS. Vous devez avoir accepté une offre privée pour pouvoir l'utiliser Oracle Database@AWS.
- Accordez à votre principal IAM les autorisations de politique répertoriées dansAutoriser les utilisateurs à provisionner Oracle Database@AWS des ressources. Ces autorisations sont nécessaires à l'utilisation Oracle Database@AWS.

Services OCI pris en charge sur Oracle Database@AWS

Oracle Database@AWS prend en charge les services Oracle Cloud Infrastructure (OCI) suivants :

- Service de base de données Oracle Exadata sur une infrastructure dédiée — Fournit un environnement Exadata entièrement géré et dédié accessible depuis. AWS Pour plus

d'informations, consultez le service de base de données Oracle Cloud Exadata sur une infrastructure dédiée dans la documentation OCI.

- Base de données autonome sur une infrastructure Exadata dédiée : fournit un environnement de base de données hautement automatisé et entièrement géré fonctionnant en OCI avec des ressources matérielles et logicielles dédiées. Pour plus d'informations, voir À propos de la base de données autonome sur une infrastructure Exadata dédiée dans la documentation OCI.

Régions prises en charge pour Oracle Database@AWS

Vous pouvez l'utiliser Oracle Database@AWS dans les domaines suivants Régions AWS :

USA Est (Virginie du Nord)

Vous pouvez utiliser le AZs avec le support physique IDs `use1-az4` et`use1-az6`.

USA Ouest (Oregon)

Vous pouvez utiliser le AZs avec le support physique IDs `usw2-az3` et`usw2-az4`.

Asie-Pacifique (Tokyo)

Vous pouvez utiliser le AZs avec le support physique IDs `apne1-az1` et`apne1-az4`.

USA Est (Ohio)

Vous pouvez utiliser le AZs avec le support physique IDs `use2-az1` et`use2-az2`.

Europe (Francfort)

Vous pouvez utiliser le AZs avec le support physique IDs `euc1-az1` et`euc1-az2`.

Canada (Centre)

Vous pouvez utiliser l'AZ avec l'identifiant physique`cac1-az4`.

Asie-Pacifique (Sydney)

Vous pouvez utiliser l'AZ avec l'identifiant physique`apse2-az4`.

Pour trouver dans votre compte les noms de zones de zone de données logiques correspondant à la zone de zone de disponibilité physique précédente IDs, exécutez la commande suivante.

```
aws ec2 describe-availability-zones \
```

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

Planification de l'espace d'adresse IP dans Oracle Database@AWS

Planifiez soigneusement l'espace d'adressage IP dans Oracle Database@AWS. Tenez compte de la consommation d'adresses IP en fonction du nombre de clusters de machines virtuelles, y compris le VMs nombre de clusters que vous pouvez provisionner sur le réseau ODB. Pour plus d'informations, consultez la section Conception du réseau ODB dans la documentation Oracle Cloud Infrastructure.

Rubriques

- Restrictions relatives aux adresses IP dans le réseau ODB
- Exigences CIDR du sous-réseau client pour le réseau ODB
- Exigences CIDR du sous-réseau de sauvegarde pour le réseau ODB
- Scénarios de consommation IP pour le réseau ODB

Restrictions relatives aux adresses IP dans le réseau ODB

Notez les restrictions suivantes concernant les plages d'adresses CIDR dans le réseau ODB :

- Vous ne pouvez pas modifier la plage CIDR du client ou du sous-réseau de sauvegarde pour le réseau ODB après l'avoir créé.
- Vous ne pouvez pas utiliser les plages d'adresses CIDR VPC dans la colonne Associations restreintes du tableau des restrictions d'association de blocs IPv4 CIDR.
- Pour Exadata X9M, les adresses IP 100.106.0.0/16 et 100.107.0.0/16 sont réservées à l'interconnexion du cluster par automatisation OCI. Vous ne pouvez donc pas effectuer les opérations suivantes :
  - Attribuez ces plages au client ou à la plage CIDR de sauvegarde du réseau ODB.
  - Utilisez ces plages pour un VPC CIDR utilisé pour se connecter au réseau ODB.
- Les plages CIDR suivantes sont réservées à Oracle Cloud Infrastructure et ne peuvent pas être utilisées pour le réseau ODB :
  - Plage réservée Oracle Cloud CIDR 169.254.0.0/16

  - Classe réservée D 224.0.0.0 — 239.255.255.255
  - Classe réservée E 240.0.0.0 — 255.255.255.255
- Vous ne pouvez pas chevaucher les plages d'adresses IP CIDR pour les sous-réseaux client et de sauvegarde.
- Vous ne pouvez pas superposer les plages d'adresses CIDR d'adresses IP allouées aux sous-réseaux client et de sauvegarde avec les plages d'adresses CIDR VPC utilisées pour se connecter au réseau ODB.
- Vous ne pouvez pas approvisionner VMs un cluster de machines virtuelles sur différents réseaux ODB. Le réseau est une propriété du cluster de machines virtuelles, ce qui signifie que vous ne pouvez approvisionner le VMs cluster de machines virtuelles que sur le même réseau ODB.

Exigences CIDR du sous-réseau client pour le réseau ODB

Dans le tableau suivant, vous pouvez trouver le nombre d'adresses IP consommées par le service et l'infrastructure pour le sous-réseau client CIDR. La taille CIDR minimale pour le sous-réseau client est /27 et la taille maximale est /16.

Nombre d'adresses IP	Consommé par	Remarques
6	Oracle Database@AWS	Ces adresses IP sont réservées quel que soit le nombre de clusters de machines virtuelles que vous provisionnez sur le réseau ODB. Oracle Database@AWS consomme ce qui suit : • 3 adresses IP réservées aux ressources du réseau ODB dans AWS • 3 adresses IP réservées au service réseau OCI
3	Chaque cluster de machines virtuelles	Ces adresses IP sont réservées aux noms d'accès client uniques (SCANs), quel que soit le nombre de noms VMs présents dans chaque cluster de machines virtuelles.
4	Chaque machine virtuelle	Ces adresses IP dépendent uniquement du nombre d'adresses IP VMs dans l'infrastructure.

Exigences CIDR du sous-réseau de sauvegarde pour le réseau ODB

Dans le tableau suivant, vous pouvez trouver le nombre d'adresses IP consommées par le service et l'infrastructure pour le sous-réseau de sauvegarde CIDR. La taille CIDR minimale pour le sous-réseau de sauvegarde est /28 et la taille maximale est /16.

Nombre d'adresses IP	Consommé par	Remarques
3	Oracle Database@AWS	Ces adresses IP sont réservées quel que soit le nombre de clusters de machines virtuelles que vous provisionnez sur le réseau ODB. Oracle Database@AWS consomme ce qui suit : • 2 adresses IP au début de la plage CIDR • 1 adresse IP à la fin de la plage CIDR
3	Chaque machine virtuelle	Ces adresses IP dépendent uniquement du nombre d'adresses IP VMs dans l'infrastructure.

Scénarios de consommation IP pour le réseau ODB

Dans le tableau suivant, vous pouvez voir les adresses IP consommées dans le réseau ODB pour différentes configurations de clusters de machines virtuelles. Alors que /28 est la plage d'adresse CIDR minimale technique pour que le sous-réseau client puisse déployer 1 cluster de machines virtuelles avec 2 VMs, nous vous recommandons d'utiliser au moins une plage d'adresses CIDR /27. Dans ce cas, la plage d'adresses IP n'est pas entièrement consommée par les clusters de machines virtuelles et permet l'allocation d'adresses IP supplémentaires.

Configuration	Client IPs consommé	Nombre IPs minimum de clients	Backup IPs consommé	Backup IPs minimum
1 cluster de machines	17 (6 services + 3 clusters + 4*2)	32 (plage CIDR /27)	9 (3 services + 3*2)	16 (plage CIDR 2/28)

Configuration	Client IPs consommé	Nombre IPs minimum de clients	Backup IPs consommé	Backup IPs minimum
virtuelles avec 2 VMs				
1 cluster de machines virtuelles avec 3 VMs	21 (6 services + 3 clusters + 4*3)	32 (plage CIDR /27)	12 (3 services + 3*3)	16 (plage CIDR 2/28)
1 cluster de machines virtuelles avec 4 VMs	25 (6 services + 3 clusters + 4*4)	32 (plage CIDR /27)	15 (3 services + 3*4)	16 (plage CIDR 2/28)
1 cluster de machines virtuelles avec 8 VMs	41 (6 services + 3 clusters + 4*8)	64 (plage CIDR 6/26)	27 (3 services + 3*8)	32 (plage CIDR /27)

Le tableau suivant indique le nombre d'instances de chaque configuration possibles en fonction d'une plage d'adresses CIDR client spécifique. Par exemple, 1 cluster de machines virtuelles avec 4 VMs consomme 24 adresses IP dans le sous-réseau client. Si la plage CIDR est de /25, 128 adresses IP sont disponibles. Ainsi, vous pouvez provisionner 5 clusters de machines virtuelles dans le sous-réseau.

Configuration du cluster de machines virtuelles	Numéro avec /27 (32 IPs)	Numéro avec /26 (64 IPs)	Numéro avec /25 (128 IPs)	Numéro avec /24 (256 IPs)	Numéro quand /23 (512 IPs)	Numéro quand /22 (1024 IPs)
1 cluster de machines virtuelles avec 2 VMs (16 IPs)	1	3	7	15	30	60

Configuration du cluster de machines virtuelles	Numéro avec /27 (32 IPs)	Numéro avec /26 (64 IPs)	Numéro avec /25 (128 IPs)	Numéro avec /24 (256 IPs)	Numéro quand /23 (512 IPs)	Numéro quand /22 (1024 IPs)
1 cluster de machines virtuelles avec 3 VMs (20 IPs)	1	3	6	12	24	48
1 cluster de machines virtuelles avec 4 VMs (24 IPs)	1	2	5	10	20	40
2 clusters de machines virtuelles de 2 VMs chacun (27 IPs)	1	2	4	9	18	36
2 clusters de machines virtuelles de 3 VMs chacun (35 IPs)	0	1	3	7	14	28
2 clusters de machines virtuelles de 4 VMs chacun (43 IPs)	0	1	2	5	11	23

Étape 1 : créer un réseau ODB dans Oracle Database@AWS

Un réseau ODB est un réseau privé isolé qui héberge l'infrastructure OCI dans une zone de disponibilité (AZ). Un réseau ODB et une infrastructure Oracle Exadata sont des conditions préalables au provisionnement de clusters de machines virtuelles et à la création de bases de données Exadata. Vous pouvez créer le réseau ODB et l'infrastructure Oracle Exadata dans l'un ou l'autre ordre. Pour plus d’informations, consultez Réseau ODB et Peering ODB.

Cette tâche suppose que vous avez luPlanification de l'espace d'adresse IP dans Oracle Database@AWS. Pour modifier ou supprimer le réseau ODB ultérieurement, voirGestion de la base de données Oracle@AWS.

Pour créer un réseau ODB

1. Connectez-vous à la Oracle Database@AWS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/odb/.
2. Choisissez votre AWS région en haut à droite. Pour de plus amples informations, veuillez consulter Régions prises en charge pour Oracle Database@AWS.
3. Dans le volet de gauche, choisissez ODB networks.
4. Choisissez Créer un réseau ODB.
5. Pour le nom du réseau ODB, entrez un nom de réseau. Le nom doit comporter de 1 à 255 caractères et commencer par un caractère alphabétique ou un trait de soulignement. Il ne peut pas contenir de tirets consécutifs.
6. Pour la zone de disponibilité, choisissez un nom AZ. Pour les informations prises en charge AZs, voirRégions prises en charge pour Oracle Database@AWS.
7. Pour le CIDR du sous-réseau client, spécifiez une plage d'adresses CIDR pour les connexions client. Pour de plus amples informations, veuillez consulter Exigences CIDR du sous-réseau client pour le réseau ODB.
8. Pour le CIDR du sous-réseau Backup, spécifiez une plage d'adresses CIDR pour les connexions de sauvegarde. Pour isoler le trafic de sauvegarde et améliorer la résilience, nous vous recommandons de ne pas superposer le CIDR de sauvegarde et le CIDR client. Pour de plus amples informations, veuillez consulter Exigences CIDR du sous-réseau de sauvegarde pour le réseau ODB.
9. Pour la configuration DNS, choisissez l'une des options suivantes :

   Par défaut

   Dans le champ Préfixe du nom de domaine, entrez un nom à utiliser comme préfixe pour votre domaine. Le nom de domaine est fixé comme oraclevcn.com. Par exemple, si vous entrez**`myhost`**, le nom de domaine complet est myhost.oraclevcn.com.

   Nom de domaine personnalisé

   Pour Nom de domaine, entrez un nom de domaine complet. Par exemple, vous pouvez saisir myhost.myodb.com.
10. (Facultatif) Pour les intégrations de services, sélectionnez un service à intégrer à votre réseau à l'aide de VPC Lattice. Oracle Database@AWS s'intègre Services AWS à divers outils afin de fournir des fonctionnalités et des options de connectivité améliorées pour vos bases de données Oracle. Sélectionnez l'une des intégrations suivantes :

Amazon S3

Activez l'accès direct au réseau ODB à Amazon S3. Vos bases de données peuvent accéder à S3 pour l'importation/exportation de données ou pour des sauvegardes personnalisées. Vous pouvez saisir une politique JSON. Pour de plus amples informations, veuillez consulter Sauvegardes gérées par l'utilisateur vers Amazon S3 dans Oracle Database@AWS.

Zéro-ETL

Activez l'analyse en temps réel et le machine learning sur les données transactionnelles à l'aide d'Amazon Redshift. Pour de plus amples informations, veuillez consulter Intégration d'Oracle Database@AWS Zero-ETL à Amazon Redshift.

> **Note**
>
> Lorsque vous créez votre réseau ODB, Oracle Database@ préconfigure AWS automatiquement l'accès au réseau pour les sauvegardes gérées par Oracle sur Amazon S3. Vous ne pouvez ni activer ni désactiver cette intégration. Pour de plus amples informations, veuillez consulter AWS intégrations de services.

11. (Facultatif) Dans le champ Tags, entrez jusqu'à 50 tags pour le réseau. Une balise est une paire clé-valeur que vous pouvez utiliser pour organiser et suivre vos ressources.
12. Choisissez Créer un réseau ODB.

Après avoir créé un réseau ODB, vous pouvez le relier à un VPC. Le peering ODB est une connexion réseau créée par l'utilisateur qui permet de router le trafic de manière privée entre un Amazon VPC et un réseau ODB. Après le peering, une EC2 instance Amazon au sein du VPC peut communiquer avec les ressources du réseau ODB comme si elles faisaient partie du même réseau. Pour de plus amples informations, veuillez consulter Configuration du peering ODB vers un Amazon VPC dans Oracle Database@AWS.

Étape 2 : créer une infrastructure Oracle Exadata dans Oracle Database@AWS

L'infrastructure Oracle Exadata est l'architecture sous-jacente des serveurs de base de données, des serveurs de stockage et des réseaux qui exécutent les bases de données Oracle Exadata.

Choisissez Exadata X9M ou X11M comme modèle de système. Vous pouvez ensuite créer des clusters de machines virtuelles sur l'infrastructure Exadata à l'aide de la AWS console.

Vous pouvez créer l'infrastructure Oracle Exadata et le réseau ODB dans l'un ou l'autre ordre. Il n'est pas nécessaire de spécifier les informations réseau lors de la création de l'infrastructure.

Vous ne pouvez pas modifier une infrastructure Oracle Exadata après l'avoir créée. Pour supprimer une infrastructure Exadata, voirSuppression d'une infrastructure Oracle Exadata dans Oracle Database@AWS.

Pour créer une infrastructure Exadata

1. Connectez-vous à la Oracle Database@AWS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/odb/.
2. Dans le volet de gauche, choisissez Exadata infrastructures.
3. Choisissez Create Exadata infrastructure.
4. Pour le nom de l'infrastructure Exadata, entrez un nom. Le nom doit comporter de 1 à 255 caractères et commencer par un caractère alphabétique ou un trait de soulignement. Il ne peut pas contenir de tirets consécutifs.
5. Pour la zone de disponibilité, choisissez l'une des zones prises en charge AZs. Ensuite, sélectionnez Suivant.
6. Pour le modèle de système Exadata, choisissez Exadata.X9M ou Exadata.X11M. Pour Exadata.X11M, choisissez également les types de serveurs suivants :

   - Pour le type de serveur de base de données, choisissez le type de modèle de serveur de base de données de votre infrastructure Exadata. Actuellement, le seul choix est X11M.
   - Pour le type de serveur de stockage, choisissez le type de modèle de serveur de stockage de votre infrastructure Exadata. Actuellement, le seul choix est le X11M-HC.
7. Pour les serveurs de base de données, conservez la valeur par défaut de 2 ou déplacez le curseur pour sélectionner jusqu'à 32 serveurs. Pour en spécifier plus de 2, demandez une augmentation de limite à OCI.

   Chaque serveur de base de données Exadata X9M en prend en charge 126. OCPUs Chaque serveur de base de données Exadata X11M prend en charge 760. ECPUs Le nombre total de calculs change à mesure que vous modifiez le nombre de serveurs. Pour plus d'informations sur OCPUs et ECPUs, voir Modèles de calcul dans une base de données autonome dans la documentation Oracle.

8. Pour les serveurs de stockage, conservez la valeur par défaut de 3 ou déplacez le curseur pour sélectionner jusqu'à 64 serveurs. Pour en spécifier plus de 3, demandez une augmentation de limite à OCI. Chaque serveur de stockage X9M fournit 64 To. Chaque serveur de stockage X11m fournit 80 To. Le nombre total de To de stockage change à mesure que vous modifiez le nombre de serveurs. Ensuite, sélectionnez Suivant.
9. Pour la fenêtre de maintenance, configurez à quel moment la maintenance du système peut avoir lieu :

    a. Pour les préférences de planification, sélectionnez l'une des options suivantes :

        - Calendrier géré par Oracle : Oracle détermine le moment optimal pour les activités de maintenance.
        - Calendrier géré par le client : vous spécifiez à quel moment les activités de maintenance peuvent avoir lieu.

    b. Pour le mode Patching, sélectionnez l'une des options suivantes :

        - Continuation : les mises à jour sont appliquées à un nœud à la fois, ce qui permet à la base de données de rester disponible pendant l'application des correctifs.
        - Non continu : les mises à jour sont appliquées simultanément à tous les nœuds, ce qui peut entraîner une interruption de service.

    c. Si vous avez sélectionné Planification gérée par le client, configurez les paramètres supplémentaires suivants :

        - Pour les mois de maintenance, sélectionnez les mois pendant lesquels la maintenance peut être effectuée.
        - Pour Semaine du mois, sélectionnez la semaine du mois où la maintenance peut être effectuée (première, deuxième, troisième, quatrième ou dernière).
        - Pour Jour de la semaine, sélectionnez le jour où la maintenance peut être effectuée (du lundi au dimanche).
        - Pour Heure de début, sélectionnez l'heure à laquelle la fenêtre de maintenance commence. L'heure est en UTC.
        - Pour le délai de notification, sélectionnez combien de jours à l'avance vous souhaitez être informé de la maintenance à venir.

> **Note**
>
> Oracle Cloud Infrastructure effectue la maintenance du système pendant cette fenêtre. Pendant la maintenance, votre infrastructure Exadata reste disponible, mais vous pouvez rencontrer de brèves périodes de latence plus élevée.

10. (Facultatif) Pour les contacts de notification de maintenance OCI, entrez jusqu'à 10 adresses e-mail. AWS transmet ces adresses e-mail à OCI. Lorsque des mises à jour sont effectuées, OCI envoie des notifications aux adresses répertoriées.
11. (Facultatif) Pour les balises, entrez jusqu'à 50 balises pour l'infrastructure. Une balise est une paire clé-valeur que vous pouvez utiliser pour organiser et suivre vos ressources.
12. Choisissez Next et passez en revue les paramètres de votre infrastructure.
13. Choisissez Create Exadata infrastructure.

Étape 3 : créer un cluster de machines virtuelles Exadata ou un cluster de machines virtuelles autonome dans Oracle Database@AWS

Un cluster de machines virtuelles Exadata est un ensemble de bases de données Oracle Exadata VMs sur lequel vous pouvez créer des bases de données Oracle Exadata. Vous créez les clusters de machines virtuelles sur l'infrastructure Exadata. Vous pouvez déployer plusieurs clusters de machines virtuelles avec différentes infrastructures Oracle Exadata dans le même réseau ODB. Vous avez un contrôle administratif total sur les bases de données que vous créez sur les clusters de machines virtuelles Exadata.

Un cluster de machines virtuelles autonomes est un pool préalloué de ressources de calcul et de stockage Oracle Exadata, virtualisé au niveau de la machine virtuelle, qui exécute des bases de données autonomes (ADB). Contrairement aux bases de données gérées par l'utilisateur que vous créez sur un cluster de machines virtuelles Exadata, une base de données autonome s'ajuste automatiquement, applique des correctifs et est gérée par Oracle plutôt que par un administrateur de base de données.

Tenez compte des limites suivantes lorsque vous créez des clusters de machines virtuelles :

- Vous pouvez déployer un cluster de machines virtuelles uniquement dans l'AZ où vous avez créé votre réseau ODB et votre infrastructure Oracle Exadata.
- Si vous ne partagez pas un cluster de machines virtuelles entre plusieurs comptes, il doit se trouver dans la même infrastructure Compte AWS que l'infrastructure Oracle Exadata. Si vous partagez AWS RAM un réseau ODB et une infrastructure Oracle Exadata à partir d'un AWS compte avec un compte fiable, ce dernier peut créer des clusters de machines virtuelles dans son propre compte.
- Vous ne pouvez déployer que des clusters de machines virtuelles sur votre réseau ODB. Aucune autre ressource n'est autorisée.
- Vous ne pouvez pas modifier l'allocation de stockage après avoir créé un cluster de machines virtuelles.

> **⚠ Important**
>
> Le processus de création peut prendre plus de 6 heures, selon la taille du cluster de machines virtuelles.

Exadata VM cluster

Pour créer un cluster de machines virtuelles Exadata

1. Connectez-vous à la Oracle Database@AWS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/odb/.
2. Dans le volet de gauche, choisissez Exadata VM clusters.
3. Choisissez Créer un cluster de machines virtuelles.
4. Pour le nom du cluster de machines virtuelles, entrez un nom. Le nom doit comporter de 1 à 255 caractères et commencer par un caractère alphabétique ou un trait de soulignement. Il ne peut pas contenir de tirets consécutifs.
5. (Facultatif) Pour le nom du cluster Grid Infrastructure, entrez une version de l'infrastructure Grid pour votre cluster de machines virtuelles qui correspond à la version de base de données Oracle que vous utilisez. Le nom doit comporter de 1 à 11 caractères et ne peut pas contenir de tirets.
6. Pour Fuseau horaire, entrez un fuseau horaire.

7. Pour les options de licence, choisissez Bring Your Own License (BYOL) ou License Included, puis choisissez Next. Cette licence est la licence OCI fournie par Oracle, et non une licence fournie par AWS.
8. Configurez les paramètres de l'infrastructure Exadata comme suit :

   a. Pour Infrastructure, choisissez ce qui suit :

      - Pour le nom de l'infrastructure Exadata, choisissez l'infrastructure à utiliser pour ce cluster de machines virtuelles.
      - Pour la version Grid Infrastructure, choisissez la version à utiliser pour ce cluster de machines virtuelles.
      - Pour la version de l'image Exadata, choisissez la version à utiliser pour ce cluster de machines virtuelles. Nous vous recommandons de choisir la version présentée, qui est la version la plus élevée disponible.

   b. Pour les serveurs de base de données, sélectionnez un ou plusieurs serveurs de base de données pour héberger votre cluster de machines virtuelles.

   c. Pour la configuration, procédez comme suit :

      - Choisissez le nombre de cœurs du processeur, la mémoire et le stockage local pour chaque machine virtuelle, ou acceptez les valeurs par défaut.
      - Choisissez la quantité totale de stockage Exadata pour le cluster de machines virtuelles ou acceptez la valeur par défaut.

   d. (Facultatif) Pour l'allocation de stockage, sélectionnez l'une des options suivantes :

      - Activer l'allocation de stockage pour les instantanés fragmentés d'Exadata
      - Activer l'allocation de stockage pour les sauvegardes locales

      L'allocation de stockage utilisable change au fur et à mesure que vous sélectionnez des options. Vous ne pourrez pas modifier cette allocation de stockage ultérieurement. Passez en revue votre sélection, puis choisissez Next.
9. Configurez la connectivité comme suit :

   a. Pour le réseau ODB, choisissez un réseau ODB existant.

   b. Dans le champ Préfixe du nom d'hôte, entrez un préfixe pour le cluster de machines virtuelles. Assurez-vous de ne pas inclure le nom de domaine. Le préfixe constitue la première partie du nom d'hôte du cluster de machines virtuelles Oracle Exadata.

> **Note**
>
> Le nom de domaine de l'hôte est fixé comme oraclevcn.com.

c. Pour le port de l'écouteur SCAN (TCP/IP), entrez un numéro de port pour l'accès TCP à l'écouteur à nom d'accès client unique (SCAN). Le port par défaut est 1521. Vous pouvez également saisir un port SCAN personnalisé compris entre 1024 et 8999, à l'exception des numéros de port suivants : 2484, 6100, 6200, 7060, 7070, 7085 et 7879. Ensuite, sélectionnez Suivant.

d. Pour les paires de clés SSH, entrez la partie clé publique d'une ou de plusieurs paires de clés utilisées pour l'accès SSH au cluster de machines virtuelles. Ensuite, sélectionnez Suivant.

10. (Facultatif) Choisissez les diagnostics et les balises comme suit :

    a. Choisissez d'activer ou non la collecte de diagnostics pour les événements de diagnostic, le moniteur de santé, les journaux d'incidents et les collectes de traces. Oracle peut utiliser ces informations de diagnostic pour identifier, suivre et résoudre les problèmes.

    b. Pour les balises, entrez jusqu'à 50 balises pour le cluster de machines virtuelles. Une balise est une paire clé-valeur que vous pouvez utiliser pour organiser et suivre vos ressources. Ensuite, sélectionnez Suivant.

11. Vérifiez vos paramètres. Choisissez ensuite Create VM cluster.

Autonomous VM cluster

Pour créer un cluster de machines virtuelles autonome

1. Connectez-vous à la Oracle Database@AWS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/odb/.
2. Dans le volet de gauche, choisissez Autonomous VM clusters.
3. Choisissez Créer un cluster de machines virtuelles autonome.
4. Pour le nom du cluster de machines virtuelles, entrez un nom. Le nom doit comporter de 1 à 255 caractères et commencer par un caractère alphabétique ou un trait de soulignement. Il ne peut pas contenir de tirets consécutifs.
5. Pour Fuseau horaire, entrez un fuseau horaire.

6. Pour les options de licence, choisissez Bring Your Own License (BYOL) ou License Included, puis choisissez Next. Cette licence est la licence OCI fournie par Oracle, et non une licence fournie par AWS.
7. Configurez les paramètres de l'infrastructure Exadata comme suit :

   a. Pour le nom de l'infrastructure Exadata, choisissez l'infrastructure à utiliser pour ce cluster de machines virtuelles autonomes.

   b. Pour les serveurs de base de données, sélectionnez un ou plusieurs serveurs de base de données pour héberger votre cluster de machines virtuelles autonomes.

   c. Pour la configuration, procédez comme suit :

      - Choisissez le nombre de cœurs ECPU par machine virtuelle, la mémoire de base de données par processeur, le stockage de base de données et le nombre maximum de bases de données de conteneurs autonomes ou acceptez les valeurs par défaut.
      - Choisissez la quantité totale de stockage Exadata pour le cluster de machines virtuelles autonomes ou acceptez la valeur par défaut.
8. Configurez la connectivité comme suit :

   a. Pour le réseau ODB, choisissez un réseau ODB existant.

   b. Pour le port du récepteur SCAN (TCP/IP), entrez un numéro de port pour le port (non TLS). Le port par défaut est 1521. Vous pouvez également saisir un port (TLS) compris entre 1024 et 8999, à l'exception des numéros de port suivants : 2484, 6100, 6200, 7060, 7070, 7085 et 7879. Ensuite, sélectionnez Suivant.

      Sélectionnez Activer l'authentification TLS mutuelle (MTLS) pour autoriser l'authentification TLS mutuelle.
9. (Facultatif) Choisissez les diagnostics et les balises comme suit :

   a. Choisissez de planifier la configuration des modifications dans le calendrier géré par Oracle ou dans le calendrier géré par le client. Si vous choisissez un calendrier géré par le client, définissez les mois de maintenance, les semaines du mois, le jour de la semaine et l'heure de début (UTC).

   b. Pour les balises, entrez jusqu'à 50 balises pour le cluster de machines virtuelles autonomes. Une balise est une paire clé-valeur que vous pouvez utiliser pour organiser et suivre vos ressources. Ensuite, sélectionnez Suivant.
10. Vérifiez vos paramètres. Choisissez ensuite Create Autonomous VM cluster.

Étape 4 : Création de bases de données Oracle Exadata dans Oracle Cloud Infrastructure

Dans Oracle Database@AWS, vous pouvez créer et gérer les ressources suivantes à l'aide de la AWS console, de la CLI ou APIs :

- réseaux ODB
- Infrastructure Oracle Exadata
- Clusters de machines virtuelles Exadata et clusters de machines virtuelles autonomes
- Connexions d'appairage ODB

Pour créer et gérer des bases de données Oracle Exadata sur l'infrastructure que vous avez créée, vous devez utiliser la console Oracle Cloud Infrastructure plutôt que le Oracle Database@AWS tableau de bord. Vous pouvez créer une base de données Exadata gérée par l'utilisateur sur un cluster de machines virtuelles Exadata et une base de données autonome sur un cluster de machines virtuelles Exadata autonome. Pour plus d'informations sur la création de bases de données Oracle dans OCI, voir Exadata Database dans la documentation Oracle Cloud Infrastructure.

Pour créer des bases de données Oracle Exadata

1. Connectez-vous à la Oracle Database@AWS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/odb/.
2. Dans le volet de gauche, choisissez Exadata VM clusters ou Autonomous VM clusters.
3. Choisissez un cluster de machines virtuelles pour voir la page de détails.
4. Choisissez Gérer dans OCI pour être redirigé vers la console Oracle Cloud Infrastructure.
5. Créez votre base de données Exadata ou votre base de données autonome gérée par l'utilisateur dans OCI.

Configuration du peering ODB vers un Amazon VPC dans Oracle Database@AWS

Le peering ODB est une connexion réseau créée par l'utilisateur qui permet de router le trafic de manière privée entre un Amazon VPC et un réseau ODB. Il existe une one-to-one relation entre un VPC et un réseau ODB. Après avoir créé une connexion d'appairage à l'aide de la console, de la CLI ou de l'API, veillez à mettre à jour vos tables de routage VPC et à configurer la résolution DNS. Pour un aperçu conceptuel du peering ODB, voir. Peering ODB

Création d'une connexion d'appairage ODB dans Oracle Database@AWS

Avec les connexions de peering ODB, vous pouvez établir une connectivité réseau privée entre votre infrastructure Oracle Exadata et les applications exécutées sur votre Amazon. VPCs Chaque connexion d'appairage ODB est une ressource distincte que vous pouvez créer, afficher et supprimer indépendamment du réseau ODB.

Lorsque vous créez une connexion d'appairage ODB, vous pouvez spécifier des plages d'adresses CIDR du réseau homologue. Cette technique limite l'accès au réseau aux sous-réseaux requis, réduit les cibles potentielles d'attaques et permet une segmentation du réseau plus granulaire pour répondre aux exigences de conformité.

Vous pouvez créer les types de connexions d'appairage ODB suivants :

Peering ODB sur un même compte

Vous pouvez créer une connexion d'appairage ODB entre un réseau ODB et un Amazon VPC dans le même compte. AWS

Peering ODB entre comptes

Vous pouvez créer une connexion d'appairage ODB entre un réseau ODB d'un compte et un Amazon VPC d'un autre compte, une fois que le réseau ODB a été partagé à l'aide de. AWS RAM Les comptes propriétaires de VPC peuvent gérer les plages d'adresses CIDR spécifiées dans la connexion d'appairage sans être également propriétaires du réseau ODB.

Il existe une relation 1:1 entre un VPC et un réseau ODB. Vous ne pouvez pas créer de connexion d'appairage ODB entre un VPC et plusieurs réseaux ODB ou entre un réseau ODB et plusieurs. VPCs

Console

1. Connectez-vous à la Oracle Database@AWS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/odb/.
2. Dans le volet de navigation, choisissez ODB peering connections.
3. Choisissez Créer une connexion d'appairage ODB.
4. (Facultatif) Pour le nom de peering ODB, entrez un nom unique pour votre connexion.
5. Pour le réseau ODB, choisissez le réseau ODB à associer.
6. Pour le réseau homologue, choisissez l'Amazon VPC à associer à votre réseau ODB.
7. (Facultatif) Pour le réseau homologue CIDRs, spécifiez des blocs CIDR supplémentaires provenant du VPC homologue qui peuvent accéder au réseau ODB. Si vous ne le spécifiez pas CIDRs, tous les CIDRs membres du VPC homologue sont autorisés à y accéder.
8. (Facultatif) Dans Tags, ajoutez une paire clé/valeur.
9. Choisissez Créer une connexion d'appairage ODB.

Après avoir créé une connexion d'appairage ODB, configurez vos tables de routage Amazon VPC pour acheminer le trafic vers le réseau ODB apparenté. Pour de plus amples informations, veuillez consulter Configuration des tables de routage VPC pour le peering ODB. Notez qu'Oracle Database@ configure AWS automatiquement les tables de routage du réseau ODB.

AWS CLI

Pour créer une connexion d'appairage ODB, utilisez la `create-odb-peering-connection` commande.

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

Pour limiter l'accès au réseau ODB à des plages CIDR spécifiques, utilisez le `--peer-network-cidrs-to-be-added` paramètre. Si vous ne spécifiez pas de plages CIDR, toutes les plages y ont accès.

```
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"
```

Pour répertorier vos connexions d'appairage ODB, utilisez la `list-odb-peering-connections` commande.

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

Pour obtenir des informations sur une connexion d'appairage ODB spécifique, utilisez la `get-odb-peering-connection` commande.

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

Mettre à jour une connexion d'appairage ODB

Vous pouvez mettre à jour une connexion d'appairage ODB existante pour ajouter ou supprimer un réseau homologue. CIDRs Vous contrôlez les sous-réseaux du VPC homologue qui ont accès à votre réseau ODB.

Console

1. Connectez-vous à la Oracle Database@AWS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/odb/.
2. Dans le volet de navigation, choisissez ODB peering connections.
3. Sélectionnez la connexion d'appairage ODB que vous souhaitez mettre à jour.
4. Choisissez Actions, puis choisissez Mettre à jour la connexion d'appairage.
5. Dans la CIDRs section Réseau homologue, ajoutez ou supprimez des blocs CIDR selon vos besoins :
   - Pour ajouter CIDRs, choisissez Ajouter un CIDR et entrez le bloc CIDR.
   - Pour supprimer CIDRs, cliquez sur le X à côté du bloc CIDR que vous souhaitez supprimer.
6. Choisissez Mettre à jour la connexion d'appairage.

AWS CLI

Pour ajouter un réseau homologue CIDRs à une connexion d'appairage ODB, spécifiez le paramètre `--peer-network-cidrs-to-be-added` dans la `update-odb-peering-connection` commande.

```
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"
```

Pour supprimer un réseau homologue CIDRs d'une connexion d'appairage ODB, spécifiez le paramètre `--peer-network-cidrs-to-be-removed` dans la `update-odb-peering-connection` commande.

```
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"
```

Configuration des tables de routage VPC pour le peering ODB

Une table de routage contient un ensemble de règles, appelées acheminements, qui déterminent la direction du trafic réseau à partir de votre sous-réseau ou de votre passerelle. Le CIDR de destination dans une table de routage est une plage d'adresses IP vers laquelle vous souhaitez que le trafic soit acheminé. Si vous avez spécifié un VPC pour l'appairage ODB vers votre réseau ODB, mettez à jour votre table de routage VPC avec la plage d'adresses IP de destination de votre réseau ODB. Pour plus d'informations sur le peering ODB, consultez. Peering ODB

Pour mettre à jour une table de routage, utilisez la AWS CLI `ec2 create-route` commande. Les exemples suivants mettent à jour les tables de routage Amazon VPC. Pour de plus amples informations, veuillez consulter Configuration des tables de routage VPC pour le 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
```

Les tables de routage réseau ODB sont automatiquement mises à jour avec le VPC. CIDRs Pour autoriser l'accès au réseau ODB uniquement à un sous-réseau spécifique CIDRs plutôt qu'à

l'ensemble CIDRs du VPC, vous pouvez spécifier un réseau homologue CIDRs lors de la création d'une connexion d'appairage ODB ou mettre à jour une connexion d'appairage ODB existante pour ajouter ou supprimer des plages d'adresses CIDR appairées. Pour plus d'informations, consultez Création d'une connexion d'appairage ODB dans Oracle Database@AWS et Mettre à jour une connexion d'appairage ODB.

Pour plus d'informations sur les tables de routage VPC, consultez les tables de routage de sous-réseaux dans le guide de l'utilisateur d'Amazon Virtual Private Cloud et ec2 create-route dans le Command Reference.AWS CLI

Configuration du DNS pour Oracle Database@AWS

Amazon Route 53 est un service Web de système de noms de domaine (DNS) hautement disponible et évolutif que vous pouvez utiliser pour le routage DNS. Lorsque vous créez une connexion d'appairage ODB entre votre réseau ODB et un VPC, vous avez besoin d'un mécanisme permettant de résoudre les requêtes DNS relatives aux ressources du réseau ODB depuis le VPC. Vous pouvez utiliser Amazon Route 53 pour configurer les ressources suivantes :

- Un point de terminaison sortant

  Le point de terminaison est requis pour envoyer des requêtes DNS au réseau ODB.
- Une règle de résolution

  Cette règle spécifie le nom de domaine des requêtes DNS que le résolveur Route 53 transmet au DNS pour le réseau ODB.

Comment fonctionne le DNS dans Oracle Database@AWS

Oracle Database@AWS gère automatiquement la configuration du système de noms de domaine (DNS) pour le réseau ODB. Pour le nom de domaine, vous pouvez soit spécifier un préfixe personnalisé pour le nom de domaine par défaut, `oraclevcn.com` soit un nom de domaine entièrement personnalisé. Pour de plus amples informations, veuillez consulter Étape 1 : créer un réseau ODB dans Oracle Database@AWS.

Lors Oracle Database@AWS du provisionnement d'un réseau ODB, il crée les ressources suivantes :

- Un réseau cloud virtuel (VCN) Oracle Cloud Infrastructure (OCI) avec les mêmes blocs CIDR que le réseau ODB

Ce VCN se trouve dans la location OCI liée au client. Il existe un mappage 1:1 entre un réseau ODB et un OCI VCN. Chaque réseau ODB est associé à un OCI VCN.

- Un résolveur DNS privé au sein de l'OCI VCN

  Ce résolveur DNS gère les requêtes DNS au sein de l'OCI VCN. L'automatisation OCI crée des enregistrements pour le cluster de machines virtuelles. Les scans utilisent le `*.oraclevcn.com` nom de domaine complet (FQDN).
- Un point d'écoute DNS au sein du VCN OCI pour le résolveur DNS privé

  Vous trouverez le point de terminaison d'écoute DNS sur la page des détails du réseau ODB de la Oracle Database@AWS console.

Configuration d'un point de terminaison sortant dans un réseau ODB dans Oracle Database@AWS

Un point de terminaison sortant permet d'envoyer des requêtes DNS depuis votre VPC vers un réseau ou une adresse IP. Le point de terminaison indique les adresses IP d'où proviennent les requêtes. Pour transférer les requêtes DNS de votre VPC vers votre réseau ODB, créez un point de terminaison sortant à l'aide de la console Route 53. Pour plus d'informations, consultez la section Transfert de requêtes DNS sortantes vers votre réseau.

Pour configurer un point de terminaison sortant dans un réseau ODB

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de gauche, sélectionnez Points de terminaison sortants.
3. Dans la barre de navigation, choisissez la région du VPC dans lequel vous souhaitez créer le point de terminaison sortant.
4. Choisissez Create outbound endpoint (Créer point de terminaison sortant).
5. Complétez la section Paramètres généraux pour les points de terminaison sortants comme suit :

   a. Choisissez un groupe de sécurité qui autorise la connectivité TCP et UDP sortante aux entités suivantes :

      - Adresses IP utilisées par les résolveurs pour les requêtes DNS sur votre réseau ODB
      - Ports utilisés par les résolveurs pour les requêtes DNS sur votre réseau ODB

b. Pour Endpoint Type (Type de point de terminaison), choisissez IPv4.

c. Pour Protocoles pour ce point de terminaison, choisissez Do53.

6. Dans les adresses IP, fournissez les informations suivantes :

- Spécifiez les adresses IP ou laissez le résolveur Route 53 choisir les adresses IP pour vous parmi les adresses disponibles dans le sous-réseau. Choisissez un minimum de 2 à un maximum de 6 adresses IP pour les requêtes DNS. Nous vous recommandons de choisir des adresses IP dans au moins deux zones de disponibilité différentes.
- Pour Sous-réseau, choisissez des sous-réseaux présentant les caractéristiques suivantes :
  - Tables de routage qui incluent des routes vers les adresses IP de l'écouteur DNS sur le réseau ODB
  - Listes de contrôle d'accès réseau (ACLs) qui autorisent le trafic UDP et TCP vers les adresses IP et les ports utilisés par les résolveurs pour les requêtes DNS sur le réseau ODB
  - Réseau autorisant ACLs le trafic provenant de résolveurs sur la plage de ports de destination 1024 à 65535

7. (Facultatif) Pour les balises, spécifiez les balises pour le point de terminaison.

8. Sélectionnez Soumettre.

Configuration d'une règle de résolution dans Oracle Database@AWS

Une règle de résolution est un ensemble de critères qui déterminent le mode d'acheminement des requêtes DNS. Réutilisez ou créez une règle qui spécifie le nom de domaine des requêtes DNS que le résolveur transmet au DNS pour le réseau ODB.

Utilisation d'une règle de résolution existante

Pour utiliser une règle de résolution existante, votre action dépend du type de règle :

Une règle pour le même domaine dans la même AWS région que le VPC de votre Compte AWS

Associez la règle à votre VPC au lieu de créer une nouvelle règle. Choisissez la règle dans le tableau de bord des règles et associez-la à celle applicable VPCs dans la AWS région.

Une règle pour le même domaine dans la même région que votre VPC mais dans un compte différent

AWS Resource Access Manager Utilisez-le pour partager la règle entre le compte distant et le vôtre. Lorsque vous partagez une règle, vous partagez également le point de terminaison sortant

correspondant. Après avoir partagé la règle avec votre compte, choisissez-la dans le tableau de bord des règles et associez-la VPCs à celle de votre compte. Pour plus d'informations, consultez la section Gestion des règles de transfert.

Création d'une nouvelle règle de résolution

Si vous ne pouvez pas réutiliser une règle de résolution existante, créez-en une nouvelle à l'aide de la console Amazon Route 53.

Pour créer une nouvelle règle de résolution

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de gauche, sélectionnez Règles.
3. Dans la barre de navigation, choisissez la région du VPC où se trouve le point de terminaison sortant.
4. Choisissez Créer une règle.
5. Complétez les sections relatives à la règle pour le trafic sortant comme suit :
   a. Pour Type de règle, choisissez Règle directe.
   b. Pour Nom de domaine, spécifiez le nom de domaine complet du réseau ODB.
   c. Pour VPCs cela, utilisez cette règle, associez-la au VPC à partir duquel les requêtes DNS sont transmises à votre réseau ODB.
   d. Pour Point de terminaison sortant, choisissez le point de terminaison sortant que vous avez créé dans. Configuration d'un point de terminaison sortant dans un réseau ODB dans Oracle Database@AWS

   > **Note**
   >
   > Le VPC associé à cette règle ne doit pas nécessairement être le même que celui dans lequel vous avez créé le point de terminaison sortant.

6. Complétez la section Adresses IP cibles comme suit :
   a. Pour l'adresse IP, spécifiez l'adresse IP de l'écouteur DNS sur votre réseau ODB.
   b. Pour Port, spécifiez 53. Il s'agit du port utilisé par le résolveur pour les requêtes DNS.

> **Note**
>
> Le résolveur Route 53 transmet les requêtes DNS qui correspondent à cette règle et proviennent d'un VPC associé à cette règle au point de terminaison sortant référencé. Ces requêtes sont transmises aux adresses IP cibles que vous spécifiez dans les adresses IP cibles.

c. Pour le protocole de transmission, choisissez Do53.

7. (Facultatif) Pour les balises, spécifiez les balises pour la règle.
8. Sélectionnez Soumettre.

Test de votre configuration DNS dans Oracle Database@AWS

Après avoir créé votre point de terminaison sortant et votre règle de résolution, testez pour vous assurer que le DNS est correctement résolu. À l'aide d'une EC2 instance Amazon dans le VPC de votre application, effectuez une résolution DNS comme suit :

Pour Linux ou macOS

Utilisez une commande du formulaire`dig` *`record-name record-type`*.

Pour Windows

Utilisez une commande du formulaire`nslookup -type=`*`record-name record-type`*.

Configuration des passerelles de transit Amazon VPC pour Oracle Database@AWS

Amazon VPC Transit Gateways est un hub de transit réseau qui interconnecte des clouds privés virtuels (VPCs) et des réseaux sur site. Chaque VPC de l' hub-and-spokearchitecture peut se connecter à la passerelle de transit pour accéder aux autres VPC connectés. VPCs AWS Transit Gateway prend en charge le trafic pour les deux IPv4 et IPv6.

En Oracle Database@AWS, un réseau ODB prend en charge une connexion d'appairage avec un seul VPC. Si vous connectez une passerelle de transit à un VPC connecté à un réseau ODB, vous pouvez en connecter plusieurs VPCs à cette passerelle. Les applications exécutées dans

ces différents environnements VPCs peuvent accéder à un cluster de machines virtuelles Exadata exécuté sur votre réseau ODB.

Le schéma suivant montre une passerelle de transit connectée à deux réseaux locaux VPCs et à un réseau local.

Dans le schéma précédent, un VPC est relié à un réseau ODB. Dans cette configuration, le réseau ODB peut acheminer le trafic vers toutes les personnes VPCs rattachées à la passerelle de transit. La table de routage de chaque VPC inclut à la fois la route locale et les routes qui envoient le trafic destiné au réseau ODB vers la passerelle de transit.

Dans AWS Transit Gateway, vous êtes facturé en fonction du nombre de connexions que vous effectuez avec la passerelle de transit par heure et du volume de trafic qui y circule AWS Transit Gateway. Pour plus d'informations sur les coûts, consultez la section AWS Transit Gateway tarification.

Exigences

Assurez-vous que votre Oracle Database@AWS environnement répond aux exigences suivantes :

- Le VPC connecté à votre réseau ODB doit se trouver dans le même. Compte AWS Si le VPC apparenté se trouve sur un compte différent de celui du réseau ODB, les connexions à la passerelle de transit échouent quelles que soient les configurations de partage.
- Le VPC connecté à votre réseau ODB doit être connecté à une passerelle de transit.

> **Note**
>
> Si la passerelle de transit est configurée pour le partage, elle peut résider dans n'importe quel compte. Ainsi, la passerelle elle-même n'a pas besoin d'être dans le même compte que le réseau VPC et ODB.

- La pièce jointe de la passerelle de transit doit se trouver dans la même zone de disponibilité (AZ) que le réseau ODB.

Limitations

Notez les limites suivantes des passerelles Amazon VPC Transit pour : Oracle Database@AWS

- Amazon VPC Transit Gateways ne propose pas d'intégration native pour utiliser un réseau ODB en tant que pièce jointe. Par conséquent, les fonctionnalités VPC telles que les suivantes ne sont pas disponibles :
  - Résolution des noms d'hôte DNS publics en adresses IP privées
  - Notification d'événement pour les modifications de la topologie du réseau ODB, du routage et de l'état de connexion
- Le trafic de multidiffusion vers le réseau ODB n'est pas pris en charge.

Mise en place et configuration d'une passerelle de transit

Vous créez et configurez une passerelle de transit à l'aide de la console ou `aws ec2` des commandes Amazon VPC. La procédure suivante suppose qu'aucun réseau ODB n'est connecté à un VPC dans votre. Compte AWS Si un réseau ODB et un VPC sont déjà connectés à votre compte, ignorez les étapes 1 à 3.

> **Note**
>
> Si vous attachez ou reconnectez les pièces jointes à votre VPC, assurez-vous de saisir à nouveau les plages CIDR sur le réseau ODB ODB.

Pour installer et configurer une passerelle de transit pour Oracle Database@AWS

1. Créez un réseau ODB. Pour de plus amples informations, veuillez consulter Étape 1 : créer un réseau ODB dans Oracle Database@AWS.
2. Créez un VPC en utilisant le même compte que celui qui contient le réseau ODB. Pour plus d'informations, consultez la section Créer un VPC dans le guide de l'utilisateur Amazon VPC.
3. Créez une connexion d'appairage ODB entre votre réseau ODB et votre VPC. Pour de plus amples informations, veuillez consulter Configuration du peering ODB vers un Amazon VPC dans Oracle Database@AWS.
4. Configurez une passerelle de transit en suivant les étapes décrites dans Commencer à utiliser Amazon VPC Transit Gateways. La passerelle doit se trouver dans le même emplacement Compte AWS que le réseau ODB et le VPC, ou être partagée par un autre compte.

> **Important**
>
> Créez la pièce jointe de passerelle de transit dans la même zone AZ que le réseau ODB.

5. Ajoutez des plages CIDR à votre réseau ODB pour les réseaux locaux VPCs et ceux que vous souhaitez rattacher à votre réseau principal. Pour de plus amples informations, veuillez consulter Mettre à jour un réseau ODB dans Oracle Database@AWS.

   Si vous utilisez la CLI, exécutez la commande `update-odb-network` avec `--peered-cidrs-to-be-added` et`--peered-cidrs-to-be-removed`. Pour plus d'informations, consultez la référence de la commande AWS CLI.

Configuration du AWS Cloud WAN pour Oracle Database@AWS

AWS Le Cloud WAN est un service de réseau étendu (WAN) géré. Vous pouvez utiliser AWS le Cloud WAN pour créer, gérer et surveiller un réseau mondial unifié qui connecte les ressources réparties entre votre cloud et vos environnements sur site.

Dans AWS le Cloud WAN, un réseau mondial est un réseau privé unique qui fait office de conteneur de haut niveau pour vos objets réseau. Un réseau central est la partie de votre réseau mondial gérée par AWS.

AWS Le cloud WAN offre les principaux avantages suivants :

- Gestion centralisée du réseau qui simplifie les opérations tout en préservant la sécurité dans plusieurs régions
- Réseaux centraux avec segmentation intégrée pour isoler le trafic via plusieurs domaines de routage
- Support des politiques visant à automatiser la gestion du réseau et à définir des configurations cohérentes sur l'ensemble de votre réseau mondial

Dans Oracle Database@AWS, un réseau ODB prend en charge le peering vers un seul VPC. Si vous connectez un réseau central AWS Cloud WAN à un VPC pair, cela permet le routage du trafic mondial. Les applications connectées dans plusieurs VPCs régions peuvent accéder aux clusters de machines virtuelles Exadata de votre réseau ODB. Vous pouvez isoler le trafic réseau ODB dans son propre segment ou autoriser l'accès à d'autres segments.

Le schéma suivant montre un réseau central AWS Cloud WAN connecté à trois réseaux locaux VPCs et à un réseau local.

AWS Le Cloud WAN ne propose pas d'intégration native pour utiliser un réseau ODB en tant que pièce jointe. Par conséquent, les fonctionnalités VPC telles que les suivantes ne sont pas disponibles :

- Résolution des noms d'hôte DNS publics en adresses IP privées
- Notification d'événement pour les modifications de la topologie du réseau ODB, du routage et de l'état de connexion

Dans AWS le Cloud WAN, les frais suivants vous sont facturés à l'heure :

- Nombre de régions (limites du réseau principal)
- Nombre de connexions au réseau central
- La quantité de trafic qui traverse votre réseau principal via les pièces jointes

Pour obtenir des informations détaillées sur les tarifs, consultez la section Tarification du AWS Cloud WAN.

Pour configurer un réseau central pour Oracle Database@AWS

1. Ajoutez des plages CIDR à votre réseau ODB pour les réseaux locaux VPCs et ceux que vous souhaitez rattacher à votre réseau principal. Pour de plus amples informations, veuillez consulter Mettre à jour un réseau ODB dans Oracle Database@AWS.

   > **Note**
   >
   > Si vous attachez ou reconnectez les pièces jointes à votre VPC, assurez-vous de saisir à nouveau les plages CIDR sur le réseau ODB ODB.

2. Suivez les étapes décrites dans Créer un réseau mondial et un réseau central AWS Cloud WAN.

Partage des droits dans Oracle Database@AWS

Avec Oracle Database@AWS, vous pouvez partager les droits relatifs à Oracle Database@AWS sur le AWS Marketplace au sein d'une même organisation. Comptes AWS AWS Cela permet aux autres comptes de fournir leur propre infrastructure Oracle Exadata et leurs propres ressources réseau ODB à l'aide de votre abonnement.

Méthodes de partage

Oracle Database@AWS prend en charge deux méthodes de partage :

Partage des droits avec AWS License Manager

- Donnez à d'autres comptes la possibilité de fournir leur propre infrastructure Oracle Exadata et leurs propres ressources réseau ODB
- Chaque compte fonctionne de manière indépendante avec un contrôle complet du cycle de vie des ressources
- Idéal pour permettre le provisionnement en libre-service entre les équipes ou les unités commerciales

Partage de ressources avec AWS Resource Access Manager (AWS RAM)

- Partagez l'infrastructure Oracle Exadata et les ressources du réseau ODB déjà provisionnées
- Centralisez la gestion de l'infrastructure tout en permettant aux comptes destinataires de créer des clusters de machines virtuelles
- Optimisez les coûts en faisant en sorte que plusieurs comptes utilisent la même infrastructure

Vous pouvez utiliser les deux méthodes de partage simultanément en fonction des besoins de votre organisation.

Limitations relatives au partage des droits dans Oracle Database@AWS

Lorsque vous partagez des AWS droits Oracle Database@, gardez à l'esprit les limites suivantes :

- Vous ne pouvez partager qu'avec les Comptes AWS membres de votre AWS organisation
- Vous ne pouvez pas partager avec l'ensemble d'une unité organisationnelle (UO) ou avec l'ensemble de l'organisation
- Un compte ne peut bénéficier des droits que d'un seul compte acheteur (d'une offre privée)
- Un compte acheteur ne peut pas partager ses droits avec un autre compte acheteur
- Les comptes des destinataires doivent initialiser le AWS service Oracle Database@ avant de pouvoir utiliser les droits partagés
- Les opérations d'octroi de droits ne peuvent être effectuées que depuis la région de l'est des États-Unis (Virginie du Nord)

Partage des AWS droits Oracle Database@ entre les comptes

Pour permettre la collaboration tout en optimisant les coûts, partagez les AWS droits Oracle Database@ avec d'autres personnes Comptes AWS au sein de la même organisation. AWS Cette rubrique explique comment partager des droits à l'aide de AWS License Manager.

Conditions préalables au partage des droits

Avant de partager les AWS droits Oracle Database@, assurez-vous que vous disposez des éléments suivants :

- Un AWS abonnement Oracle Database@ actif (vous devez être le compte acheteur ayant accepté l'offre privée) AWS Marketplace
- Le IDs nombre de AWS comptes de votre organisation avec lesquels vous souhaitez partager des droits
- Autorisations nécessaires pour que le concédant et le bénéficiaire puissent utiliser les ressources et les opérations du AWS License Manager (pour plus d'informations, voir Gestion des identités et des accès pour License Manager dans le Guide de l'utilisateur du AWS License Manager)
- Autorisations répertoriées ci-dessous pour vous (donateur) et le bénéficiaire des droits (bénéficiaire)

Autorisations requises pour le partage des droits

Outre les autorisations AWS License Manager, Oracle Database@AWS nécessite les autorisations suivantes :

Autorisations du concédant

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

Autorisations du bénéficiaire

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

Partage des AWS droits Oracle Database@ avec un autre compte à l'aide de License Manager AWS

Pour partager des droits avec un autre AWS compte, vous devez créer une licence à l'aide de AWS License Manager. Pour plus d'informations, consultez la section Distribute License Manager des droits du License Manager dans le Guide de l'utilisateur du AWS License Manager.

Après avoir créé la subvention, le bénéficiaire (bénéficiaire) doit :

- Acceptez et activez la subvention. Pour plus d'informations, consultez la section Acceptation et activation des autorisations dans le License Manager dans le Guide de l'utilisateur du AWS License Manager.
- Suivez les instructions d'initialisation d'Oracle AWS Database@.

Une fois l'initialisation terminée, le bénéficiaire peut provisionner les AWS ressources Oracle Database@ en utilisant les droits partagés.

Partage de ressources dans Oracle Database@AWS

Avec Oracle Database@AWS, vous pouvez partager l'infrastructure Exadata et votre réseau ODB entre plusieurs Comptes AWS membres d'une même organisation. AWS Cela vous permet de provisionner l'infrastructure une seule fois et de la réutiliser sur des comptes fiables, ce qui vous permet de réduire les coûts tout en séparant les responsabilités.

Lorsque vous partagez des ressources :

- Le compte propriétaire de la ressource (compte propriétaire) garde le contrôle sur le cycle de vie de la ressource.
- Les comptes qui ont accès à des ressources partagées (comptes fiables) peuvent consulter et utiliser ces ressources en fonction des autorisations accordées.
- Les comptes fiables peuvent créer leurs propres ressources sur une infrastructure partagée, mais ne peuvent pas supprimer les ressources partagées sous-jacentes.

Intégration d'Oracle Database@AWS avec AWS RAM

Oracle Database@AWS utilise AWS Resource Access Manager (AWS RAM) pour permettre un partage sécurisé et contrôlé des ressources entre les comptes. Vous pouvez AWS RAM ainsi partager en toute sécurité vos AWS ressources Oracle Database@ entre plusieurs AWS comptes au sein d'une même AWS organisation. AWS RAM simplifie le partage des ressources, réduit les frais opérationnels et assure la sécurité et la visibilité des ressources Oracle Database@AWS partagées.

Avec AWS RAM, vous partagez les ressources que vous possédez en créant un partage de ressources. Un partage de ressources indique les ressources à partager et les personnes Comptes AWS avec lesquelles elles doivent être partagées.

Avantages du partage des ressources dans Oracle Database@AWS

Le partage des AWS ressources Oracle Database@ entre les comptes offre les avantages suivants :

- Optimisation des coûts — Provisionnez une infrastructure Exadata coûteuse une seule fois via un compte administratif et partagez-la avec plusieurs comptes, réduisant ainsi les coûts globaux.

- Séparation des responsabilités : maintenez des limites claires entre les administrateurs de l'infrastructure et les utilisateurs de bases de données tout en permettant la collaboration.
- Gestion simplifiée : centralisez le provisionnement et la gestion de l'infrastructure tout en permettant des opérations de base de données distribuées.
- Gouvernance cohérente : appliquez des politiques et des contrôles cohérents sur l'ensemble des ressources partagées.

Par exemple, un administrateur peut provisionner l'infrastructure Oracle Exadata et le réseau ODB dans ses comptes Compte AWS et les partager avec des comptes de développeurs. Les développeurs peuvent ensuite créer des clusters de machines virtuelles sur cette infrastructure partagée sans avoir à provisionner leur propre matériel coûteux. Cette approche réduit considérablement les coûts tout en maintenant une séparation adéquate des responsabilités entre les comptes.

Comment fonctionne le partage des ressources dans Oracle Database@AWS

Vous pouvez partager les ressources Oracle Database@AWS suivantes :

- Infrastructure Oracle Exadata
- Réseau ODB

Oracle Database@AWS partage les ressources précédentes selon le processus suivant :

1. Le compte acheteur (le compte qui accepte l'offre AWS privée d'Oracle Database@ via AWS Marketplace) fournit des AWS ressources Oracle Database@, telles que l'infrastructure Exadata et un réseau ODB.
2. Le compte acheteur crée un partage de ressources en utilisant AWS RAM, en spécifiant les ressources à partager et les comptes fiables avec lesquels les partager.
3. Les partages de ressources pour les comptes fiables au sein d'une même organisation sont automatiquement acceptés.
4. Avant d'utiliser des ressources partagées, les comptes approuvés doivent initialiser le AWS service Oracle Database@ dans leur compte en utilisant la `aws odb initialize-service` commande ou en choisissant Activer le compte dans la console Oracle Database@.AWS

5. Après l'initialisation, les comptes fiables peuvent créer leurs propres ressources sur l'infrastructure partagée, telles que des clusters de machines virtuelles sur une infrastructure Exadata partagée et un réseau ODB.

Autorisations sur les ressources partagées pour les comptes fiables

Lorsque vous partagez des ressources, Oracle Database@ sélectionne AWS automatiquement des actions spécifiques (autorisations gérées) pour chaque type de ressource :

Pour l'infrastructure Exadata

Oracle Database@AWS accorde les autorisations suivantes aux comptes approuvés :

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

Pour le réseau ODB

Les autorisations suivantes sont accordées aux comptes de confiance :

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

Le partage des ressources respecte la nature hiérarchique des ressources Oracle Database@AWS . Par exemple, si vous partagez l'infrastructure Exadata, les comptes fiables peuvent créer des

clusters de machines virtuelles sur cette infrastructure, mais ils ne peuvent ni modifier ni supprimer l'infrastructure Exadata elle-même.

Lorsqu'une ressource n'est pas partagée, les comptes de confiance perdent la possibilité de créer de nouvelles ressources sur l'infrastructure partagée. Cependant, toutes les ressources qu'ils ont déjà créées restent accessibles et fonctionnelles.

Limitations du partage des ressources Oracle Database@AWS

Avant de partager des ressources, gardez à l'esprit les limites suivantes.

Limites relatives au partage des ressources

Lorsque vous partagez des AWS ressources Oracle Database@, gardez à l'esprit les limites suivantes :

- Vous ne pouvez partager des ressources qu'avec Compte AWS IDs.
- Vous ne pouvez partager des ressources qu'au Comptes AWS sein d'une même AWS organisation.
- Vous partagez des ressources au sein d'une AWS région spécifique. Pour partager des ressources entre régions, vous devez créer des partages de ressources distincts dans chaque région.
- Lorsque vous créez un partage de ressources, les actions (autorisations gérées) pour chaque type de ressource sont automatiquement sélectionnées et ne peuvent pas être modifiées.
- Vous ne pouvez pas utiliser Oracle Database@AWS comme ressource et la partager avec d'autres personnes. Comptes AWS
- Un compte sécurisé ne peut utiliser les ressources partagées qu'à partir d'un seul compte acheteur (provenant d'une offre privée). Ainsi, deux comptes acheteurs ne peuvent pas partager des ressources avec le même compte de confiance.
- Un compte acheteur ne peut pas partager de ressources avec un autre compte acheteur.
- Les ressources partagées avec un compte fiable doivent d'abord être partagées par le compte acheteur dans la région d'origine de l'acheteur.
- Lorsque vous annulez le partage d'une ressource, nous vous recommandons d'attendre environ 15 minutes avant de partager à nouveau la même ressource avec le même compte approuvé.

Limites relatives à la création et à l'utilisation de ressources partagées

Lorsque vous créez ou utilisez des AWS ressources Oracle Database@, gardez à l'esprit les limites suivantes :

- Seul le compte acheteur peut créer une infrastructure Exadata et des ressources réseau ODB. Le compte acheteur est celui qui accepte l'offre AWS privée d'Oracle Database@.
- Les comptes de confiance peuvent créer des ressources uniquement sur l'infrastructure Exadata partagée par le compte acheteur.
- Les comptes approuvés doivent initialiser le AWS service Oracle Database@ dans leur compte avant de pouvoir utiliser des ressources partagées.

Limitations relatives à la suppression de ressources partagées

- Vous ne pouvez pas supprimer une infrastructure Exadata contenant des clusters de machines virtuelles créés par des comptes fiables tant que ces clusters de machines virtuelles ne sont pas supprimés.
- Vous ne pouvez pas supprimer un réseau ODB doté d'une connexion d'appairage ODB créée par un compte de confiance tant que la connexion d'appairage ODB n'a pas été supprimée.
- Le compte acheteur ne peut pas supprimer les AWS ressources Oracle Database@ créées par des comptes approuvés.
- Les comptes approuvés peuvent consulter les ressources partagées, mais ne peuvent pas modifier ou supprimer les AWS ressources Oracle Database@ détenues par le compte acheteur.

Partage Oracle Database@AWS des ressources entre les comptes

Pour permettre la collaboration tout en optimisant les coûts, partagez les AWS ressources Oracle Database@ avec d'autres personnes Comptes AWS au sein de la même AWS organisation. Cette rubrique explique comment partager des ressources à l'aide de AWS Resource Access Manager (AWS RAM).

Rubriques

- Conditions préalables au partage des ressources
- Partage de AWS ressources Oracle Database@ avec un autre compte en utilisant AWS RAM
- Afficher vos partages de ressources

- Mettre à jour ou supprimer des partages de ressources à l'aide AWS RAM

Conditions préalables au partage des ressources

Avant de partager les AWS ressources Oracle Database@, assurez-vous que vous disposez des éléments suivants :

- Un AWS abonnement Oracle Database@ actif (vous devez être le compte acheteur qui a accepté l'offre privée) AWS Marketplace
- Le IDs ou les noms des ressources que vous souhaitez partager, telles que l'infrastructure Exadata ou les réseaux ODB
- Le IDs nombre de AWS comptes de votre organisation avec lesquels vous souhaitez partager des ressources
- Autorisations nécessaires pour créer des partages de ressources dans AWS RAM
- Possibilité de partager des ressources en AWS Organizations utilisant AWS RAM (pour plus d'informations, voir Activer le partage des ressources AWS Organizations dans le Guide de AWS Resource Access Manager l'utilisateur)

Partage de AWS ressources Oracle Database@ avec un autre compte en utilisant AWS RAM

Pour partager une infrastructure Exadata ou un réseau ODB avec un autre AWS compte, vous créez un partage de ressources à l'aide de. AWS RAM Cela permet au compte de confiance de créer des clusters de machines virtuelles sur votre infrastructure Exadata.

Console

1. Ouvrez la AWS RAM console à l'adresse https://console.aws.amazon.com/ram/.
2. Choisissez Créer une ressource.
3. Dans Nom, entrez un nom descriptif pour votre partage de ressources.
4. Sous Sélectionner le type de ressource, l'une des ressources suivantes :
    - Réseau Oracle Database@ ODB AWS
    - Base de données Oracle et infrastructure Exadata AWS

5. Sélectionnez les ressources d'infrastructure Exadata que vous souhaitez partager. Choisissez Next jusqu'à ce que vous arriviez à Accorder l'accès aux principaux.
6. Sous Principaux, choisissez Comptes AWS, puis entrez le AWS compte avec IDs lequel vous souhaitez partager.
7. Sous Autorisations gérées, sélectionnez les autorisations suivantes pour autoriser le compte de confiance à créer des clusters de machines virtuelles sur l'infrastructure Exadata partagée :
   - AWSRAMDefaultAutorisationODBNetwork
   - AWSRAMDefaultAutorisationODBCloudExadataInfrastructure
8. Choisissez Créer une ressource.

AWS CLI

Pour partager des ressources à l'aide de AWS CLI, utilisez la `aws ram create-resource-share` commande. L'exemple suivant crée un partage de ressources nommé `ExadataInfraShare` qui partage l'infrastructure Exadata spécifiée avec le compte 222222222222, permettant à ce compte de créer des clusters de machines virtuelles sur l'infrastructure partagée.

```
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
```

Afficher vos partages de ressources

Pour consulter les ressources que vous avez partagées et les comptes avec lesquels vous les avez partagées :

Console

1. Ouvrez la AWS RAM console à l'adresse https://console.aws.amazon.com/ram/.
2. Choisissez Ressources partagées pour afficher les ressources que vous avez partagées avec d'autres comptes.
3. Sélectionnez un partage de ressources pour en afficher les détails, notamment les ressources partagées et les principaux partenaires avec lesquels elles sont partagées.

AWS CLI

Pour afficher vos partages de ressources à l'aide de AWS CLI, utilisez la `get-resource-shares` commande :

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

Pour afficher les ressources d'un partage de ressources spécifique, utilisez la `list-resources` commande :

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

Pour afficher les principaux (comptes) avec lesquels un partage de ressources est partagé, utilisez la `list-principals` commande :

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

Mettre à jour ou supprimer des partages de ressources à l'aide AWS RAM

Pour arrêter de partager une ressource avec un compte de confiance AWS RAM, effectuez l'une des actions suivantes :

- Supprimez la ressource du partage de ressources.
- Supprimez le compte de confiance du partage de ressources.
- Supprimez le partage de ressources.

Avant de révoquer l'accès à une ressource partagée ou de la supprimer, tenez compte des implications suivantes :

- Les comptes fiables ne peuvent plus créer de nouvelles ressources sur l'infrastructure non partagée.
- Les ressources existantes créées par des comptes fiables sur l'infrastructure partagée d'Exadata continuent de fonctionner et restent accessibles à ceux-ci Comptes AWS.

- Vous ne pouvez pas supprimer une infrastructure Exadata contenant des clusters de machines virtuelles créés par des comptes fiables tant que ces clusters de machines virtuelles ne sont pas supprimés.

Avant de mettre fin au partage des ressources, nous vous recommandons de vous coordonner avec les comptes de confiance afin de garantir une transition harmonieuse.

Pour plus d'informations, voir Mettre à jour un partage de ressources dans AWS RAM et Supprimer un partage de ressources AWS RAM dans le Guide de AWS Resource Access Manager l'utilisateur.

Initialisation Oracle Database@AWS dans un compte sécurisé

Un compte fiable est un compte Compte AWS que vous désignez comme éligible pour recevoir des partages de ressources. Il doit s'agir d'une autre personne Compte AWS de votre AWS organisation. Avant de pouvoir utiliser les AWS ressources Oracle Database@ partagées dans un compte sécurisé, vous devez initialiser le service. L'initialisation crée les métadonnées nécessaires et établit la connexion entre votre infrastructure cloud Compte AWS et Oracle.

Rubriques

- Qu'est-ce que l'initialisation d'Oracle Database@ ?AWS
- Étapes suivantes

Qu'est-ce que l'initialisation d'Oracle Database@ ?AWS

Une fois qu'une ressource a été partagée avec votre compte, vous devez initialiser le AWS service Oracle Database@ avant de pouvoir accéder à la ressource partagée ou de l'utiliser. Si vous essayez d'utiliser Oracle Database@AWS APIs sans avoir préalablement initialisé le service, vous recevez un message d'erreur.

L'initialisation est un processus ponctuel. Il crée les métadonnées nécessaires et établit une connexion entre votre infrastructure cloud Compte AWS et Oracle.

Vous pouvez initialiser le service à l'aide de la console AWS de gestion ou du AWS CLI.

Console

1. Ouvrez la AWS console Oracle Database@ à l'adresse. https://console.aws.amazon.com/odb/

2. Si c'est la première fois que vous accédez à la AWS console Oracle Database@ avec ce compte, une page de bienvenue s'affiche.
3. Choisissez Activer le compte.
4. Le processus d'initialisation du service commence. Ce processus peut prendre quelques minutes.
5. Actualisez régulièrement la page d'accueil jusqu'à ce que le bouton Activer le compte devienne le bouton Tableau de bord.
6. Choisissez Dashboard pour commencer à utiliser Oracle Database@AWS.

AWS CLI

Pour initialiser Oracle Database@AWS dans votre compte de confiance à l'aide de AWS CLI, utilisez la commande. `initialize-service`

```
aws odb initialize-service
```

Pour vérifier l'état d'initialisation, utilisez la `get-oci-onboarding-status` commande.

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

Lorsque l'initialisation est terminée, le résultat affiche un statut de`ACTIVE_LIMITED`, indiquant que votre compte peut accéder aux ressources partagées mais ne peut pas créer une nouvelle infrastructure Exadata ou un nouveau réseau ODB.

Étapes suivantes

Après avoir initialisé Oracle Database@AWS dans votre compte de confiance, vous pouvez effectuer les opérations suivantes :

- Affichez les ressources partagées à l'aide `list` des `get` commandes et ou dans la AWS console.
- Créez des clusters de machines virtuelles et des clusters de machines virtuelles autonomes sur une infrastructure Exadata partagée et un réseau ODB.
- Créez une connexion d'appairage ODB sur un réseau ODB partagé.

Pour plus d'informations sur l'utilisation de ressources partagées, consultezUtilisation de Oracle Database@AWS ressources partagées dans un compte sécurisé.

Utilisation de Oracle Database@AWS ressources partagées dans un compte sécurisé

Une fois qu'une ressource a été partagée avec votre compte de confiance et que vous avez initialisé le AWS service Oracle Database@, vous pouvez consulter et utiliser la ressource partagée. Cette rubrique explique comment utiliser des ressources partagées dans un compte sécurisé.

Rubriques

- Limitations relatives aux ressources partagées dans un compte sécurisé
- Création de clusters de machines virtuelles sur une infrastructure Exadata partagée
- Afficher les ressources partagées dans un compte de confiance
- Configuration du peering ODB avec des réseaux ODB partagés

Limitations relatives aux ressources partagées dans un compte sécurisé

Lorsque vous travaillez avec des AWS ressources Oracle Database@ partagées, tenez compte des limites suivantes :

- Le partage des ressources n'est pris en charge qu'au sein de la même AWS organisation.
- Seul le compte acheteur (le compte qui accepte l'offre AWS privée Oracle Database@) peut créer une infrastructure Exadata et des ressources réseau ODB.
- Vous ne pouvez créer des ressources que sur une infrastructure partagée et uniquement si vous disposez des autorisations nécessaires.
- Les actions spécifiques (autorisations gérées) pour chaque type de ressource sont automatiquement sélectionnées lors de la création du partage de ressources et ne peuvent pas être modifiées.
- Vous ne pouvez pas modifier ou supprimer des ressources appartenant à un autre compte.
- Les ressources que vous créez sur une infrastructure partagée appartiennent à votre compte et sont prises en compte dans vos quotas OCI. Il en va de même pour les ressources destinées aux parents.
- Si le compte propriétaire annule le partage d'une ressource, vous ne pouvez plus créer de nouvelles ressources sur cette infrastructure partagée. Cependant, vos ressources existantes continuent de fonctionner.

- Le partage de ressources entre régions n'est pas pris en charge. Vous ne pouvez partager des ressources qu'au sein d'une même AWS région.
- Les ressources du compte sécurisé sont facturées à l'acheteur de l'abonnement Oracle Database@AWS .
- Lorsque vous utilisez une ressource partagée, vous devez fournir le nom de ressource Amazon (ARN).

Création de clusters de machines virtuelles sur une infrastructure Exadata partagée

Si votre compte fiable a accès à une infrastructure Exadata et à un réseau ODB partagés, vous pouvez créer des clusters de machines virtuelles Exadata, des clusters de machines virtuelles autonomes ou des peerings ODB sur cette infrastructure.

> **Note**
>
> Lorsque vous utilisez une ressource qui vous est partagée, au lieu de simplement spécifier l'ID de la ressource, vous devez spécifier le Amazon Resource Name (ARN).

Console

1. Ouvrez la AWS console Oracle Database@ à l'adresse. https://console.aws.amazon.com/odb/
2. Dans le volet de navigation, choisissez Exadata VM clusters ou Autonomous VM clusters.
3. Choisissez Créer un cluster de machines virtuelles ou Créer un cluster de machines virtuelles autonome.
4. Pour l'infrastructure Exadata, sélectionnez l'infrastructure Exadata partagée sur laquelle vous souhaitez créer le cluster de machines virtuelles.
5. Complétez les champs restants conformément à la configuration de votre cluster de machines virtuelles.
6. Choisissez Créer un cluster de machines virtuelles ou Créer un cluster de machines virtuelles autonome.

AWS CLI

Pour créer un cluster de machines virtuelles sur une infrastructure Exadata partagée à l'aide de AWS CLI, utilisez la `create-cloud-vm-cluster` commande :

```
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..." \
```

Pour créer un cluster de machines virtuelles autonomes sur une infrastructure Exadata partagée à l'aide de AWS CLI, utilisez la `create-cloud-vm-cluster` commande :

```
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
```

Le cluster de machines virtuelles est créé sur l'infrastructure Exadata partagée spécifiée et appartient à votre compte de confiance.

Afficher les ressources partagées dans un compte de confiance

Vous pouvez consulter les ressources qui ont été partagées avec votre compte à l'aide de la console AWS de gestion ou du AWS CLI.

Console

1. Ouvrez la AWS console Oracle Database@ à l'adresse. https://console.aws.amazon.com/odb/
2. Dans le volet de navigation, choisissez le type de ressource que vous souhaitez afficher : infrastructure Exadata ou réseau ODB.
3. La console affiche les ressources partagées avec vous.

4. Sélectionnez une ressource partagée pour en afficher les détails.

AWS CLI

Pour afficher les ressources partagées à l'aide de AWS CLI, utilisez la `list` commande appropriée au type de ressource. Par exemple, pour répertorier l'infrastructure Exadata :

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

La réponse indique les ressources partagées avec vous.

Pour obtenir des informations détaillées sur une ressource partagée spécifique, utilisez la `get` commande appropriée avec l'ID de ressource :

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

Configuration du peering ODB avec des réseaux ODB partagés

Pour permettre la communication entre vos applications et vos bases de données sur les réseaux ODB partagés, vous pouvez configurer le peering ODB entre votre VPC et le réseau ODB partagé. Pour plus d'informations sur le peering ODB, consultez. Création d'une connexion d'appairage ODB dans Oracle Database@AWS

Console

1. Ouvrez la AWS console Oracle Database@ à l'adresse. https://console.aws.amazon.com/odb/
2. Dans le volet de navigation, choisissez ODB peering.
3. Choisissez Create ODB network peering.
4. Pour le réseau ODB, sélectionnez le réseau ODB partagé avec lequel vous souhaitez établir un pair.
5. Pour le réseau homologue, sélectionnez votre VPC.
6. Choisissez Create ODB network peering.

AWS CLI

Pour créer une connexion d'appairage réseau entre votre VPC et un réseau ODB partagé à l'aide de, utilisez AWS CLI la commande. `create-odb-peering-connection`

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

Après avoir créé la connexion d'appairage, mettez à jour vos tables de routage pour activer le trafic entre les réseaux d'appairage.

```
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
```

Gestion de la base de données Oracle@AWS

Vous pouvez modifier et supprimer certaines Oracle Database@AWS ressources après les avoir créées.

Mettre à jour un réseau ODB dans Oracle Database@AWS

Vous pouvez mettre à jour les ressources réseau ODB suivantes :

- Le nom du réseau ODB
- Le VPC Amazon à utiliser pour établir une connexion d'appairage ODB avec le réseau ODB
- Les plages d'adresses CIDR VPC qui peuvent accéder aux ressources Exadata du réseau ODB

> **Note**
>
> En spécifiant des plages CIDR, vous limitez la connectivité aux sous-réseaux VPC nécessaires au lieu de mettre l'intégralité du VPC à la disposition du réseau ODB.

Cette section part du principe que vous avez déjà créé un réseau ODB dansÉtape 1 : créer un réseau ODB dans Oracle Database@AWS.

Pour mettre à jour un réseau ODB

1. Connectez-vous à la Oracle Database@AWS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/odb/.
2. Dans le volet de gauche, choisissez ODB networks.
3. Sélectionnez le réseau que vous souhaitez modifier.
4. Sélectionnez Modifier.
5. (Facultatif) Pour le nom du réseau ODB, entrez un nouveau nom de réseau. Le nom doit comporter de 1 à 255 caractères et commencer par un caractère alphabétique ou un trait de soulignement. Il ne peut pas contenir de tirets consécutifs.
6. (Facultatif) Pour Peered CIDRs, spécifiez les plages CIDR à partir du VPC apparenté qui doit être connecté au réseau ODB. Pour limiter l'accès, nous vous recommandons de spécifier les plages d'adresses CIDR minimales requises.

7. (Facultatif) Pour configurer les intégrations de services, sélectionnez ou désélectionnez Amazon S3 ou Zero-ETL.
8. Choisissez Continuer, puis Modifier.

Supprimer un réseau ODB dans Oracle Database@AWS

Vous pouvez supprimer un réseau ODB. Cette section part du principe que vous avez déjà créé un réseau ODB dansÉtape 1 : créer un réseau ODB dans Oracle Database@AWS. Vous ne pouvez pas supprimer un réseau ODB actuellement utilisé par un cluster de machines virtuelles.

Pour supprimer un réseau ODB

1. Connectez-vous à la Oracle Database@AWS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/odb/.
2. Dans le volet de gauche, choisissez ODB networks.
3. Sélectionnez le réseau que vous souhaitez supprimer.
4. Sélectionnez Delete (Supprimer).
5. (Facultatif) Choisissez Supprimer les ressources OCI associées pour supprimer les ressources OCI créées avec le réseau ODB.
6. Saisissez **`delete me`** dans la zone de texte.
7. Sélectionnez Delete (Supprimer).

Suppression d'un cluster de machines virtuelles dans Oracle Database@AWS

Vous pouvez supprimer un cluster de machines virtuelles Exadata ou un cluster de machines virtuelles autonome. Cette section suppose que vous avez déjà créé un cluster de machines virtuelles dansÉtape 3 : créer un cluster de machines virtuelles Exadata ou un cluster de machines virtuelles autonome dans Oracle Database@AWS.

Pour supprimer un cluster de machines virtuelles

1. Connectez-vous à la Oracle Database@AWS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/odb/.
2. Dans le volet de gauche, choisissez Exadata VM clusters ou Autonomous VM clusters.

3. Choisissez un cluster de machines virtuelles à supprimer.
4. Sélectionnez Delete (Supprimer).
5. Lorsque vous y êtes invité, entrez **`delete me`** puis choisissez Supprimer.

Suppression d'une infrastructure Oracle Exadata dans Oracle Database@AWS

Vous pouvez supprimer une infrastructure Oracle Exadata. Cette section part du principe que vous avez déjà créé une infrastructure Oracle Exadata dansÉtape 2 : créer une infrastructure Oracle Exadata dans Oracle Database@AWS. Vous ne pouvez pas supprimer une infrastructure Exadata actuellement utilisée par un cluster de machines virtuelles.

Pour supprimer une infrastructure Oracle Exadata

1. Connectez-vous à la Oracle Database@AWS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/odb/.
2. Dans le volet de gauche, choisissez Exadata infrastructures.
3. Choisissez une infrastructure Exadata à supprimer.
4. Sélectionnez Delete (Supprimer).
5. Lorsque vous y êtes invité, entrez **`delete me`** puis choisissez Supprimer.

Supprimer une connexion d'appairage ODB

Lorsque vous n'avez plus besoin d'une connexion d'appairage ODB, vous pouvez la supprimer. Vous devez supprimer toutes les connexions d'appairage ODB avant de pouvoir supprimer un réseau ODB.

Console

1. Connectez-vous à la Oracle Database@AWS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/odb/.
2. Dans le volet de navigation, choisissez ODB peering connections.
3. Sélectionnez la connexion d'appairage ODB à supprimer.
4. Sélectionnez Delete (Supprimer).

5. Pour confirmer la suppression, entrez **`delete me`** et choisissez Supprimer.

AWS CLI

Pour supprimer une connexion d'appairage ODB, utilisez la `delete-odb-peering-connection` commande.

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

Sauvegarde dans Oracle Database@AWS

Oracle Database@AWS propose plusieurs options de sauvegarde pour protéger vos bases de données Oracle. Vous pouvez utiliser des sauvegardes gérées par Oracle qui s'intègrent parfaitement à Amazon S3 ou créer vos propres sauvegardes gérées par les utilisateurs à l'aide d'Oracle Recovery Manager (RMAN).

Sauvegardes gérées par Oracle sur Amazon S3

Lorsque vous créez un réseau ODB, Oracle Database@ configure AWS automatiquement l'accès au réseau pour les sauvegardes gérées par Oracle sur Amazon S3. OCI configure les entrées DNS et les listes de sécurité nécessaires. Ces configurations autorisent le trafic entre le réseau cloud virtuel OCI (VCN) et Amazon S3. Le réseau ODB n'active ni ne contrôle les sauvegardes automatiques.

Les sauvegardes gérées par Oracle sont entièrement gérées par OCI. Lorsque vous créez votre base de données Oracle Exadata, vous pouvez activer les sauvegardes automatiques en choisissant Activer les sauvegardes automatiques dans la console OCI. Choisissez l'une des destinations de sauvegarde suivantes :

- Amazon S3
- Stockage d'objets OCI
- Service de restauration autonome

Pour plus d'informations, consultez la section Backup Exadata Database dans la documentation OCI.

Sauvegardes gérées par l'utilisateur vers Amazon S3 dans Oracle Database@AWS

Avec Oracle Database@AWS, vous pouvez créer des sauvegardes de votre base de données gérées par l'utilisateur à l'aide du service de base de données Exadata sur une infrastructure dédiée. Vous sauvegardez vos données avec Oracle Recovery Manager (RMAN) et vous les stockez dans vos compartiments Amazon S3. Vous avez un contrôle total sur la planification des sauvegardes, les politiques de rétention et les coûts de stockage tout en conservant les avantages des services gérés d'Oracle Database@AWS.

> **Note**
>
> Oracle Database@AWS ne prend pas en charge les sauvegardes gérées par l'utilisateur pour Autonomous Database on Dedicated Infrastructure.

Les sauvegardes gérées par l'utilisateur complètent les solutions de sauvegarde AWS gérées proposées par Oracle AWS Database@. Vous pouvez utiliser des sauvegardes manuelles pour répondre aux exigences de conformité, pour la reprise après sinistre entre régions ou pour les intégrer aux flux de travail de gestion des sauvegardes existants.

Vous pouvez utiliser les techniques de sauvegarde gérées par l'utilisateur suivantes :

Sauvegarde sécurisée Oracle

: Diffusez les sauvegardes directement sur Amazon S3 avec des performances optimales.

Storage Gateway

: Utilisez Storage Gateway pour les sauvegardes basées sur des fichiers utilisant un partage NFS.

Point de montage S3

: Utilisez un client de fichiers pour monter un compartiment Amazon S3 en tant que système de fichiers local.

Conditions préalables pour les sauvegardes gérées par l'utilisateur vers Amazon S3 dans Oracle Database@AWS

Avant de sauvegarder vos bases de données Oracle Exadata sur Amazon S3, procédez comme suit :

1. Activez l'accès direct à Amazon S3 depuis votre réseau ODB.
2. Configurez la connectivité réseau et le routage entre Oracle Database@AWS et Amazon S3.

Activation de l'accès à Amazon S3 depuis votre réseau ODB

Pour sauvegarder manuellement votre base de données sur Amazon S3, activez l'accès direct à S3 depuis votre réseau ODB. Cette technique permet à vos bases de données d'accéder à Amazon S3 pour répondre aux besoins de votre entreprise, tels que l'importation/exportation de données ou

les sauvegardes gérées par les utilisateurs. Vous avez un contrôle total sur la destination cible du stockage de sauvegarde et pouvez utiliser des politiques pour restreindre l'accès à Amazon S3 à l'aide de VPC Lattice.

L'accès direct à Amazon S3 depuis votre réseau ODB n'est pas activé par défaut. Vous pouvez activer l'accès S3 lorsque vous créez ou modifiez votre réseau ODB.

Console

Pour activer l'accès direct à Amazon S3 depuis votre réseau ODB

1. Ouvrez la AWS console Oracle Database@ à l'adresse. https://console.aws.amazon.com/odb/
2. Dans le volet de navigation, sélectionnez ODB networks.
3. Sélectionnez le réseau ODB pour lequel vous souhaitez activer l'accès Amazon S3.
4. Sélectionnez Modifier.
5. Cliquez sur Amazon S3.
6. (Facultatif) Configurez un document de politique Amazon S3 pour contrôler l'accès à Amazon S3. Si vous ne spécifiez aucune politique, la politique par défaut accorde un accès complet.
7. Choisissez Continuer, puis Modifier.

AWS CLI

Pour activer l'accès direct à Amazon S3 depuis votre réseau ODB, utilisez la `update-odb-network` commande avec le `s3-access` paramètre suivant :

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

Pour configurer un document de politique Amazon S3, utilisez le `--s3-policy-document` paramètre :

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

Lorsque l'accès Amazon S3 est activé, vous pouvez accéder à Amazon S3 depuis votre réseau ODB en utilisant le DNS `s3.region.amazonaws.com` régional. OCI configure ce nom DNS par défaut.

Pour utiliser un nom DNS personnalisé, modifiez votre DNS VCN pour vous assurer que le DNS personnalisé correspond à l'adresse IP du point de terminaison du réseau de service.

Configuration de la connectivité réseau entre Oracle Database@AWS et Amazon S3

Pour autoriser les sauvegardes gérées par l'utilisateur vers Amazon S3, votre machine virtuelle doit être en mesure d'accéder au point de terminaison Amazon VPC S3. Dans la console OCI, vous pouvez modifier les règles de sécurité d'un groupe de sécurité réseau (NSG) afin de contrôler le trafic entrant et sortant. Pour les sauvegardes gérées par l'utilisateur, le trafic passe par le sous-réseau client plutôt que par le sous-réseau de sauvegarde. Dans les étapes suivantes, vous mettez à jour le NSGs sous-réseau du client afin d'ajouter la règle de sortie pour l'adresse IP du point de terminaison du VPC.

Pour autoriser l'accès des machines virtuelles au point de terminaison Amazon S3

1. Ouvrez la AWS console Oracle Database@ à l'adresse. https://console.aws.amazon.com/odb/
2. Choisissez les réseaux ODB.
3. Choisissez le nom du réseau ODB.
4. Choisissez les ressources OCI.
5. Choisissez l'onglet Intégrations de services.
6. Sous Amazon S3, notez les informations suivantes :
   - IPv4 Adresse du point de terminaison Amazon VPC S3. Vous aurez besoin de ces informations ultérieurement. Par exemple, l'adresse IP peut être`192.168.12.223`.
   - Le nom de domaine du point de terminaison Amazon VPC S3. Vous aurez besoin de ces informations ultérieurement. Par exemple, le nom de domaine peut être`s3.us-east-1.amazonaws.com`.
7. Dans le volet de navigation de gauche, choisissez Exadata VM clusters, puis choisissez le nom de votre cluster de machines virtuelles.
8. En haut de la page, choisissez l'onglet Résumé.
9. Choisissez Machines virtuelles, puis choisissez le nom de votre machine virtuelle.
10. Notez la valeur dans le nom DNS. Il s'agit du nom d'hôte que vous spécifiez lorsque vous vous connectez à votre machine virtuelle à l'aide de`ssh`.
11. En haut à droite, choisissez Gérer dans OCI. Cela ouvre la console OCI.
12. Sur la page de liste Virtual Cloud Networks, choisissez le VCN qui contient le groupe de sécurité réseau (NSG) pour le sous-réseau du client réseau ODB (). `exa_static_nsg` Pour plus

d'informations, consultez la section Gestion des règles de sécurité pour un NSG dans la documentation OCI.

13. Sur la page de détails, effectuez l'une des actions suivantes en fonction de l'option qui s'affiche :
    - Dans l'onglet Sécurité, accédez à Groupes de sécurité réseau.
    - Sous Ressources, sélectionnez Network Security Groups.
14. Choisissez le NSG pour le sous-réseau client ()`exa_static_nsg`.
15. Ajoutez une règle de sortie pour l'adresse de point de terminaison VPC que vous avez indiquée précédemment.

Pour tester la connectivité à S3 depuis votre machine virtuelle

1. `ssh`À utiliser pour vous connecter `root` à la machine virtuelle dont vous avez obtenu le nom DNS précédemment. Lorsque vous vous connectez, spécifiez un `.pem` fichier contenant vos clés SSH.
2. Exécutez les commandes suivantes pour vous assurer que la machine virtuelle peut accéder au point de terminaison Amazon S3 Amazon VPC. Utilisez le nom de domaine S3 que vous avez noté précédemment.

```
# 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
```

Sauvegarde sur Amazon S3 à l'aide d'Oracle Secure Backup

Oracle Secure Backup agit comme une interface SBT à utiliser avec Recovery Manager (RMAN). Vous pouvez utiliser RMAN avec Oracle Secure Backup pour sauvegarder vos AWS bases de données Oracle Database@ directement sur Amazon S3. Oracle Secure Backup offre les avantages suivants :

- Oracle Secure Backup optimise le transfert de données entre RMAN et S3.
- Aucun stockage de sauvegarde intermédiaire n'est nécessaire.
- Oracle Secure Backup gère le cycle de vie de vos supports de sauvegarde.

Pour effectuer une sauvegarde sur Amazon S3 à l'aide d'Oracle Secure Backup

1. Installez le module Oracle Secure Backup sur votre serveur Exadata VM. Remplacez les valeurs de l'espace réservé par votre clé AWS d'accès et votre clé d'accès secrète. Pour plus d'informations, consultez la documentation Oracle sur 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. Connectez-vous à RMAN et configurez le canal de sauvegarde et le type de périphérique par défaut.

```
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. Vérifiez la configuration.

```
RMAN> SHOW ALL;
```

4. Sauvegardez la base de données.

```
RMAN> BACKUP DATABASE;
```

5. Vérifiez que la sauvegarde s'est correctement terminée.

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

Sauvegarde sur Amazon S3 à l'aide AWS Storage Gateway d'Amazon EC2

AWS Storage Gateway est un service hybride qui connecte votre environnement sur site aux services de AWS Cloud stockage. Pour les AWS sauvegardes Oracle Database@, vous pouvez utiliser Storage Gateway pour créer un flux de sauvegarde basé sur des fichiers qui écrit directement sur

Amazon S3. Contrairement à la technique Oracle Secure Backup, vous gérez le cycle de vie des sauvegardes.

Dans cette solution, vous créez une EC2 instance Amazon distincte pour configurer Storage Gateway. Vous ajoutez également un volume Amazon EBS pour mettre en cache les lectures et les écritures sur Amazon S3.

Cette technique présente les avantages suivants :

- Vous n'avez pas besoin d'un gestionnaire de médias tel qu'Oracle Secure Backup.
- Aucun stockage de sauvegarde intermédiaire n'est nécessaire.

Pour déployer votre Storage Gateway et créer un partage de fichiers

1. Ouvrez AWS Management Console at https://console.aws.amazon.com/storagegateway/home/ et choisissez la AWS région dans laquelle vous souhaitez créer votre passerelle.
2. Déployez et activez une passerelle de fichiers Amazon S3 en utilisant une EC2 instance Amazon comme hub. Suivez les instructions de la section Déployer un EC2 hôte Amazon personnalisé pour S3 File Gateway dans le guide de l'utilisateur de Storage Gateway.

   Lorsque vous configurez votre passerelle de fichiers, veillez à effectuer les opérations suivantes :

   - Ajoutez au moins un volume Amazon EBS pour le stockage en cache, d'une taille d'au moins 150 GiB.
   - Ouvrez le TCP/UDP port 2049 pour l'accès NFS dans votre groupe de sécurité. Cela vous permet de créer des partages de fichiers NFS.
   - Ouvrez le port TCP 80 pour le trafic entrant afin de permettre un accès HTTP unique lors de l'activation de la passerelle. Après activation, vous pouvez fermer ce port.
3. Créez un point de terminaison Amazon VPC pour une connectivité privée entre votre réseau ODB et Storage Gateway. Pour plus d'informations, consultez Accéder à un AWS service à l'aide d'un point de terminaison VPC d'interface.
4. Créez un partage de fichiers pour votre compartiment Amazon S3 via la console Storage Gateway. Pour plus d'informations, consultez la section Création d'un partage de fichiers.

Pour sauvegarder votre base de données sur Amazon S3 à l'aide de Storage Gateway

1. Dans un terminal, utilisez-le `ssh` pour vous connecter au nom DNS de la machine virtuelle Exadata. Pour trouver le nom DNS, consultezConditions préalables pour les sauvegardes gérées par l'utilisateur vers Amazon S3 dans Oracle Database@AWS.
2. Créez un répertoire sur le serveur de cluster de machines virtuelles Exadata pour le montage NFS. L'exemple suivant crée le répertoire `/home/oracle/sgw_mount/`.

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

3. Montez le partage NFS dans le répertoire que vous venez de créer. L'exemple suivant crée le partage dans le répertoire`/home/oracle/sgw_mount/`. *`SG-IP-address`*Remplacez-le par votre adresse IP Storage Gateway et *`your-bucket-name`* par le nom de votre compartiment S3.

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

4. Connectez-vous à RMAN et sauvegardez la base de données dans le répertoire monté. L'exemple suivant crée le canal `rman_local_bkp` et utilise le chemin du point de montage pour formater les pièces de sauvegarde.

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

5. Vérifiez que les fichiers de sauvegarde sont créés dans le répertoire de montage. L'exemple suivant montre deux pièces de sauvegarde.

```
$ 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
```

Sauvegarde sur Amazon S3 à l'aide d'un point de montage S3

Vous pouvez utiliser le point de montage Amazon S3 pour créer d'abord des sauvegardes localement, puis les copier sur Amazon S3. Cette technique crée des sauvegardes sur le stockage

local, puis les transfère vers Amazon S3 à l'aide de l'interface du point de montage. Le temps de sauvegarde est plus long que dans les autres techniques car vous devez sauvegarder les données deux fois.

> **Note**
>
> La sauvegarde directe vers Amazon S3 à l'aide du point de montage, sans préparation préalable, n'est pas prise en charge. RMAN nécessite des autorisations de système de fichiers spécifiques qui ne sont pas compatibles avec l'interface du point de montage Amazon S3.

Cette technique ne nécessite pas de licence pour un gestionnaire de médias tel qu'Oracle Secure Backup. Vous gérez le cycle de vie de vos sauvegardes.

Pour effectuer une sauvegarde sur Amazon S3 à l'aide d'un point de montage S3

1. Dans un terminal, utilisez-le `ssh` pour vous connecter au nom DNS de la machine virtuelle Exadata. Pour trouver le nom DNS, consultezConditions préalables pour les sauvegardes gérées par l'utilisateur vers Amazon S3 dans Oracle Database@AWS.
2. Installez le point de montage Amazon S3 sur le serveur de cluster Exadata VM. Pour plus d'informations sur l'installation et la configuration, consultez Mountpoint pour Amazon S3 dans le guide de l'utilisateur d'Amazon S3.

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

3. Vérifiez l'installation en exécutant la `mount-s3` commande.

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

4. Créez un répertoire de sauvegarde intermédiaire sur le stockage local du serveur de cluster de machines virtuelles Exadata. Vous allez sauvegarder votre base de données dans ce répertoire local, puis copier la sauvegarde dans votre compartiment S3. L'exemple suivant crée un répertoire`/u02/rman_bkp_local`.

   ```
   mkdir /u02/rman_bkp_local
   ```

5. Créez un répertoire pour le point de montage Amazon S3. L'exemple suivant crée un répertoire/home/oracle/s3mount.

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

6. Montez votre compartiment Amazon S3 à l'aide du point de montage. L'exemple suivant monte un compartiment S3 dans un répertoire/home/oracle/s3mount. *your-s3-bucket-name*Remplacez-le par le nom réel de votre compartiment Amazon S3.

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

7. Vérifiez que vous pouvez accéder au contenu du compartiment Amazon S3.

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

8. Connectez RMAN à votre base de données cible et sauvegardez-la dans votre répertoire de préparation local. L'exemple suivant crée le canal rman_local_bkp et utilise le chemin /u02/rman_bkp_local/ pour formater les pièces de sauvegarde.

```
$ rman TARGET /

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

9. Vérifiez que les sauvegardes sont créées dans le répertoire local :

```
$ cd /u02/rman_bkp_local/
$ ls -lart
total 4252128
drwxr-xr-x 8 oracle oinstall 4096 Jul 10 02:13 ..
-rw-r----- 1 oracle asmdba 1112223334 Jul 10 02:13 abcd1234_1921_1_1
drwxr-xr-x 2 oracle oinstall 4096 Jul 10 02:13 .
-rw-r----- 1 oracle asmdba 5556667778 Jul 10 02:14 abcd1234_1922_1_1
```

10. Copiez les fichiers de sauvegarde depuis le répertoire intermédiaire local vers le point de montage Amazon S3.

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

11. Vérifiez que vous avez correctement copié les fichiers sur 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
```

Désactivation de l'accès direct à Amazon S3

Si vous n'avez plus besoin d'un accès direct à Amazon S3 depuis votre réseau ODB, vous pouvez le désactiver. L'activation ou la désactivation de l'accès réseau direct à S3 n'affecte pas l'accès réseau aux sauvegardes gérées par Oracle sur Amazon S3.

Console

Pour désactiver l'accès direct à Amazon S3

1. Ouvrez la AWS console Oracle Database@ à l'adresse. https://console.aws.amazon.com/odb/
2. Dans le volet de navigation, sélectionnez ODB networks.
3. Sélectionnez le réseau ODB pour lequel vous souhaitez désactiver l'accès à Amazon S3.
4. Sélectionnez Modifier.
5. Décochez la case Activer l'accès S3.
6. Choisissez Modifier le réseau ODB.

AWS CLI

Utilisez la commande `update-odb-network` avec le paramètre `s3-access`.

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

Résolution des problèmes liés à l'intégration Amazon S3

Si vous rencontrez des problèmes avec les sauvegardes gérées par Oracle vers Amazon S3 ou avec l'accès direct à Amazon S3, envisagez les étapes de résolution des problèmes suivantes :

Impossible d'accéder à Amazon S3 depuis votre base de données

Vérifiez les éléments suivants :

- Vérifiez que l'accès Amazon S3 est activé pour votre réseau ODB. Utilisez l'`GetOdbNetwork`action pour vérifier si le `s3Access` statut est`Enabled`.
- Assurez-vous d'utiliser le nom DNS régional correct :`s3.region.amazonaws.com`.
- Vérifiez que votre base de données Oracle dispose des autorisations nécessaires pour accéder à Amazon S3.

Échec des sauvegardes gérées par Oracle

Vérifiez les éléments suivants :

- Les sauvegardes gérées par Oracle sur Amazon S3 sont activées par défaut et ne peuvent pas être désactivées. Si les sauvegardes échouent, consultez les journaux de base de données Oracle pour voir s'ils contiennent des messages d'erreur spécifiques.
- Vérifiez que les ressources Amazon VPC Lattice sont correctement configurées en consultant les ressources d'intégration des services.
- Contactez le support Oracle pour obtenir de l'aide concernant les problèmes de sauvegarde automatique gérés par Oracle. Pour de plus amples informations, veuillez consulter Obtenir de l'aide pour Oracle Database@AWS.

Intégration d'Oracle Database@AWS Zero-ETL à Amazon Redshift

L'intégration Zero-ETL est une solution entièrement gérée qui rend les données transactionnelles et opérationnelles disponibles dans Amazon Redshift à partir de plusieurs sources. Avec cette solution, vous pouvez répliquer des données vers Amazon Redshift à partir de vos bases de données Oracle exécutées sur Oracle Exadata ou d'une base de données autonome sur une infrastructure Exadata dédiée. La synchronisation automatique évite le processus traditionnel d'extraction, de transformation et de chargement (ETL). Il permet également des analyses en temps réel et des charges de travail basées sur l'IA. Pour plus d’informations, consultez Intégrations zéro ETL dans le Guide de gestion Amazon Redshift.

L'intégration Zero-ETL offre les avantages suivants :

- Réplication des données en temps réel : synchronisation continue des données entre les bases de données Oracle et Amazon Redshift avec une latence minimale
- Élimination des pipelines ETL complexes : il n'est pas nécessaire de créer et de gérer des solutions d'intégration de données personnalisées
- Frais d'exploitation réduits — Configuration et gestion automatisées grâce à AWS APIs
- Architecture d'intégration des données simplifiée — Intégration parfaite entre Oracle Database@AWS et AWS les services d'analyse
- Sécurité améliorée — Chiffrement intégré et contrôles AWS d'accès IAM

Amazon Redshift ne facture pas de frais supplémentaires pour l'intégration zéro ETL avec Oracle Database@.AWS Vous payez pour les ressources Amazon Redshift existantes utilisées pour créer et traiter les données de modification créées dans le cadre d'une intégration zéro ETL. Pour plus d’informations, consultez Tarification d’Amazon Redshift.

Versions de base de données prises en charge pour une intégration zéro ETL dans Oracle Database@AWS

L'intégration Zero-ETL prend en charge les versions de base de données Oracle suivantes :

- Oracle Exadata — Base de données Oracle 19c

- Base de données autonome sur une infrastructure dédiée — Oracle Database 19c et 23ai

Comment fonctionne l'intégration Zero-ETL dans Oracle Database@AWS

L'intégration zéro ETL permet à Oracle Database@ de répliquer AWS les données vers Amazon Redshift. L'intégration utilise Amazon VPC Lattice pour créer une connectivité réseau sécurisée. La technologie de capture des données modifiées (CDC) garantit la synchronisation des données en temps réel. Vous gérez l'intégration par le biais de AWS Glue APIs.

L'architecture d'intégration Zero-ETL inclut les éléments suivants :

- Connectivité sécurisée — Utilise SSL/TLS le chiffrement sur le port TLS 2484 pour le transfert de données
- AWS Secrets Manager — Stocke les informations d'identification et les certificats de base de données en toute sécurité à l'aide du service de gestion des AWS clés
- AWS Intégration Glue : fournit une interface de gestion unifiée pour les intégrations sans ETL

La réplication s'effectue selon les étapes suivantes :

1. Établissement d'une connexion sécurisée à la base de données Oracle à l'aide du protocole SSL sur le port 2484
2. Réalisation d'un vidage complet initial des bases de données, schémas et tables sélectionnés
3. Configuration de la capture des données de modification (CDC) pour une réplication continue en temps réel
4. Écrire les données répliquées dans le cluster Amazon Redshift cible

> **Important**
>
> L'intégration Zero-ETL n'est pas activée par défaut. Vous devez le configurer à l'aide de AWS Glue APIs. Vous ne pouvez pas configurer l'intégration Zero-ETL directement à l'aide d'Oracle AWS APIs Database@.

Conditions préalables à l'intégration zéro ETL dans Oracle Database@AWS

Avant de configurer l'intégration Zero-ETL, assurez-vous de remplir les conditions préalables suivantes.

Prérequis généraux

- AWS Configuration d'Oracle Database@ : assurez-vous qu'au moins un cluster de machines virtuelles est provisionné et en cours d'exécution.
- Intégration avec Zero-ETL activée : assurez-vous que votre cluster de machines virtuelles ou votre cluster de machines virtuelles autonome est associé à un réseau ODB sur lequel Zero-ETL est activé.
- Versions de base de données Oracle prises en charge : vous devez utiliser Oracle Database 19c (Oracle Exadata) ou Oracle Database 19c/23ai (base de données autonome sur infrastructure dédiée).
- Même AWS région — La base de données Oracle source et le cluster Amazon Redshift cible doivent se trouver dans la même AWS région.

Conditions requises pour la base de données Oracle

Vous devez configurer votre base de données Oracle avec les paramètres suivants.

Configuration utilisateur de réplication

Créez un utilisateur de réplication dédié dans chaque base de données enfichable (PDB) que vous souhaitez répliquer :

- Pour Oracle Exadata : créez un utilisateur `ODBZEROETLADMIN` avec un mot de passe sécurisé.
- Pour une base de données autonome sur une infrastructure dédiée, utilisez l'`GGADMIN`utilisateur existant.

Accordez les autorisations suivantes à l'utilisateur de réplication.

```
-- 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";
```

Journalisation supplémentaire

Activez la journalisation supplémentaire sur votre base de données Oracle pour capturer les données de modification.

```
-- 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;
```

Pour configurer une intégration zéro ETL entre Oracle Database@ et Amazon AWS Redshift, vous devez configurer le protocole SSL.

Pour les bases de données Oracle Exadata

Vous devez configurer manuellement le protocole SSL sur le port 2484. Cette tâche implique les opérations suivantes :

- Configuration `(PROTOCOL=tcps)(PORT=2484)` dans `listener.ora`

- Configuration du portefeuille à l'aide de `sqlnet.ora`
- Génération et configuration de certificats SSL (voir Comment configurer SSL/TCPS pour Exadata Cloud Database (Exacc/EXACS) (Doc ID 2947301.1) dans la documentation My Oracle Support)

Pour les bases de données autonomes

Le protocole SSL sur le port 2484 est activé par défaut. Aucune configuration supplémentaire n'est requise.

> **Important**
>
> Le port SSL est fixé à 2484.

AWS prérequis de service

Avant de configurer l'intégration Zero-ETL, configurez AWS Secrets Manager et configurez les autorisations IAM.

Configurer le Gestionnaire de AWS Secrets

Stockez les informations d'identification de votre base de données Oracle dans AWS Secrets Manager comme suit :

1. Créez une clé gérée par le client (CMK) dans le service de gestion des AWS clés.
2. Stockez les informations d'identification de la base de données dans AWS Secrets Manager à l'aide de la clé CMK.
3. Configurez les politiques de ressources pour autoriser l'accès à Oracle Database@AWS .

Pour obtenir l'ID et le mot de passe de votre clé TDE, utilisez la technique décrite dans Méthodes de chiffrement prises en charge pour utiliser Oracle comme source pour le Service de Migration AWS de base de données. La commande suivante génère le portefeuille base64.

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

L'exemple suivant montre un secret pour Oracle Exadata. Pour*asm_service_name*, *111.11.11.11* représente l'adresse IP virtuelle du nœud de machine virtuelle. Vous pouvez également enregistrer l'écouteur ASM avec 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'exemple suivant montre un secret pour une base de données autonome sur une infrastructure dédiée.

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

Configuration des autorisations IAM

Créez des politiques IAM qui autorisent les opérations d'intégration sans ETL. L'exemple de politique suivant permet de décrire, de créer, de mettre à jour et de supprimer des opérations pour un cluster de machines virtuelles Exadata. Pour un cluster de machines virtuelles autonomes, utilisez la valeur `cloud-autonomous-vm-cluster` plutôt que `cloud-vm-cluster` l'ARN de la ressource.

Considérations relatives à l'intégration zéro ETL dans Oracle Database@AWS

Lorsque vous configurez une intégration zéro ETL entre Amazon Redshift Oracle Database@AWS et Amazon Redshift, tenez compte des directives suivantes :

Temps de chargement initial des données

: Le temps de chargement complet initial dépend de la taille de votre base de données. Les bases de données volumineuses peuvent prendre plusieurs heures, voire plusieurs jours, pour effectuer la synchronisation initiale.

Performance des bases de données Oracle

: La capture des données de modification peut avoir un impact sur les performances des bases de données Oracle, en particulier lors de volumes de transactions élevés. Après avoir activé l'intégration Zero-ETL, surveillez les performances de votre base de données.

Modifications de schéma

: Les modifications du langage de définition des données (DDL) dans la base de données Oracle source peuvent nécessiter une intervention manuelle pour recréer l'intégration. Planifiez soigneusement les modifications du schéma.

Pour des considérations générales, consultez la section Considérations relatives à l'utilisation d'intégrations sans ETL avec Amazon Redshift.

Limites de l'intégration zéro ETL dans Oracle Database@AWS

Notez les limites générales suivantes :

PDB unique par intégration

: Chaque intégration Zero-ETL ne peut répliquer que les données d'une seule base de données enfichable (PDB). Les filtres de données tels que `include: pdb1.*.*, include: pdb2.*.*` ceux-ci ne sont pas pris en charge.

Intégration unique par base de données autonome ou infrastructure Exadata

: Chaque intégration Zero-ETL ne peut répliquer que les données d'une seule base de données autonome sur une infrastructure dédiée.

Port SSL fixe

Les connexions SSL doivent utiliser le port 2484.

Même exigence de région

Le cluster de AWS machines virtuelles Oracle Database@ source et le cluster Amazon Redshift cible doivent se trouver dans la même région. AWS La réplication entre régions n'est pas prise en charge.

Pas de support MTL

Le protocole TLS mutuel (MTLS) n'est pas pris en charge. Si le protocole MTL est activé dans votre base de données OCI, vous devez le désactiver pour utiliser l'intégration zéro ETL.

Paramètres d'intégration immuables

Une fois que vous avez créé l'ARN ou la clé KMS secrète associée à une intégration, vous ne pouvez pas la modifier. Vous devez supprimer et recréer l'intégration pour modifier ces paramètres.

Chiffrement TDE au niveau des colonnes

Le chiffrement transparent des données (TDE) au niveau des colonnes n'est pas pris en charge pour les bases de données Oracle Exadata. Seul le TDE au niveau de l'espace disque logique est pris en charge.

Prise en charge du type de données

Certains types de données spécifiques à Oracle peuvent ne pas être entièrement pris en charge ou nécessiter une transformation lors de la réplication. Testez minutieusement vos types de données spécifiques avant de déployer votre base de données en production.

Configuration des AWS intégrations Oracle Database@ avec Amazon Redshift

Pour configurer l'intégration Zero-ETL entre votre base de données Oracle et Amazon Redshift, procédez comme suit :

1. Activez Zero-ETL sur votre réseau ODB.
2. Configurez les conditions requises pour la base de données Oracle.
3. Configurez le Gestionnaire de AWS Secrets Manager et le Service de gestion des AWS clés.

4. Configurez les autorisations IAM.
5. Configurez les politiques relatives aux ressources Amazon Redshift.
6. Créez l'intégration Zero-ETL.
7. Créez la base de données cible dans Amazon Redshift.

Étape 1 : Activez Zero-ETL pour votre réseau ODB

Vous pouvez activer l'intégration zéro ETL pour le réseau ODB associé à votre cluster de machines virtuelles source. Par défaut, cette intégration est désactivée.

Console

Pour activer l'intégration Zero-ETL

1. Ouvrez la AWS console Oracle Database@ à l'adresse. https://console.aws.amazon.com/odb/
2. Dans le volet de navigation, sélectionnez ODB networks.
3. Sélectionnez le réseau ODB pour lequel vous souhaitez activer l'intégration zéro ETL.
4. Sélectionnez Modifier.
5. Sélectionnez Zero-ETL.
6. Choisissez Continuer, puis Modifier.

AWS CLI

Pour activer l'intégration Zero-ETL, utilisez la `update-odb-network` commande avec le `--zero-etl-access` paramètre :

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

Pour activer l'intégration zéro ETL pour le réseau ODB associé à votre cluster de machines virtuelles source, utilisez la `update-odb-network` commande. Cette commande configure l'infrastructure réseau requise pour l'intégration sans ETL.

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

Étape 2 : Configuration de votre base de données Oracle

Complétez la configuration de la base de données Oracle comme décrit dans les conditions préalables :

- Créez des utilisateurs de réplication et accordez les autorisations nécessaires.
- Activez les journaux de restauration archivés.
- Configurez le protocole SSL (Oracle Exadata uniquement).
- Configurez les utilisateurs ASM le cas échéant (Oracle Exadata uniquement).

Étape 3 : configurer le Gestionnaire de AWS Secrets Manager et le service de gestion des AWS clés

Créez une clé gérée par le client (CMK) et stockez les informations d'identification de votre base de données.

1. Créez une clé CMK dans le service de gestion des AWS clés à l'aide de la `create-key` commande.

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

2. Stockez les informations d'identification de votre base de données dans 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. Associez une politique de ressources au secret pour autoriser l'accès à Oracle Database@AWS .

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

Dans la commande précédente, `secret-resource-policy.json` contient le code JSON suivant.

JSON

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

4. Attachez une politique de ressources à la clé CMK. La politique de ressources CMK doit inclure des autorisations pour le principal de service Oracle Database@ et le principal de AWS service Amazon Redshift afin de prendre en charge l'intégration chiffrée sans ETL.

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

Le `cmk-resource-policy.json` fichier doit inclure les déclarations de politique suivantes. La première instruction autorise l'accès au AWS service Oracle Database@, et la seconde autorise Amazon Redshift à créer des autorisations sur la clé KMS pour les opérations de données chiffrées.

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"
          ]
        }
      }
    }
  ]
}
```

Étape 4 : Configuration des autorisations IAM

Créez et attachez des politiques IAM qui autorisent les opérations d'intégration sans 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 politique suivante accorde les autorisations nécessaires.

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": "*"
    }
  ]
}
```

Étape 5 : Configuration des politiques de ressources Amazon Redshift

Configurez des politiques de ressources sur votre cluster Amazon Redshift afin d'autoriser les intégrations entrantes.

```
aws redshift put-resource-policy \
  --no-verify-ssl \
  --resource-arn "your-redshift-cluster-arn" \
  --policy '{
    "Version": "2012-10-17",
```

```
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "Service": "redshift.amazonaws.com"
        },
        "Action": [
          "redshift:AuthorizeInboundIntegration"
        ],
        "Condition": {
          "StringEquals": {
            "aws:SourceArn": "your-vm-cluster-arn"
          }
        }
      },
      {
        "Effect": "Allow",
        "Principal": {
          "AWS": "your-account-id"
        },
        "Action": [
          "redshift:CreateInboundIntegration"
        ]
      }
    ]
  }' \
  --region us-west-2
```

> **Tip**
>
> Vous pouvez également utiliser l'option Corriger pour moi dans la AWS console. Cette option configure automatiquement les politiques Amazon Redshift requises sans que vous ayez à le faire manuellement.

Étape 6 : Créez l'intégration Zero-ETL à l'aide de AWS Glue

Créez l'intégration Zero-ETL à l'aide de la AWS Glue `create-integration` commande. Dans cette commande, vous spécifiez le cluster de machines virtuelles source et l'espace de noms Amazon Redshift cible.

L'exemple suivant crée une intégration avec un PDB nommé pdb1 running in a Exadata VM cluster. Vous pouvez également créer un cluster de machines virtuelles autonomes en le `cloud-vm-cluster` remplaçant par `cloud-autonomous-vm-cluster` dans l'ARN source. La spécification d'une clé KMS est facultative. Si vous spécifiez une clé, elle peut être différente de celle dans laquelle vous l'avez crééeÉtape 3 : configurer le Gestionnaire de AWS Secrets Manager et le service de gestion des AWS clés.

```
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"
```

La commande renvoie un ARN d'intégration et définit le statut sur`creating`. Vous pouvez surveiller l'état de l'intégration à l'aide de la `describe-integrations` commande.

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

> **Important**
>
> Un seul PDB par intégration est pris en charge. Le filtre de données doit spécifier un seul PDB, `include: pdb1.*.*` par exemple. La source doit se trouver dans la même AWS région et dans le même compte que ceux dans lesquels l'intégration est créée.

Étape 7 : créer une base de données cible dans Amazon Redshift

Une fois l'intégration active, créez une base de données cible dans votre 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";
```

Après avoir créé la base de données cible, vous pouvez interroger les données répliquées.

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

-- Connect to the new database
\c target_database_name

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

Vérifiez l'intégration Zero-ETL

Vérifiez que l'intégration fonctionne en interrogeant le statut de l'intégration dans AWS Glue et en vous assurant que vos modifications Oracle sont répliquées sur Amazon Redshift.

Pour vérifier que votre intégration Zero-ETL fonctionne correctement

1. Vérifiez l'état de l'intégration.

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

   Le statut doit être `ACTIVE` ou`REPLICATING`.

2. Vérifiez la réplication des données en apportant des modifications à votre base de données Oracle et en vérifiant qu'elles apparaissent dans Amazon Redshift.
3. Surveillez les métriques de réplication sur Amazon CloudWatch (si disponible).

Filtrage des données pour les intégrations sans ETL dans Oracle Database@AWS

Oracle Database@AWS Les intégrations Zero-ETL prennent en charge le filtrage des données. Vous pouvez l'utiliser pour contrôler les données que votre base de données Oracle Exadata source réplique vers votre entrepôt de données cible. Au lieu de répliquer l'intégralité de la base de données, vous pouvez appliquer un ou plusieurs filtres pour inclure ou exclure des tables spécifiques de manière sélective. Cela vous permet d'optimiser les performances de stockage et de requête en garantissant que seules les données pertinentes sont transférées. Le filtrage est limité aux niveaux de la base de données et de la table. Le filtrage au niveau des colonnes et des lignes n'est pas pris en charge.

Oracle Database et Amazon Redshift gèrent la casse des noms d'objets différemment, ce qui affecte à la fois la configuration du filtre de données et les requêtes cibles. Notez ce qui suit :

- Oracle Database stocke les noms des bases de données, des schémas et des objets en majuscules, sauf s'ils sont explicitement cités dans l'instruction `CREATE`. Par exemple, si vous créez `mytable` (sans guillemets), le dictionnaire de données Oracle enregistre le nom de la table sous la forme `MYTABLE`. Si vous citez le nom de l'objet dans votre déclaration de création, le dictionnaire de données Oracle préserve le cas.
- Les filtres de données sans extraction, transformation ni chargement (sans ETL) distinguent les majuscules et minuscules et doivent correspondre exactement aux noms d'objets tels qu'ils apparaissent dans le dictionnaire de données Oracle. Par exemple, si le dictionnaire Oracle stocke le schéma et le nom de la table`REINVENT.MYTABLE`, créez un filtre à l'aide de`include: ORCL.REINVENT.MYTABLE`.
- Les requêtes Amazon Redshift utilisent par défaut des noms d'objets en minuscules, sauf entre guillemets explicites. Par exemple, une requête `MYTABLE` (sans guillemets) recherche `mytable`.

Tenez compte des différences de casses lorsque vous créez le filtre Amazon Redshift et que vous interrogez les données. Les considérations relatives au filtrage Oracle Database@AWS sont les mêmes que pour Amazon RDS for Oracle. Pour des exemples illustrant la manière dont le cas peut affecter les filtres de données dans une base de données Oracle, consultez les exemples de RDS pour Oracle dans le guide de l'utilisateur d'Amazon Relational Database Service.

Surveillance de l'intégration Zero-ETL

La surveillance régulière de votre intégration Zero-ETL garantit des performances optimales et permet d'identifier les problèmes à un stade précoce.

Surveillance de l'état de l'intégration

Surveillez l'état de vos intégrations Zero-ETL à l'aide de 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
```

Les statuts d'intégration incluent :

- création — L'intégration est en cours de configuration
- actif : l'intégration consiste à exécuter et à répliquer les données
- modification — La configuration de l'intégration est en cours de mise à jour
- needs_attention — L'intégration nécessite une intervention manuelle
- échec — L'intégration a rencontré une erreur
- suppression — L'intégration est supprimée

Surveillance des performances

Surveillez les aspects suivants de vos performances d'intégration Zero-ETL :

- Délai de réplication : différence de temps entre le moment où une modification se produit dans Oracle et le moment où elle apparaît dans Amazon Redshift
- Débit de données : volume de données répliquées par unité de temps
- Taux d'erreur : fréquence des erreurs ou des échecs de réplication
- Utilisation des ressources : utilisation du processeur, de la mémoire et du réseau sur les systèmes source et cible

Utilisez Amazon CloudWatch pour surveiller ces indicateurs et configurer des alarmes pour les seuils critiques.

Gestion des intégrations sans ETL dans Oracle Database@AWS

Après avoir créé une intégration zéro ETL, vous pouvez effectuer diverses opérations de gestion, notamment modifier et supprimer des intégrations. Cette section couvre la gestion continue de vos intégrations Zero-ETL.

Modification des intégrations zéro ETL

Vous pouvez uniquement modifier le nom, la description et les options de filtrage des données pour une intégration zéro ETL dans un entrepôt de données pris en charge. Vous ne pouvez pas modifier la AWS clé du service de gestion des clés utilisée pour chiffrer l'intégration, ni les bases de données source ou cible.

Conditions préalables à la modification des intégrations

Avant de modifier une intégration zéro ETL, assurez-vous que vous disposez des éléments suivants :

- Autorisations requises : votre utilisateur ou rôle IAM doit disposer de `odb:UpdateOutboundIntegration` cette autorisation en plus des AWS Glue autorisations standard.
- Intégration en état actif — L'intégration doit être dans un `ACTIVE` état, et non dans `CREATINGMODIFYING`,`DELETING`, ou`FAILED`.
- Syntaxe de filtre de données valide : les nouveaux filtres de données doivent suivre la syntaxe de include/exclude modèle prise en charge.

Modification des filtres de données

Vous pouvez modifier les tables ou les schémas qui sont répliqués en modifiant le filtre de données. Ainsi, vous pouvez ajouter ou supprimer des objets de base de données de la réplication sans recréer l'intégralité de l'intégration.

Pour modifier le filtre de données d'une intégration, utilisez la `modify-integration` commande.

```
aws glue modify-integration \
```

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

Vous pouvez également modifier le nom et la description de l'intégration en même temps. Dans l'exemple suivant, vous modifiez le nom, les descriptions et les filtres de l'intégration pour deux schémas dans`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

Lorsque vous modifiez le filtre de données, l'intégration entre dans un `modifying` état et effectue une resynchronisation des données. L'intégration arrête la réplication, applique les nouveaux paramètres de filtre et reprend la réplication avec une opération de rechargement de la cible. Surveillez l'état de l'intégration pour vous assurer que la modification est terminée avec succès.

Considérations relatives aux modifications des filtres de données pour les intégrations sans ETL

Tenez compte des points suivants lorsque vous modifiez des filtres de données :

- Limite PDB unique — Vous ne pouvez spécifier qu'une seule base de données enfichable (PDB) par intégration. Les filtres de données similaires `include: pdb1.*.*, include: pdb2.*.*` ne sont pas pris en charge
- Interruption de la réplication : la réplication des données s'arrête pendant le processus de modification et reprend après l'application du nouveau filtre.
- Rechargement des données : l'intégration effectue un rechargement complet des données correspondant aux nouveaux critères de filtre.
- Impact sur les performances : les modifications importantes du filtre de données peuvent prendre beaucoup de temps et affecter les performances de la base de données source lors du rechargement.

Limitations relatives aux modifications des paramètres d'intégration zéro ETL

Vous ne pouvez pas modifier les paramètres suivants après avoir créé une intégration zéro ETL :

- ARN secret — Le secret du Gestionnaire de AWS secrets contenant les informations d'identification de la base de données
- Clé KMS : clé gérée par le client utilisée pour le chiffrement
- ARN source — Le cluster de machines virtuelles Oracle Database@AWS
- ARN cible : cluster ou espace de noms Amazon Redshift

Pour modifier ces paramètres, supprimez l'intégration Zero-ETL existante et créez-en une nouvelle.

Suppression d'intégrations zéro ETL

Lorsque vous n'avez plus besoin d'une intégration zéro ETL, vous pouvez la supprimer pour arrêter la réplication et nettoyer les ressources associées.

Suppression à l'aide de AWS Glue

Supprimez une intégration Zero-ETL à l'aide de l'API AWS Glue.

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

Vous pouvez supprimer des intégrations dans les états suivants :

- actif
- besoins_attention
- failed
- synchronisation

Effets de la suppression

Lorsque vous supprimez une intégration zéro ETL, tenez compte des effets suivants :

La réplication s'arrête.

Oracle Database@AWS ne reproduit pas les nouvelles modifications apportées par Amazon Redshift.

Les données existantes sont préservées.

Les données déjà répliquées sur Amazon Redshift restent disponibles.

La base de données cible est conservée.

La base de données Amazon Redshift créée à partir de l'intégration n'est pas automatiquement supprimée.

> **Important**
>
> La suppression est irréversible. Si vous devez reprendre la réplication après la suppression, créez une nouvelle intégration qui effectue un chargement initial complet.

Bonnes pratiques pour une gestion zéro ETL

Suivez ces bonnes pratiques pour garantir des performances, une sécurité et une rentabilité optimales de vos intégrations sans ETL.

Bonnes pratiques opérationnelles

Ces pratiques opérationnelles permettent de maintenir des intégrations zéro ETL fiables et efficaces.

Surveillance régulière

Configurez des CloudWatch alarmes pour surveiller l'état de l'intégration et les indicateurs de performance.

Rotation des informations d'identification

Changez régulièrement les mots de passe des bases de données et mettez-les à jour dans AWS Secrets Manager.

Vérification des sauvegardes

Vérifiez régulièrement que vos sauvegardes de base de données Oracle incluent les composants nécessaires à la reprise après sinistre.

Tests de performance

Testez l'impact de l'intégration zéro ETL sur les performances de votre base de données Oracle, en particulier pendant les périodes de pointe.

Planification des modifications de schéma

Planifiez et testez les modifications de schéma dans un environnement de développement avant de les appliquer à la production.

Bonnes pratiques de sécurité

Mettez en œuvre ces mesures de sécurité pour protéger votre intégration et vos données Zero-ETL.

Accès sur la base du moindre privilège

Accordez uniquement les autorisations minimales nécessaires aux utilisateurs de réplication et aux rôles AWS IAM.

Sécurité du réseau

Utilisez des groupes de sécurité et NACLs limitez l'accès au réseau aux seuls ports et sources requis.

Chiffrement au repos

Assurez-vous que les bases de données Oracle et les clusters Amazon Redshift utilisent le chiffrement au repos.

Journaux d’audit

Activez la journalisation des audits sur Oracle et Amazon Redshift pour suivre l'accès aux données et les modifications.

Gestion des secrets

Utilisez AWS les fonctionnalités de rotation automatique de Secrets Manager dans la mesure du possible.

Optimisation des coûts

Appliquez ces stratégies pour optimiser les coûts tout en maintenant des performances d'intégration zéro ETL efficaces.

Filtrage des données

Utilisez des filtres de données précis pour répliquer uniquement les données dont vous avez besoin, réduisant ainsi les coûts de stockage et de calcul.

Optimisation d'Amazon Redshift

Utilisez les types de nœuds Amazon Redshift appropriés et implémentez la compression des données pour optimiser les coûts.

Surveillance de l'utilisation

Passez régulièrement en revue votre utilisation et vos coûts d'intégration Zero-ETL via AWS Cost Explorer.

Nettoyez les intégrations inutilisées

Supprimez les intégrations qui ne sont plus nécessaires pour éviter des frais récurrents.

Résolution des problèmes d'intégration Zero-ETL

Cette section fournit des conseils pour résoudre les problèmes courants liés à l'intégration sans ETL.

Aucun échec de configuration de l'intégration ETL

Authentication failures (Échecs d’authentification)

- Vérifiez que l'utilisateur de réplication existe et possède le mot de passe correct dans AWS Secrets Manager.
- Assurez-vous que toutes les autorisations requises ont été accordées à l'utilisateur de réplication.
- Vérifiez que l'ARN secret est correct et accessible par Oracle Database@AWS.
- Vérifiez que la politique de ressources CMK autorise l'accès par le principal de service Oracle Database@AWS .

Problèmes liés à la connectivité réseau

- Assurez-vous que l'intégration Zero-ETL est activée sur votre réseau ODB.
- Vérifiez que le protocole SSL est correctement configuré sur le port 2484 (Exadata uniquement).
- Vérifiez que l'écouteur de base de données Oracle est en cours d'exécution et accepte les connexions.

- Assurez-vous que les groupes de sécurité réseau et NACLs autorisez le trafic sur le port 2484.
- Vérifiez que le nom du service indiqué dans votre secret correspond au nom du service Oracle réel.

Erreurs d'autorisation

- Vérifiez que votre utilisateur ou rôle IAM dispose des autorisations nécessaires pour les opérations AWS Glue d'intégration.
- Vérifiez que la politique de ressources Amazon Redshift autorise les intégrations entrantes depuis votre cluster de machines virtuelles.
- Assurez-vous qu'Oracle Database@AWS a obtenu l'accès à vos secrets et à votre clé du service de gestion des AWS clés.

Problèmes de réplication

Défaillances de chargement initiales

- Vérifiez que la base de données Oracle dispose de suffisamment de ressources pour prendre en charge l'opération de chargement complet.
- Assurez-vous que la journalisation supplémentaire est activée sur la base de données source.
- Vérifiez s'il existe des blocages ou des contraintes au niveau de la table susceptibles d'empêcher l'extraction des données.

Modifier les problèmes de capture de données

- Vérifiez que la base de données Oracle dispose d'un espace de journalisation et d'un taux de rétention adéquats.
- Vérifiez que l'utilisateur de réplication a accès aux journaux de restauration archivés.
- Pour les systèmes compatibles ASM, assurez-vous que l'utilisateur ASM est correctement configuré.
- Surveillez les performances de la base de données Oracle pour vous assurer que le CDC n'est pas à l'origine de conflits de ressources.

Retard de réplication élevé

- Surveillez les métriques de retard de réplication dans CloudWatch.
- Vérifiez la présence de volumes de transactions élevés ou de transactions importantes dans la base de données source.
- Vérifiez que le cluster Amazon Redshift dispose d'une capacité suffisante pour gérer les données entrantes.

Problèmes de cohérence des données

Données manquantes ou incomplètes

- Vérifiez que le filtre de données inclut tous les schémas et tables requis.
- Vérifiez les types de données non pris en charge susceptibles d'être à l'origine d'échecs de réplication.
- Assurez-vous que l'utilisateur de réplication dispose des autorisations SELECT sur toutes les tables requises.

Erreurs de conversion de type de données

- Consultez les mappages de types de données pris en charge entre Oracle et Redshift.
- Vérifiez les types de données spécifiques à Oracle susceptibles de nécessiter un traitement personnalisé.
- Envisagez de modifier votre schéma Oracle pour utiliser des types de données plus compatibles.

Surveillance et débogage

Utilisez les approches suivantes pour surveiller et résoudre les problèmes d'intégration zéro ETL :

- Surveillance de l'état de l'intégration — Vérifiez régulièrement l'état de l'intégration à l'aide de`aws glue describe-integrations`.
- CloudWatch métriques — Surveillez CloudWatch les métriques disponibles pour les performances et les erreurs de réplication.
- Surveillance des bases de données Oracle : surveillez les performances des bases de données Oracle et l'utilisation des ressources.
- Surveillance Redshift : surveillez les performances du cluster Amazon Redshift et l'utilisation du stockage.

Pour les problèmes complexes qui ne peuvent pas être résolus à l'aide de ce guide de dépannage, contactez AWS Support les informations suivantes :

- ARN d'intégration et état actuel.
- Les messages d'erreur issus de l'intégration décrivent les opérations.
- Configurations de base de données Oracle et de clusters Amazon Redshift.

- Chronologie du moment où le problème a commencé à se produire.

Sécurité dans Oracle Database@AWS

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre AWS OCI et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui s'exécute Services AWS dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, notamment de la sensibilité de vos données, des exigences de votre organisation et des lois et réglementations applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée modèle lors de son utilisation Oracle Database@AWS. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos Oracle Database@AWS ressources.

Vous pouvez gérer l'accès à vos Oracle Database@AWS ressources. La méthode que vous utilisez pour gérer l'accès dépend du type de tâche que vous devez effectuer Oracle Database@AWS :

- Utilisez des politiques Gestion des identités et des accès AWS (IAM) pour attribuer des autorisations qui déterminent qui est autorisé à gérer les Oracle Database@AWS ressources. Par exemple, vous pouvez utiliser IAM pour déterminer qui est autorisé à créer, décrire, modifier et supprimer l'infrastructure Exadata, les clusters de machines virtuelles ou les ressources de balises.
- Utilisez les fonctionnalités de sécurité de votre moteur de base de données Oracle pour contrôler qui peut se connecter aux bases de données sur une instance de base de données. Ces fonctions agissent comme si la base de données se trouvait sur votre réseau local.
- Utilisez des connexions SSL (Secure Socket Layers) ou TLS (Transport Layer Security) avec les bases de données Exadata. Pour plus d'informations, voir Préparation aux connexions TLS sans portefeuille.

- Oracle Database@AWS n'est pas immédiatement accessible depuis Internet et n'est déployé AWS que sur des sous-réseaux privés.
- Oracle Database@AWS utilise de nombreux ports TCP (Transmission Control Protocol) par défaut pour diverses opérations. Pour la liste complète des ports, voir Affectations de ports par défaut.
- Pour stocker et gérer les clés à l'aide du chiffrement transparent des données (TDE), activé par défaut, utilisez des Oracle Database@AWS coffres-forts OCI ou Oracle Key Vault. Oracle Database@AWS ne supporte pas AWS Key Management Service.
- Par défaut, la base de données est configurée à l'aide de clés de chiffrement gérées par Oracle. La base de données prend également en charge les clés gérées par le client.
- Pour améliorer la protection des données, utilisez Oracle Data Safe avec Oracle Database@AWS.

Les rubriques suivantes expliquent comment procéder à la configuration Oracle Database@AWS pour atteindre vos objectifs de sécurité et de conformité.

Rubriques

- Protection des données dans Oracle Database@AWS
- Gestion des identités et des accès pour Oracle Database@AWS
- Validation de conformité pour Oracle Database@AWS
- Résilience dans Oracle Database@AWS
- Utilisation de rôles liés à un service pour Oracle Database@AWS
- Oracle Database@AWS mises à jour des politiques AWS gérées

Protection des données dans Oracle Database@AWS

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l’authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.

- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Oracle Database@AWS ou autre à Services AWS l'aide de la console, de l'API ou. AWS CLI AWS SDKs Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement des données

Les bases de données Exadata utilisent Oracle Transparent Data Encryption (TDE) pour chiffrer vos données. Vos données sont également protégées dans des tablespaces temporaires, des segments annulés, des redo logs et lors d'opérations de base de données internes telles que JOIN et SORT. Pour plus d'informations, consultez la section Sécurité des données.

Chiffrement en transit

Les bases de données Exadata utilisent les fonctionnalités natives de chiffrement et d'intégrité d'Oracle Net Services pour sécuriser les connexions à la base de données. Pour plus d'informations, consultez la section Sécurité des données en transit.

Gestion des clés

Le chiffrement transparent des données inclut un magasin de clés pour stocker en toute sécurité les clés de chiffrement principales et un cadre de gestion pour gérer le magasin de clés de manière sûre et efficace et effectuer les opérations de maintenance des clés. Pour plus d'informations, voir Pour administrer les clés de chiffrement de Vault.

Gestion des identités et des accès pour Oracle Database@AWS

Gestion des identités et des accès AWS (IAM) est un AWS service qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Oracle AWS Database@. IAM est un AWS service que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion de l’accès à l’aide de politiques
- Comment Oracle Database@AWS fonctionne avec IAM
- Stratégies basées sur l’identité pour Oracle Database@AWS
- AWS politiques gérées pour Oracle Database@AWS
- Oracle Database@AWS authentification et autorisation dans OCI
- Résolution des problèmes Oracle Database@AWS d'identité et d'accès

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes Oracle Database@AWS d'identité et d'accès)
- Administrateur du service : déterminez l’accès des utilisateurs et soumettez les demandes d’autorisation (voir Comment Oracle Database@AWS fonctionne avec IAM)

- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir Stratégies basées sur l'identité pour Oracle Database@AWS)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle d'utilisateur à un rôle IAM (console) ou en appelant une opération d' AWS API AWS CLI ou d'API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès entre comptes, les accès entre services et pour les applications exécutées sur Amazon. EC2 Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Politiques basées sur l’identité

Les stratégies basées sur l’identité sont des documents de stratégie d’autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Définition d’autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l’utilisateur IAM.

Les politiques basées sur l’identité peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l’utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l’accès à une ressource spécifique. Vous devez spécifier un principal dans une politique basée sur les ressources.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d’autorisations : une limite des autorisations définit le nombre maximum d’autorisations qu’une politique basée sur l’identité peut accorder à une entité IAM. Pour plus d’informations, consultez Limites d’autorisations pour des entités IAM dans le Guide de l’utilisateur IAM.
- Politiques de contrôle des services (SCPs) — Spécifiez les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d’informations, consultez Politiques de contrôle de service dans le Guide de l’utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCPs) : définissez le maximum d'autorisations disponibles pour les ressources de vos comptes. Pour plus d'informations, voir Politiques de contrôle des ressources (RCPs) dans le guide de AWS Organizations l'utilisateur.

- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Oracle Database@AWS fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Oracle Database@AWS, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Oracle Database@.AWS

Fonctionnalité IAM	Oracle Database@AWS soutien
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACLs	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont Oracle Database@AWS les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Oracle Database@AWS

Prend en charge les politiques basées sur l’identité : oui

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Définition d’autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l’utilisateur IAM.

Avec les politiques IAM basées sur l’identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l’utilisateur IAM.

Exemples de politiques basées sur l'identité pour Oracle Database@AWS

Pour consulter des exemples de politiques AWS basées sur l'identité Oracle Database@, consultez. Stratégies basées sur l’identité pour Oracle Database@AWS

Politiques basées sur les ressources au sein de Oracle Database@AWS

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l’accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d’actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions politiques pour Oracle Database@AWS

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des Oracle Database@AWS actions, voir Actions définies par Oracle Database@AWS dans le Service Authorization Reference.

Les actions de politique en Oracle Database@AWS cours utilisent le préfixe suivant avant l'action :

```
odb
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Pour consulter des exemples de politiques AWS basées sur l'identité Oracle Database@, consultez. Stratégies basées sur l'identité pour Oracle Database@AWS

Ressources politiques pour Oracle Database@AWS

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des types de Oracle Database@AWS ressources et leurs caractéristiques ARNs, reportez-vous à la section Ressources définies par Oracle Database@AWS dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, voir Actions définies par Oracle Database@AWS.

Pour consulter des exemples de politiques AWS basées sur l'identité Oracle Database@, consultez. Stratégies basées sur l'identité pour Oracle Database@AWS

Clés de conditions de politique pour Oracle Database@AWS

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de Oracle Database@AWS condition, voir Clés de condition pour Oracle Database@AWS dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, voir Actions définies par Oracle Database@AWS.

Pour consulter des exemples de politiques AWS basées sur l'identité Oracle Database@, consultez. Stratégies basées sur l’identité pour Oracle Database@AWS

ACLs in Oracle Database@AWS

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec Oracle Database@AWS

Prend en charge ABAC (identifications dans les politiques) : partiellement

Le contrôle d’accès par attributs (ABAC) est une stratégie d’autorisation qui définit les autorisations en fonction des attributs nommés balise. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

Pour contrôler l’accès basé sur des étiquettes, vous devez fournir les informations d’étiquette dans l’élément de condition d’une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d’informations sur ABAC, consultez Définition d’autorisations avec l’autorisation ABAC dans le Guide de l’utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l’ABAC, consultez Utilisation du contrôle d’accès par attributs (ABAC) dans le Guide de l’utilisateur IAM.

Utilisation d'informations d'identification temporaires avec Oracle Database@AWS

Prend en charge les informations d’identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au

lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Autorisations principales interservices pour Oracle Database@AWS

Prend en charge les sessions d'accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant un AWS service, combinées au AWS service demandeur pour adresser des demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

Rôles de service pour Oracle Database@AWS

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez la section Créer un rôle pour déléguer des autorisations à un AWS service dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber Oracle Database@AWS les fonctionnalités. Modifiez les rôles de service uniquement lorsque Oracle Database@AWS vous recevez des instructions à cet effet.

Rôles liés à un service pour Oracle Database@AWS

Prend en charge les rôles liés à un service : oui

Un rôle lié à un service est un type de rôle lié à un AWS service. Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles Oracle Database@AWS liés à un service, consultez. Utilisation de rôles liés à un service pour Oracle Database@AWS

Stratégies basées sur l’identité pour Oracle Database@AWS

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources Oracle Database@AWS . Pour octroyer aux utilisateurs des autorisations d’effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM.

Pour apprendre à créer une politique basée sur l’identité IAM à l’aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l’utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Oracle Database@AWS, y compris le format du ARNs pour chacun des types de ressources, voir Actions, ressources et clés de condition pour Oracle Database@AWS dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Oracle Database@AWS
- Autoriser les utilisateurs à provisionner Oracle Database@AWS des ressources
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des AWS ressources Oracle Database@ dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l’identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d’informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l’utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l’exécution d’une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre

privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un AWS service spécifique, tel que CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console Oracle Database@AWS

Pour accéder à la AWS console Oracle Database@, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails relatifs aux AWS ressources Oracle Database@ de votre. Compte AWS Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Autoriser les utilisateurs à provisionner Oracle Database@AWS des ressources

Cette politique permet aux utilisateurs d'avoir un accès complet aux Oracle Database@AWS ressources de provisionnement. Pour configurer la résolution DNS à partir de votre VPC, créez un résolveur Route 53 sortant et ajoutez des règles pour transférer le trafic DNS avec le nom de domaine OCI vers l'adresse IP de l'écouteur 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": "*"
        }
    ]
}
```

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or 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 politiques gérées pour Oracle Database@AWS

Pour ajouter des autorisations aux ensembles d'autorisations et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour créer des politiques gérées par le client IAM qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le guide de l'utilisateur IAM.

Services AWS maintenir et mettre à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent parfois des autorisations supplémentaires à une politique AWS gérée pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (jeux d'autorisations et rôles) auxquelles la politique est attachée. Les services sont plus susceptibles de mettre à jour une politique AWS gérée lorsqu'une nouvelle fonctionnalité est lancée ou lorsque de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques ne portent donc pas atteinte à vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique `ReadOnlyAccess` AWS gérée fournit un accès en lecture seule à toutes Services AWS les ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

Rubriques

- AWS politique gérée : Amazon ODBService RolePolicy

AWS politique gérée : Amazon ODBService RolePolicy

Vous ne pouvez pas associer `AmazonODBServiceRolePolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet d' Oracle Database@AWS effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour Oracle Database@AWS.

Pour en savoir plus sur la politique, y compris la dernière version du document de politique JSON, consultez Amazon ODBService RolePolicy dans le AWS Managed Policy Reference Guide.

Oracle Database@AWS authentification et autorisation dans OCI

Lorsque vous créez AWS APIs des ressources pour Oracle Database@AWS, ces ressources résident logiquement dans votre location Oracle Cloud Infrastructure (OCI) associée. Pour déployer ces ressources, AWS communiquez avec OCI APIs en votre nom. Pour atténuer le problème confus des adjoints, OCI peut être Oracle Database@AWS utilisé AWS STS en tant qu'entité de confiance et transférer les sessions d'accès pour autoriser votre intention d'utiliser l'OCI APIs dans votre location liée. Par conséquent, les événements sont enregistrés pour l'`sts:getCallerIdentity`API à partir de l'espace IP OCI dans l'historique de vos AWS CloudTrail parcours et événements. Attendez-vous à ces événements lorsque vous utilisez Oracle Database@AWS APIs.

Résolution des problèmes Oracle Database@AWS d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation d'Oracle Database@AWS et d'IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Oracle Database@AWS
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes Oracle Database@AWS ressources

Je ne suis pas autorisé à effectuer une action dans Oracle Database@AWS

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `odb:`*`GetWidget`* fictives.

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

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `odb:GetWidget`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Oracle Database@AWS.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Oracle AWS Database@. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes Oracle Database@AWS ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d’informations, consultez les éléments suivants :

- Pour savoir si Oracle Database@AWS prend en charge ces fonctionnalités, consultez. Comment Oracle Database@AWS fonctionne avec IAM
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d’identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d’identité) dans le Guide de l’utilisateur IAM.
- Pour en savoir plus sur la différence entre l’utilisation des rôles et des politiques basées sur les ressources pour l’accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l’utilisateur IAM.

Validation de conformité pour Oracle Database@AWS

Lorsque vous utilisez Oracle Database@AWS , votre responsabilité en matière de conformité dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. La documentation d'Oracle sur la conformité dans le cloud est disponible sur le site Web d'Oracle

Résilience dans Oracle Database@AWS

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d’une zone à l’autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l’échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS mondiale, Oracle Database@AWS propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

Utilisation de rôles liés à un service pour Oracle Database@AWS

Oracle Database@AWS utilise des Gestion des identités et des accès AWS rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. Oracle Database@AWS Les rôles liés au service sont prédéfinis Oracle Database@AWS et incluent toutes les autorisations dont le service a besoin pour appeler d'autres personnes en votre Services AWS nom.

Un rôle lié à un service facilite son utilisation Oracle Database@AWS car il n'est pas nécessaire d'ajouter manuellement les autorisations nécessaires. Oracle Database@AWS définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul Oracle Database@AWS peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer les rôles uniquement après la suppression préalable de leurs ressources connexes. Cela protège vos Oracle Database@AWS ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Autorisations de rôle liées à un service pour Oracle Database@AWS

Oracle Database@AWS utilise le rôle lié à un service nommé AWSService RoleFor ODB pour permettre d'appeler Oracle Database@AWS au Services AWS nom de vos ressources.

Le rôle lié à un service AWSService RoleFor ODB fait confiance aux services suivants pour assumer le rôle :

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

Ce rôle lié à un service est associé à une politique appelée `AmazonODBServiceRolePolicy` qui lui accorde l'autorisation d'opérer dans votre compte. Pour de plus amples informations, veuillez consulter AWS politique gérée : Amazon ODBService RolePolicy.

> **Note**
>
> Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Si vous rencontrez le message d'erreur suivant :
> Impossible de créer la ressource. Vérifiez que vous êtes autorisé à créer un rôle lié à un service. Dans le cas contraire, attendez et réessayez ultérieurement.
> Vérifiez que les autorisations suivantes sont activées :
>
> ```
> {
>     "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"
>         }
>     }
> }
> ```
>
> Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour Oracle Database@AWS

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez une base de données Exadata, Oracle Database@AWS crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez une base de données Exadata, le rôle lié au service est à nouveau Oracle Database@AWS créé pour vous.

Modification d'un rôle lié à un service pour Oracle Database@AWS

Oracle Database@AWS ne vous permet pas de modifier le rôle lié au service AWSService RoleFor ODB. Après avoir créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Toutefois, vous pouvez modifier la description

du rôle à l'aide d'IAM. Pour plus d'informations, consultez la section Modification d'un rôle lié à un service dans le Guide de l'utilisateur d'IAM.

Supprimer un rôle lié à un service pour Oracle Database@AWS

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Toutefois, vous devez supprimer toutes vos ressources avant de pouvoir supprimer le rôle lié à un service.

Nettoyage d'un rôle lié à un service pour Oracle Database@AWS

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service, vous devez d'abord vérifier qu'aucune session n'est active pour le rôle et supprimer toutes les ressources utilisées par le rôle.

Pour vérifier si une session est active pour le rôle lié à un service dans la console IAM

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le panneau de navigation de la console IAM, choisissez Rôles. Choisissez ensuite le nom (et non la case à cocher) du rôle AWSService RoleFor ODB.
3. Sur la page Summary (Récapitulatif) du rôle sélectionné, choisissez l'onglet Access Advisor.
4. Dans l'onglet Access Advisor, consultez l'activité récente pour le rôle lié à un service.

> **Note**
>
> Si vous ne savez pas si le rôle AWSService RoleFor ODB Oracle Database@AWS est utilisé, vous pouvez essayer de le supprimer. Si le service utilise le rôle, la suppression échoue et vous pouvez voir Régions AWS où le rôle est utilisé. Si le rôle est utilisé, vous devez attendre que la session se termine avant de pouvoir le supprimer. Vous ne pouvez pas révoquer la session d'un rôle lié à un service.

Si vous souhaitez supprimer le rôle AWSService RoleFor ODB, vous devez d'abord supprimer toutes vos Oracle Database@AWS ressources.

Régions prises en charge pour les rôles Oracle Database@AWS liés à un service

Oracle Database@AWS prend en charge l'utilisation de rôles liés au service partout Régions AWS où le service est disponible. Pour plus d'informations, consultez Régions AWS and Endpoints.

Oracle Database@AWS mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées Oracle Database@AWS depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique du Oracle Database@AWS document.

Modifier	Description	Date
Autorisations de rôle liées à un service pour Oracle Database@AWS : mise à jour de la politique existante	Oracle Database@AWS a ajouté de nouvelles autorisations `AmazonODBServiceRolePolicy` au rôle `AWSServiceRoleForODB` lié au service. Ces autorisations permettent Oracle Database@AWS d'effectuer les opérations suivantes : • Décrire les pièces jointes Amazon VPC Transit Gateway • Décrire les EC2 pièces jointes Amazon • Activer une EventBridge source Amazon Pour de plus amples informations, veuillez consulter Autorisations de rôle liées à un service pour Oracle Database@AWS.	30 juin 2025
Autorisations de rôle liées à un service pour Oracle Database@AWS : mise à jour de la politique existante	Oracle Database@AWS a ajouté de nouvelles autorisations `AmazonODBServiceRolePolicy` au rôle `AWSServiceRoleForODB` lié au service. Ces autorisations permettent Oracle Database@AWS d'effectuer les opérations suivantes :	26 juin 2025

Modifier	Description	Date
	• Décrire une EventBridge source Amazon • Décrire et créer un bus d'événements Pour de plus amples informations, veuillez consulter Autorisations de rôle liées à un service pour Oracle Database@AWS.	
AWS politique gérée : Amazon ODBService RolePolicy— Nouvelle politique de rôles liés aux services	Oracle Database@AWS a ajouté le `AmazonODB ServiceRolePolicy` pour le rôle `AWSServic eRoleForODB` lié au service. Pour de plus amples informations, veuillez consulter AWS politique gérée : Amazon ODBService RolePolicy.	2 décembre 2024
Oracle Database@AWS a commencé à suivre les modifications	Oracle Database@AWS a commencé à suivre les modifications apportées AWS à ses politiques gérées.	2 décembre 2024

Surveillance d'Oracle Database@AWS

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité Oracle Database@AWS et des performances de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller Oracle Database@AWS, signaler tout problème et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez CloudWatch suivre l'utilisation du processeur ou d'autres indicateurs de vos EC2 instances Amazon et lancer automatiquement de nouvelles instances en cas de besoin. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.
- Amazon CloudWatch Logs vous permet de surveiller, de stocker et d'accéder à vos fichiers journaux à partir d' EC2 instances Amazon et d'autres sources. CloudTrail CloudWatch Les journaux peuvent surveiller les informations contenues dans les fichiers journaux et vous avertir lorsque certains seuils sont atteints. Vous pouvez également archiver vos données de journaux dans une solution de stockage hautement durable. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon CloudWatch Logs.
- Amazon EventBridge peut être utilisé pour automatiser vos AWS services et répondre automatiquement aux événements du système, tels que les problèmes de disponibilité des applications ou les modifications des ressources. Les événements AWS liés aux services sont diffusés EventBridge en temps quasi réel. Vous pouvez écrire des règles simples pour préciser les événements qui vous intéressent et les actions automatisées à effectuer quand un événement correspond à une règle. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.
- AWS CloudTrailcapture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.

Surveillance Oracle Database@AWS avec Amazon CloudWatch

Vous pouvez surveiller Oracle Database@AWS l'utilisation CloudWatch, qui collecte les données brutes et les transforme en indicateurs lisibles en temps quasi réel. Ces statistiques sont enregistrées pour une durée de 15 mois ; par conséquent, vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue de la façon dont votre service ou application web s'exécute. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

CloudWatch Métriques Amazon pour Oracle Database@AWS

Le Oracle Database@AWS service transmet des métriques à Amazon CloudWatch dans l'espace de `AWS/ODB` noms pour les clusters de machines virtuelles, les bases de données de conteneurs et les bases de données enfichables.

Rubriques

- Mesures pour les clusters de machines virtuelles dans le cloud
- Métriques pour les bases de données de conteneurs
- Métriques pour les bases de données enfichables

Mesures pour les clusters de machines virtuelles dans le cloud

Le Oracle Database@AWS service indique les métriques suivantes dans l'espace de `AWS/ODB` noms des clusters de machines virtuelles dans le cloud.

Métrique	Description	Uunités
`ASMDiskgroupUtilization`	Pourcentage d'espace utilisable utilisé dans un groupe de disques. L'espace utilisable est l'espace disponible pour la croissance. Le groupe de disques DATA stocke nos fichiers de base de données Oracle. Le groupe de disques RECO contient des fichiers de	Pourcentage

Métrique	Description	Uunités
	base de données destinés à la restauration, tels que des archives et des journaux de flashback.	
`CpuUtilization`	Pourcentage d'utilisation du processeur.	Pourcentage
`FilesystemUtilization`	Pourcentage d'utilisation du système de fichiers provisionné.	Pourcentage
`LoadAverage`	Charge moyenne du système sur 5 minutes.	Entier
`MemoryUtilization`	Pourcentage de mémoire disponible pour démarrer de nouvelles applications, sans échange. La mémoire disponible peut être obtenue à l'aide de la commande suivante : `cat /proc/meminfo`	Pourcentage
`NodeStatus`	Indique si l'hôte est joignable.	Entier
`OcpusAllocated`	Le nombre de personnes OCPUs allouées.	Entier
`SwapUtilization`	Pourcentage d'utilisation de l'espace de swap total.	Pourcentage

Métriques pour les bases de données de conteneurs

Le Oracle Database@AWS service indique les métriques suivantes dans l'espace de `AWS/ODB` noms des bases de données de conteneurs.

Métrique	Description	Uunités
`BlockChanges`	Le nombre moyen de blocs modifiés par seconde.	Changements par seconde
`CpuUtilization`	L'utilisation du processeu r exprimée en pourcenta ge, agrégée pour tous les groupes de consommateurs. Le pourcentage d'utilisation est indiqué par rapport au nombre CPUs de bases de données autorisées à utiliser, soit deux fois le nombre de OCPUs.	Pourcentage
`CurrentLogons`	Le nombre de connexions réussies pendant l'intervalle sélectionné.	Nombre
`ExecuteCount`	Nombre d'appels utilisateur et récursifs ayant exécuté des instructions SQL pendant l'intervalle sélectionné.	Nombre
`ParseCount`	Le nombre d'analyses complètes et logicielles pendant l'intervalle sélection né.	Nombre
`StorageAllocated`	Quantité totale d'espace de stockage allouée à la base de données au moment de la collecte.	Go
`StorageAllocatedBy Tablespace`	Quantité totale d'espace de stockage allouée au tablespac e au moment de la collecte.	Go

Métrique	Description	Uunités
	Dans le cas d'une base de données de conteneurs, cette métrique fournit des tablespaces de conteneur racine.	
`StorageUsed`	Quantité totale d'espace de stockage utilisée par la base de données au moment de la collecte.	Go
`StorageUsedByTablespace`	Quantité totale d'espace de stockage utilisée par le tablespace au moment de la collecte. Dans le cas d'une base de données de conteneurs, cette métrique fournit des tablespaces de conteneur racine.	Go
`StorageUtilization`	Pourcentage de la capacité de stockage allouée actuellement utilisée. Représente l'espace total alloué pour tous les tablespaces.	Pourcentage
`StorageUtilizationByTablespace`	Cela indique le pourcentage d'espace de stockage utilisé par le tablespace au moment de la collecte. Dans le cas d'une base de données de conteneurs, cette métrique fournit des tablespaces de conteneur racine.	Pourcentage

Métrique	Description	Uunités
`TransactionCount`	Le nombre combiné de validations et d'annulations utilisateur pendant l'intervalle sélectionné.	Nombre
`UserCalls`	Le nombre combiné d'appels d'ouverture de session, d'analyse et d'exécution pendant l'intervalle sélection né.	Nombre

Métriques pour les bases de données enfichables

Le Oracle Database@AWS service indique les métriques suivantes dans l'espace de `AWS/ODB` noms pour les bases de données enfichables.

Métrique	Description	Uunités
`AllocatedStorageUtilizationByTablespace`	Pourcentage d'espace utilisé par le tablespace, par rapport à l'ensemble des espaces alloués. Pour les bases de données de conteneurs, cette métrique fournit des données pour les tablespaces de conteneurs racines. (Statisti que : moyenne, intervalle : 30 minutes)	Pourcentage
`AvgGCCRBlockReceiveTime`	Durée moyenne de réception des blocs CR (lecture cohérente) du cache global. Pour les bases de données RAC/cluster uniquemen	Millisecondes

Métrique	Description	Uunités
	t. (Statistique : moyenne, intervalle : 5 minutes)	
`AvgGCCurrentBlockReceiveTime`	Durée moyenne de réception des blocs actuels du cache global. Les statistiques indiquent la valeur moyenne. Pour les bases de données Real Application Cluster (RAC) uniquement. (Statistique : moyenne, intervalle : 5 minutes)	Millisecondes
`BlockChanges`	Le nombre moyen de blocs modifiés par seconde. (Statistique : moyenne, intervalle : 1 minute)	changements par seconde
`BlockingSessions`	Sessions de blocage en cours. Non applicable aux bases de données de conteneurs. (Statistique : maximum, intervalle : 15 minutes)	Nombre
`CPUTimeSeconds`	Taux moyen d'accumulation du temps processeur par les sessions de premier plan dans l'instance de base de données au cours de l'intervalle de temps. La composante temps processeur de la moyenne des sessions actives. (Statistique : moyenne, intervalle : 1 minute)	Secondes par seconde
`CpuCount`	Le nombre de CPUs pendant l'intervalle sélectionné.	Nombre

Métrique	Description	Uunités
`CpuUtilization`	L'utilisation du processeu r exprimée en pourcenta ge, agrégée pour tous les groupes de consommateurs. Le pourcentage d'utilisation est indiqué par rapport au nombre CPUs de bases de données autorisées à utiliser, soit deux fois le nombre de OCPUs. (Statistique : moyenne, intervalle : 1 minute)	Pourcentage
`CurrentLogons`	Le nombre de connexions réussies pendant l'intervalle sélectionné. (Statistiques : somme, intervalle : 1 minute)	Nombre
`DBTimeSeconds`	Taux moyen d'accumulation du temps de base de données (CPU + attente) par les sessions de premier plan dans l'instance de base de données au cours de l'intervalle de temps. Également connu sous le nom de sessions actives moyennes. (Statistique : moyenne, intervalle : 1 minute)	Secondes par seconde

Métrique	Description	Uunités
`DbmgmtJobExecutionsCount`	Nombre d'exécutions de tâches SQL sur une seule base de données gérée ou un groupe de bases de données, ainsi que leur statut. Les dimensions du statut peuvent être les valeurs suivantes : « Successed », « Failed », «InProgress. » (Statistique : somme, intervalle : 1 minute)	Nombre
`ExecuteCount`	Nombre d'appels utilisateur et récursifs ayant exécuté des instructions SQL pendant l'intervalle sélectionné. (Statistique : somme, intervalle : 1 minute)	Nombre
`FRASpaceLimit`	Limite d'espace de la zone de restauration rapide. Non applicable aux bases de données enfichables. (Statistique : maximum, intervalle : 15 minutes)	Go
`FRAUtilization`	L'utilisation de la zone de restauration rapide. Non applicable aux bases de données enfichables. (Statistique : moyenne, intervalle : 15 minutes)	Pourcentage

Métrique	Description	Uunités
GCCRBlocksReceived	Les blocs CR (lecture cohérente) du cache global reçus par seconde. Pour les bases de données RAC/cluster uniquement. (Statistique : moyenne, intervalle : 5 minutes)	Blocs par seconde
GCCurrentBlocksReceived	Représente les blocs actuels du cache global reçus par seconde. Les statistiques indiquent la valeur moyenne. Pour les bases de données Real Application Cluster (RAC) uniquement. (Statistique : moyenne, intervalle : 5 minutes)	Blocs par seconde
IOPS	Nombre moyen d'opérations d'entrée-sortie par seconde. (Statistique : moyenne, intervalle : 1 minute)	Opérations par seconde
IOThroughputMB	Débit moyen en Mo par seconde. (Statistique : moyenne, intervalle : 1 minute)	Mo par seconde
InterconnectTrafficMB	Taux moyen de transfert de données entre nœuds. Pour les bases de données RAC/cluster uniquement. (Statistique : moyenne, intervalle : 5 minutes)	Mo par seconde

Métrique	Description	Uunités
`InvalidObjects`	Nombre d'objets de base de données non valide. Non applicable aux bases de données de conteneur s. (Statistique : maximum, intervalle : 24 heures)	Nombre
`LogicalBlocksRead`	Nombre moyen de blocs lus SGA/Memory (cache tampon) par seconde. (Statistique : moyenne, intervalle : 1 minute)	Lectures par seconde
`MaxTablespaceSize`	Taille maximale possible du tablespace. Pour les bases de données de conteneurs, cette métrique fournit des données pour les tablespaces de conteneurs racines. (Statisti que : maximum, intervalle : 30 minutes)	Go
`MemoryUsage`	Taille totale du pool de mémoire en Mo. (Statisti que : moyenne, intervalle : 15 minutes)	Mo
`MonitoringStatus`	État de surveillance de la ressource. Si la collecte d'une métrique échoue, les informati ons d'erreur sont capturées dans cette métrique. (Statisti que : moyenne, intervalle : 5 minutes)	Non applicable

Métrique	Description	Uunités
`NonReclaimableFRA`	La zone de récupération rapide non récupérable. Non applicable aux bases de données enfichables. (Statistique : moyenne, intervalle : 15 minutes)	Pourcentage
`OcpusAllocated`	Le nombre réel de personnes OCPUs allouées par le service pendant l'intervalle de temps sélectionné. (Statistique : nombre, intervalle : 1 minute)	Entier
`ParseCount`	Le nombre d'analyses complètes et logicielles pendant l'intervalle sélectionné. (Statistique : somme, intervalle : 1 minute)	Nombre
`ParsesByType`	Le nombre d'analyses physiques ou logicielles par seconde. (Statistique : moyenne, intervalle : 1 minute)	Analyses par seconde
`ProblematicScheduledDBMSJobs`	Les tâches de base de données planifiées problématiques comptent. Non applicable aux bases de données de conteneurs. (Statistique : maximum, intervalle : 15 minutes)	Nombre

Métrique	Description	Uunités
`ProcessLimitUtilization`	Le processus limite l'utilisation. Non applicable aux bases de données enfichables. (Statistique : moyenne, intervalle : 1 minute)	Pourcentage
`Processes`	Les processus de base de données comptent. Non applicable aux bases de données enfichables. (Statistique : maximum, intervalle : 1 minute)	Nombre
`ReclaimableFRA`	La zone de récupération rapide récupérable. Non applicable aux bases de données enfichables. (Statistique : moyenne, intervalle : 15 minutes)	Pourcentage
`ReclaimableFRASpace`	L'espace récupérable de la zone de récupération rapide. Non applicable aux bases de données enfichables. (Statistique : moyenne, intervalle : 15 minutes)	Go
`RedoSizeMB`	La quantité moyenne de redo générée, en Mo par seconde. (Statistique : moyenne, intervalle : 1 minute)	Mo par seconde

Métrique	Description	Uunités
`SessionLimitUtilization`	La session limite l'utilisation. Non applicable aux bases de données enfichables. (Statistique : moyenne, intervalle : 1 minute)	Pourcentage
`Sessions`	Nombre de sessions dans la base de données. (Statistique : moyenne, intervalle : 1 minute)	Nombre
`StorageAllocated`	La quantité maximale d'espace allouée par tablespace pendant l'intervalle. Pour les bases de données de conteneurs, cette métrique fournit des données pour les tablespaces de conteneurs racines. (Statistique : maximum, intervalle : 30 minutes)	Go
`StorageAllocatedByTablespace`	La quantité maximale d'espace allouée par tablespace pendant l'intervalle. Pour les bases de données de conteneurs, cette métrique fournit des données pour les tablespaces de conteneurs racines. (Statistique : maximum, intervalle : 30 minutes)	Go

Métrique	Description	Uunités
StorageUsed	La quantité maximale d'espace utilisée pendant l'intervalle. (Statistique : maximum, intervalle : 30 minutes)	Go
StorageUsedByTablespace	La quantité maximale d'espace utilisée par le tablespace pendant l'interva lle. Pour les bases de données de conteneurs, cette métrique fournit des données pour les tablespaces de conteneur s racines. (Statistique : maximum, intervalle : 30 minutes)	Go
StorageUtilization	Pourcentage de la capacité de stockage allouée actuellem ent utilisée. Représente l'espace total alloué pour tous les tablespaces. (Statisti que : moyenne, intervalle : 30 minutes)	Pourcentage
StorageUtilization ByTablespace	Pourcentage de l'espace utilisé, par tablespace. Pour les bases de données de conteneurs, cette métrique fournit des données pour les tablespaces de conteneur s racines. (Statistique : moyenne, intervalle : 30 minutes)	Pourcentage

Métrique	Description	Uunités
`TransactionCount`	Le nombre combiné de validations et d'annulations utilisateur pendant l'interva lle sélectionné. (Statistique : somme, intervalle : 1 minute)	Nombre
`TransactionsByStatus`	Le nombre de transacti ons validées ou annulées par seconde. (Statistique : moyenne, intervalle : 1 minute)	Transactions par seconde
`UnusableIndexes`	Les index inutilisables sont pris en compte dans le schéma de base de données. Non applicable aux bases de données de conteneur s. (Statistique : maximum, intervalle : 24 heures)	Nombre
`UsableFRA`	La zone de récupération rapide utilisable. Non applicabl e aux bases de données enfichables. (Statistique : moyenne, intervalle : 15 minutes)	Pourcentage
`UsedFRASpace`	L'utilisation de l'espace dans la zone de restauration rapide. Non applicable aux bases de données enfichables. (Statisti que : maximum, intervalle : 15 minutes)	Go

Métrique	Description	Uunités
`UserCalls`	Le nombre combiné d'appels d'ouverture de session, d'analyse et d'exécution pendant l'intervalle sélection né. (Statistique : somme, intervalle : 1 minute)	Nombre
`WaitTimeSeconds`	Taux moyen d'accumul ation du temps d'attente non inactif par les sessions de premier plan dans l'instanc e de base de données au cours de l'intervalle de temps. Composant du temps d'attente de Average Active Sessions. (Statistique : moyenne, intervalle : 5 minutes)	Secondes par seconde

CloudWatch Dimensions Amazon pour Oracle Database@AWS

Vous pouvez filtrer Oracle Database@AWS les données des métriques en utilisant n'importe quelle dimension dans le tableau suivant.

Dimension	Filtre les données demandées pour . . .
`cloudVmClusterId`	Identifiant d'un cluster de machines virtuelles.
`cloudExadataInfras tructureId`	Identifiant de l'infrastructure Exadata.
`collectionName`	Le nom d'une collection.
`deploymentType`	Le type d'infrastructure.
`diskgroupName`	Nom d'un groupe de disques

Dimension	Filtre les données demandées pour . . .
errorCode	Un code d'erreur.
errorSeverity	La gravité d'une erreur.
filesystemName	Le nom d'un système de fichiers.
hostName	Nom de la machine hôte.
instanceName	Nom d'une instance de base de données.
instanceNumber	Numéro d'instance d'une instance de base de données.
ioType	Type d' I/O opération.
jobId	Identifiant unique pour une tâche.
managedDatabaseGroupId	L'identifiant d'unManaged Database Group.
managedDatabaseId	L'identifiant d'unManaged Database.
memoryPool	Type de pool de mémoire.
memoryType	Type de mémoire.
ociCloudVmClusterId	Identifiant OCI d'un cluster de machines virtuelles.
ociCloudExadataInfrastructureId	Identifiant OCI de l'infrastructure Exadata.
parseType	Type d'analyse syntaxique.
resourceId	Identifiant d'une ressource.
resourceId_Database	Identifiant d'une base de données.
resourceId_DbNode	Identifiant d'un nœud de base de données.
resourceName	Nom d'une ressource.

Dimension	Filtre les données demandées pour . . .
`resourceName_Database`	Nom d'une base de données.
`resourceName_DbNode`	Nom d'un nœud de base de données.
`resourceType`	Type de base de données.
`schemaName`	Le nom d'un schéma.
`status`	État d'une base de données.
`tablespaceContents`	Le contenu d'un tablespace.
`tablespaceName`	Nom d'un tablespace.
`tablespaceType`	Type de tablespace.
`transactionStatus`	État d'une transaction.
`waitClass`	Une classe d'événements d'attente.

Surveillance Oracle Database@AWS des événements sur Amazon EventBridge

Vous pouvez surveiller les Oracle Database@AWS événements dans EventBridge, qui fournit un flux de données en temps réel provenant d'applications et de AWS services. EventBridge achemine ces données vers des cibles telles qu' AWS Lambda Amazon Simple Notification Service.

> **Note**
>
> EventBridge s'appelait auparavant Amazon CloudWatch Events. Pour plus d'informations, consultez EventBridge l'évolution d'Amazon CloudWatch Events dans le guide de EventBridge l'utilisateur Amazon.

Vue d'ensemble des Oracle Database@AWS événements

Oracle Database@AWS les événements sont des messages structurés qui indiquent des changements dans le cycle de vie des ressources. Un bus d'événements est un routeur qui reçoit des événements et les transmet à zéro ou plusieurs destinations, ou cibles. Oracle Database@AWS les événements peuvent être générés à partir des sources suivantes :

Evénements de AWS

Ces événements sont générés Oracle Database@AWS APIs sur le AWS côté et sont transmis au bus d'événements par défaut de votre Compte AWS.

Événements de l'OCI

Ces événements sont générés directement à partir d'OCI, tels que les événements liés à l'infrastructure Oracle Exadata ou aux clusters de machines virtuelles. Lorsque vous vous abonnez à Oracle Database@AWS, un bus d'événements avec préfixe `aws.partner/odb/` est créé dans votre répertoire Compte AWS pour recevoir les événements de l'OCI.

Oracle Database@AWS événements de AWS

Oracle Database@AWS les événements AWS incluent les modifications du cycle de vie liées au réseau ODB lors de la création et de la suppression. Ces événements sont transmis au bus d'événements par défaut de votre Compte AWS. Le type de livraison est le meilleur effort.

Événements du réseau ODB

Événement	ID de l'événement	Message
Création	ODB-ÉVÉNEMENT-0001	Réseau ODB ODBNet_ID créé avec succès
Échec de la création	ODB-ÉVÉNEMENT-0011	Impossible de créer le réseau ODB ODBNet_ID
Suppression	ODB-ÉVÉNEMENT-0002	Réseau ODB ODBNet_ID supprimé avec succès
Échec de la suppression	ODB-ÉVÉNEMENT-0012	Impossible de supprimer le réseau ODB ODBNet_ID

Exemple : événement de création d'un réseau ODB

L'exemple suivant montre un événement lié à la réussite de la création d'un réseau 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 événements de l'OCI

La plupart des événements sont générés directement à partir de l'OCI. Oracle Database@AWS crée un bus d'événements avec le préfixe `aws.partner/odb/` « your » Compte AWS pour recevoir les événements de l'OCI. Nous vous recommandons de ne pas supprimer ce bus d'événements.

OCI propose des types d'événements complets, notamment les suivants :

- Infrastructure Oracle Exadata
- Événements relatifs aux clusters de machines virtuelles
- Événements CDB
- Événements PDB

Pour plus d'informations sur les types d'événements spécifiques et les détails pris en charge par OCI, consultez Oracle Exadata Database Service sur les événements d'infrastructure dédiés et les événements pour une base de données autonome sur une infrastructure Exadata dédiée.

Filtrage Oracle Database@AWS des événements

Vous pouvez suivre les bonnes pratiques EventBridge suggérées en matière de configuration des bus d'événements sur Event Bus sur Amazon EventBridge. En fonction de vos cas d'utilisation, vous pouvez définir des EventBridge règles pour filtrer les événements et des cibles pour recevoir et utiliser des événements.

Filtrage des événements réseau ODB à partir de AWS

Pour les événements réseau ODB provenant de AWS, vous pouvez filtrer en utilisant le modèle d'événements suivant :

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

Vous pouvez appliquer ce modèle à l'aide de l' EventBridge `put-rule`API avec le bus d'événements par défaut. Pour plus d'informations, consultez PutRulele Amazon EventBridge API Reference.

Filtrer Oracle Database@AWS les événements depuis OCI

Pour les Oracle Database@AWS événements issus de l'OCI, vous pouvez configurer une règle à l'aide d'une commande similaire à l'exemple fourni PutRuledans le Amazon EventBridge API Reference. Respectez les consignes suivantes :

- Utilisez un modèle d'événement personnalisé en fonction des types d'événements que vous souhaitez filtrer.
- EventBusNameDéfini sur le nom du bus Oracle Database@AWS créé.

Pour plus d'informations sur la manière de filtrer les événements et de définir EventBridge des cibles entre les comptes, consultez la section Envoi et réception d'événements entre Comptes AWS les comptes sur Amazon EventBridge.

Oracle Database@AWS Événements de résolution des problèmes

Si vous rencontrez un problème avec l'organisation ou le contenu de l'événement, procédez comme suit :

- Pour les événements du réseau ODB, contactez AWS Support.
- Pour les Oracle Database@AWS événements autres que ceux du réseau ODB, contactez le support Oracle Cloud.

Pour de plus amples informations, veuillez consulter Obtenir de l'aide pour Oracle Database@AWS.

Journalisation des appels Oracle Database@AWS d'API à l'aide AWS CloudTrail

Oracle Database@AWS est intégré à AWS CloudTrailun service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS. CloudTrail capture tous les appels d'API Oracle Database@AWS sous forme d'événements. Les appels capturés incluent des appels provenant de la Oracle Database@AWS console et des appels de code vers les opérations de l' Oracle Database@AWS API. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite Oracle Database@AWS, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur root.
- Si la demande a été faite au nom d'un utilisateur du centre d'identité IAM.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

> **Note**
>
> Oracle Database@AWS enregistre les appels d'`GetCallerIdentity`API depuis AWS Security Token Service (STS) dans vos CloudTrail journaux. Ces appels d'API STS vérifient l'identité de Oracle Database@AWS lorsque vous interagissez avec OCI en votre nom. Ils constituent une partie normale et sécurisée des AWS opérations et n'exposent pas d'informations sensibles.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrailLake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console sont multirégionaux. Vous ne pouvez créer un journal de suivi en une ou plusieurs régions à l'aide de l' AWS CLI. Il est recommandé de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un journal de suivi pour une seule région, il convient de n'afficher que les événements enregistrés dans le journal de suivi pour une seule région Région AWS. Pour plus d'informations sur les journaux de suivi, consultez Créez un journal de suivi dans vos Compte AWS et Création d'un journal de suivi pour une organisation dans le AWS CloudTrail Guide de l'utilisateur.

Vous pouvez envoyer une copie de vos événements de gestion en cours dans votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter des requêtes SQL sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et

que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et requêtes de données sur les événements de Lake entraînent des coûts. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Oracle Database@AWS événements de gestion dans CloudTrail

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

Oracle Database@AWS enregistre toutes les opérations Oracle Database@AWS du plan de contrôle en tant qu'événements de gestion.

Oracle Database@AWS exemples d'événements

Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre un CloudTrail événement illustrant l'`CreateOdbNetwork`opération.


```
{
    "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"
    }
}
```

Pour plus d'informations sur le contenu des CloudTrail enregistrements, voir le contenu des CloudTrail enregistrements dans le Guide de AWS CloudTrail l'utilisateur.

Résolution des problèmes liés à Oracle Database@AWS

Utilisez les sections suivantes pour résoudre les problèmes de réseau que vous pourriez rencontrer Oracle Database@AWS.

Rubriques

- La création du réseau ODB échoue
- Problèmes de connectivité entre votre réseau VPC et ODB ou vos clusters de machines virtuelles
- Noms d'hôte ou noms d'analyse non résolus des clusters de machines virtuelles à partir d'un VPC
- Obtenir de l'aide pour Oracle Database@AWS

La création du réseau ODB échoue

Lorsque vous ne parvenez pas à créer un réseau ODB, les causes suivantes sont courantes :

Plages CIDR restreintes

Le réseau ODB utilise des plages CIDR spécifiques pour le client et les sous-réseaux de sauvegarde. Assurez-vous que les plages d'adresses CIDR que vous avez choisies pour ces sous-réseaux ne se chevauchent pas avec des plages d'adresses IP restreintes ou réservées.

Les plages CIDR suivantes sont réservées et ne peuvent pas être utilisées pour le réseau ODB :

- Plage réservée au cloud Oracle : 169,254,0,0/16
- Classe réservée D : 224.0.0.0 - 239.255.255.255
- Classe réservée E : 240.0.0.0 - 255.255.255.255
- Utilisation future de l'OCI : 100.105.0.0/16

Suivez les EC2 règles relatives aux plages CIDR décrites dans la documentation VPC. Pour en savoir plus, consultez la section Restrictions relatives aux associations de blocs CIDR.

En outre, évitez les chevauchements entre les plages CIDR spécifiées et celles utilisées pour la connectivité VPC au réseau ODB.

CIDR VPC qui se chevauche

La plage d'adresses CIDR que vous avez spécifiée pour le réseau ODB ne doit pas chevaucher les plages d'adresses CIDR utilisées par vos réseaux existants. VPCs Le chevauchement des

plages CIDR peut provoquer des conflits de routage et empêcher la création réussie du réseau ODB. Vérifiez les plages CIDR de l'appairage ODB VPCs et assurez-vous que le CIDR du réseau ODB est unique et ne se chevauche pas.

Propriété de VPCs

Le réseau ODB et le VPC auquel vous vous connectez doivent appartenir au même compte. AWS Si vous essayez de relier le réseau ODB à un VPC appartenant à un autre compte, la création échouera. Vérifiez que le réseau ODB et le VPC sont tous deux détenus par le AWS même compte.

Absence de passerelle de transit

Si vous ajoutez une plage d'adresses CIDR à la liste d'adresses CIDR homologues du réseau ODB sans associer de passerelle de transit au VPC, l'opération de création ou de mise à jour échoue. Il n'existe aucune exigence concernant les plages CIDR pour lesquelles la pièce jointe est utilisée.

Problèmes de connectivité entre votre réseau VPC et ODB ou vos clusters de machines virtuelles

Lorsque vous ne parvenez pas à vous connecter depuis votre VPC au réseau ODB ou aux clusters de machines virtuelles qu'il contient, les causes suivantes sont courantes :

- Vérification de la configuration du VPC : dans la Oracle Database@AWS console, localisez le VPC connecté au réseau ODB. Vérifiez que l'ID VPC correspond à celui indiqué dans les détails du réseau ODB.
- Inspection des tables de routage : dans la console Amazon VPC, recherchez la table de routage attachée au sous-réseau sur lequel votre application est exécutée. Recherchez un itinéraire dont le CIDR de destination correspond au CIDR du sous-réseau client du réseau ODB. Vérifiez que cette route pointe vers le bon ARN du réseau ODB. Si la route est manquante, ajoutez-en une nouvelle au CIDR du sous-réseau client du réseau ODB.
- Validation peered CIDRs — Consultez la `Peered CIDRs` section des détails du réseau ODB. Vérifiez que tous les blocs CIDR pertinents de votre VPC sont répertoriés. S'il manque un CIDR requis, mettez à jour le CIDRs peered.
- Vérification des règles des groupes de sécurité : dans la EC2 console Amazon, localisez les groupes de sécurité pour les ressources de votre VPC. Passez en revue les règles entrantes et sortantes et mettez-les à jour si nécessaire pour autoriser le trafic nécessaire.

- Confirmation des zones de disponibilité : dans la console Amazon VPC, identifiez la zone de disponibilité (AZ) de votre sous-réseau. Vérifiez que le réseau ODB est également déployé dans la même zone de disponibilité que votre sous-réseau.
- Éviter de multiples connexions d'appairage réseau ODB : vérifiez vos connexions d'appairage VPC dans la console. Oracle Database@AWS Assurez-vous de n'avoir qu'une seule connexion active à un réseau ODB. Si vous constatez plusieurs peering sur le réseau ODB, supprimez les réseaux supplémentaires.

Noms d'hôte ou noms d'analyse non résolus des clusters de machines virtuelles à partir d'un VPC

Si les noms d'hôte ou de scan des clusters de machines virtuelles ne peuvent pas être résolus à partir de votre VPC, configurez le transfert DNS sur le VPC et les ressources suivantes pour résoudre les enregistrements DNS hébergés sur le réseau ODB :

- Un point de terminaison sortant pour envoyer des requêtes DNS au réseau ODB. Pour de plus amples informations, veuillez consulter Configuration d'un point de terminaison sortant dans un réseau ODB dans Oracle Database@AWS.
- Règle de résolution pour spécifier le nom de domaine des requêtes DNS que le résolveur transmet au réseau DNS pour ODB. Pour de plus amples informations, veuillez consulter Configuration d'une règle de résolution dans Oracle Database@AWS.

Obtenir de l'aide pour Oracle Database@AWS

Découvrez comment obtenir des informations et du support pour Oracle Database@AWS.

Étendue du support Oracle et informations de contact

Oracle Cloud Support est la première ligne d'assistance pour toutes les questions relatives à Oracle Database@AWS . Pour contacter le support, connectez-vous à la console Oracle Cloud Infrastructure (OCI), puis sélectionnez l'icône du radeau de sauvetage. Si vous n'avez pas de compte My Oracle Cloud Support, consultezComptes et accès My Oracle Cloud Support.

Voici quelques exemples de problèmes pour lesquels le Support Oracle peut vous aider :

- Problèmes de connexion à la base de données (Oracle TNS)

- Problèmes de performance de la base de données Oracle
- Résolution des erreurs de base de données Oracle
- Problèmes de réseau liés aux communications avec le locataire OCI associé au service
- Le quota (limites) augmente pour recevoir plus de capacité (pour plus d'informations, voir Demande d'augmentation des limites pour les ressources de base de données)
- Mise à l'échelle pour augmenter la capacité de calcul et de stockage de votre infrastructure de base de données Oracle
- Mises à niveau matérielles de nouvelle génération
- Problèmes de facturation liés à vos AWS Marketplace frais

Si vous devez contacter le support Oracle en dehors de la console OCI, indiquez à votre agent de support Oracle que votre problème est lié à Oracle AWS Database@. Cela est dû au fait que les demandes relatives à ce service sont traitées par une équipe de support OCI spécialisée dans ces déploiements.

Contacter le support Oracle par téléphone

1. Appelez le 1 800 223-1711. Si vous résidez en dehors des États-Unis d'Amérique, consultez le répertoire mondial des contacts d'Oracle Support pour trouver les coordonnées de votre pays ou de votre région.
2. Choisissez l'option « 2 » pour ouvrir une nouvelle demande de service (SR).
3. Choisissez l'option « 4 » pour « incertain ».
4. Informez l'agent que vous rencontrez un problème avec votre système multicloud et indiquez-lui le nom du produit. Une demande de service interne sera ouverte en votre nom et un ingénieur du support OCI vous contactera directement.

Vous pouvez également poser une question sur le forum Multicloud de la communauté Cloud Customer Connect d'Oracle. Cette option est disponible pour tous les clients.

Comptes et accès My Oracle Cloud Support

Pour créer des tickets de demande de service My Oracle Cloud Support, l'administrateur du AWS service Oracle Database@ de votre organisation doit approuver votre demande. Si vous êtes l'AWS administrateur d'Oracle Database@, suivez les instructions d'intégration de My Oracle Cloud Support incluses dans l'e-mail d'activation du service Oracle AWS Database@.

Vous trouverez les instructions relatives à l'intégration auprès de My Oracle Cloud Support dans les rubriques suivantes :

- Configuration de votre compte Oracle Support
- Création d'une demande de Support

Pour savoir comment autoriser les utilisateurs à ouvrir les demandes d'assistance My Oracle Cloud Support, voir Tâches d'administrateur pour le support.

AWS Support champ d'application et informations de contact

AWS Support est votre première ligne d'assistance pour tous les AWS problèmes et questions connexes. Créez un AWS Support dossier pour votre problème, comme vous le faites pour les autres AWS services. L' AWS Support équipe collabore avec le support OCI selon les besoins.

Voici quelques exemples de AWS problèmes liés à Oracle Database@ susceptibles de vous aider : AWS Support

- Problèmes de réseau virtuel, y compris ceux liés à la traduction d'adresses réseau (NAT), aux pare-feux, au DNS et à la gestion du trafic, et aux AWS sous-réseaux
- Problèmes liés au Bastion et aux machines virtuelles (VM), notamment la connexion à l'hôte de base de données, l'installation du logiciel, la latence et les performances de l'hôte
- Rapports sur les métriques du cluster de machines virtuelles Exadata au sein d'Amazon CloudWatch
- Problèmes de facturation liés aux AWS services

Pour plus d'informations sur AWS Support, voir Commencer avec AWS Support.

Contrats de niveau de service Oracle

Si vous avez des questions concernant les accords de niveau de AWS service Oracle Database@ (SLAs) ou si vous souhaitez demander des crédits de service en cas de violation des SLA, contactez votre responsable de compte Oracle. Consultez les accords de niveau de service pour plus d'informations.

Quotas pour Oracle Database@AWS

Oracle Database@AWS est une offre multicloud. AWS ne définit ni n'impose de quotas pour les Oracle Database@AWS ressources. Les quotas sont appliqués par Oracle Cloud Infrastructure (OCI). Pour plus d'informations sur les quotas OCI, consultez la section Quotas et limites de service dans la documentation Oracle Cloud Infrastructure.

Historique du document pour le guide de Oracle Database@AWS l'utilisateur

Le tableau suivant décrit les versions de documentation pour Oracle Database@AWS.

Modification	Description	Date
Oracle Database@AWS soutient la région Asie-Pacifique (Sydney) et la région du Canada (centre)	Vous pouvez créer vos Oracle Database@AWS ressources dans ces régions. Pour plus d'informations, consultez la section Régions prises en charge pour Oracle Database@AWS.	2 février 2026
Oracle Database@AWS soutient la région Asie-Pacifique (Tokyo), la région USA Est (Ohio), la région Europe (Francfort)	Vous pouvez créer vos Oracle Database@AWS ressources dans ces régions. Pour plus d'informations, consultez la section Régions prises en charge pour Oracle Database@AWS.	22 décembre 2025
Oracle Database@AWS prend en charge le partage des droits entre Comptes AWS	Vous pouvez désormais partager les droits AWS Marketplace pour Oracle Database@ au AWS sein d'une même organisation Comptes AWS à l'aide de AWS License Manager. AWS Pour plus d'informations, voir Partage des droits dans Oracle AWS Database@.	19 décembre 2025
Oracle Database@AWS prend en charge la modification des	Oracle Database@AWS prend en charge la modificat	15 octobre 2025

filtres de données d'intégration Zero-ETL	ion des filtres de données pour les intégrations Zero-ETL existantes avec Amazon Redshift. Vous pouvez mettre à jour les modèles de filtre de données pour inclure ou exclure des schémas et des tables spécifiques de la réplication des données. Pour plus d'informations, consultez la section Gestion des intégrations Zero-ETL.	
Oracle Database@AWS prend en charge la gestion CIDR du réseau homologue pour les connexions d'appairage	Vous pouvez spécifier un réseau homologue CIDRs lorsque vous créez ou mettez à jour des connexions d'appairage ODB. Vous contrôlez les sous-réseaux du VPC homologue qui ont accès à votre réseau ODB. Un compte VPC peut mettre à jour les plages d'adresses CIDR sans être également propriétaire du réseau ODB. Pour plus d'informations, consultez Configuration de l'appairage ODB vers un Amazon VPC dans. Oracle Database@AWS	10 octobre 2025

Oracle Database@AWS prend en charge l'intégration zéro ETL avec Amazon Redshift	Oracle Database@AWS s'intègre désormais à VPC Lattice pour permettre une intégration zéro ETL avec Amazon Redshift. Pour plus d'informations, voir Intégrations de services pour Oracle AWS Database@.	2 juillet 2025
Mise à jour des autorisations de rôle lié à un service IAM	La `AmazonODBServiceRolePolicy` politique accorde désormais des autorisations supplémentaires pour décrire les pièces jointes à la passerelle de transit VPC, décrire les EC2 sous-réseaux Amazon et activer une source Amazon. EventBridge Pour plus d'informations, voir les Oracle Database@AWS mises à jour des politiques AWS gérées.	30 juin 2025
Mise à jour des autorisations de rôle lié à un service IAM	La `AmazonODBServiceRolePolicy` politique accorde désormais des autorisations supplémentaires pour décrire les événements dans Amazon EventBridge Scheduler et créer ou décrire un bus d'événements. Pour plus d'informations, voir les Oracle Database@AWS mises à jour des politiques AWS gérées.	26 juin 2025

Oracle Database@AWS soutient la région ouest des États-Unis (Oregon)	Vous pouvez créer vos Oracle Database@AWS ressources dans la région USA Ouest (Oregon). Les AZ physiques pris en charge IDs sont `usw2-az3` et `usw2-az4`. Pour plus d'informations, consultez la section Régions prises en charge pour Oracle Database@AWS.	26 juin 2025
Oracle Database@AWS soutient le partage des ressources entre Comptes AWS	Vous pouvez désormais partager l'infrastructure Exadata et les clusters de machines virtuelles avec d'autres membres de Comptes AWS votre organisation à l'aide de AWS Resource Access Manager (AWS RAM). Vous pouvez provisionner l'infrastructure une seule fois et la partager entre plusieurs comptes, réduisant ainsi les coûts tout en maintenant la séparation des responsabilités. Pour plus d'informations, voir Partage de ressources dans Oracle Database@AWS.	26 juin 2025

Oracle Database@AWS soutient les événements sur Amazon EventBridge	Oracle Database@AWS fournit des événements à Amazon EventBridge pour surveiller les modifications du cycle de vie des ressources. Les événements sont générés à la fois à partir de sources OCI AWS et vous permettent de suivre les modifications apportées au réseau ODB, à l'infrastructure Exadata, aux clusters de machines virtuelles et aux bases de données. Pour plus d'informations, consultez la section Surveillance Oracle Database@AWS des événements sur Amazon EventBridge.	26 juin 2025
Oracle Database@AWS prend en charge l'abonnement interrégional	Oracle Database@AWS prend en charge l'abonnement interrégional, vous permettant de vous abonner une seule fois et d'utiliser le service dans toutes les zones disponibles Régions AWS. Pour plus d'informations, voir S'abonner à Oracle Database@AWS dans plusieurs régions.	26 juin 2025

Oracle Database@AWS prend en charge les connexions d'appairage ODB en tant que ressource distincte	Les connexions d'appairage ODB constituent désormais une ressource distincte dédiée à APIs la création, à l'affichage et à la suppression de connexions d'appairage. Vous pouvez créer des connexions de peering entre un réseau ODB et un Amazon VPC sur le même compte ou sur des comptes différents. Pour plus d'informations, consultez la section Utilisation des connexions d'appairage ODB.	26 juin 2025
Oracle Database@AWS intègre le réseau ODB à Amazon S3	Oracle Database@AWS s'intègre désormais à VPC Lattice pour permettre des sauvegardes gérées par Oracle sur Amazon S3 et un accès direct au réseau ODB vers Amazon S3. Pour plus d'informations, voir Intégrations de services pour Oracle AWS Database@.	26 juin 2025

Oracle Database@AWS prend en charge les clusters de machines virtuelles autonomes	Vous pouvez désormais créer des clusters de machines virtuelles autonomes sur votre infrastructure Exadata. Les clusters de machines virtuelles autonomes sont des bases de données entièrement gérées qui automatisent les tâches de gestion clés à l'aide de l'apprentissage automatique et de l'IA. Pour plus d'informations, voir Étape 3 : Création d'un cluster de machines virtuelles Exadata ou d'un cluster de machines virtuelles autonome dans Oracle Database@AWS.	28 mai 2025
Oracle Database@AWS prend en charge les fenêtres de maintenance personnalisables	Vous pouvez désormais configurer des fenêtres de maintenance pour votre infrastructure Exadata avec des options pour les plannings gérés par Oracle ou gérés par le client. Vous pouvez également sélectionner les modes d'application des correctifs (roulants ou non roulants) et définir les préférences en matière de calendrier de maintenance. Pour plus d'informations, voir Création d'une infrastructure Oracle Exadata dans Oracle Database@AWS.	1er mai 2025

Oracle Database@AWS prend en charge une nouvelle zone de disponibilité (AZ)	Vous pouvez désormais créer un réseau ODB dans un AZ avec l'ID physique `use1-az4` ou`use1-az6`. Pour plus d'informations, consultez la section Infrastructure Oracle Exadata.	26 mars 2025
Oracle Database@AWS prend en charge les passerelles Amazon VPC Transit	Si vous connectez une passerelle de transit à un VPC connecté à un réseau ODB, vous pouvez en connecter plusieurs VPCs à cette passerelle. Les applications qui y sont exécutées VPCs peuvent accéder à un cluster de machines virtuelles Exadata exécuté sur votre réseau ODB. Pour plus d'informations, consultez Configuration des passerelles de transit Amazon VPC pour. Oracle Database@AWS	26 mars 2025
Oracle Database@AWS prend en charge les types de serveurs de base de données et de stockage pour Exadata X11M	Vous pouvez spécifier le type de serveur de base de données et le type de serveur de stockage lorsque vous créez une infrastructure à l'aide d'Exadata X11M. Pour plus d'informations, voir Création d'une infrastructure Oracle Exadata dans Oracle Database@AWS.	4 février 2025

Nouvelle politique relative aux rôles liés aux services	Oracle Database@AWS a ajouté une nouvelle politique `AmazonODBServiceRolePolicy` pour le rôle `AWSServiceRoleForODB` lié au service. Pour plus d'informations, consultez la rubrique Mises à jour Oracle Database@AWS des politiques gérées par AWS.	2 décembre 2024
Première version	Publication initiale du guide de Oracle Database@AWS l'utilisateur	2 décembre 2024

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.