aws

Management Guide

Amazon Redshift



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Redshift: Management Guide

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

..... xvii
Qu’est-ce qu’Amazon Redshift ? 1
Utilisez-vous pour la première fois Amazon Redshift ? 1
Présentation des fonctions d’Amazon Redshift sans serveur 2
Vue d’ensemble des clusters provisionnés Amazon Redshift 5
Gestion du cluster 6
Accès et sécurité des clusters 6
Surveillance des clusters 8
Bases de données 9
Comparaison entre Amazon Redshift sans serveur et un entrepôt des données mis en service par Amazon Redshift sans serveur 10
Utilisation des interfaces de gestion Amazon Redshift pour les clusters alloués 41
Utilisation des AWS SDK 42
Signature d'une requête HTTP 43
Configuration de la CLI Amazon Redshift 49
Amazon Redshift sans serveur 52
Qu’est-ce qu’Amazon Redshift sans serveur ? 52
Console Amazon Redshift sans serveur 53
Considérations relatives à l’utilisation d’Amazon Redshift sans serveur 57
Capacité de calcul pour Amazon Redshift sans serveur 62
Considérations et limitations de la capacité des points de terminaison sans serveur 64
AI-driven mise à l'échelle et optimisation 66
Facturation pour Amazon Redshift sans serveur 72
Facturation de la capacité de calcul 72
Facturation de la capacité de calcul à la demande 73
Facturation pour les réservations sans serveur 78
Facturation pour stockage 85
Utilisation de l’essai gratuit d’Amazon Redshift sans serveur 86
Notes d’utilisation de facturation 86
Amazon Redshift sans serveur avec regroupement des connexions 88
Optimisation des coûts pour Amazon Redshift sans serveur zéro ETL 90
Connexion à Amazon Redshift sans serveur 90
Connexion à Amazon Redshift sans serveur 91
Connexion à Amazon Redshift sans serveur via des pilotes JDBC 91

Connexion à Amazon Redshift sans serveur avec l'API de données 93
Se connecter avec SSL à Amazon Redshift sans serveur 93
Connexion à Amazon Redshift sans serveur à partir d'un point de terminaison de VPC géré par Amazon Redshift 96
Connexion à Amazon Redshift Serverless depuis un point de terminaison VPC d'interface (AWS PrivateLink) 96
Connexion à Amazon Redshift sans serveur à partir d'un point de terminaison d'un VPC Redshift dans un autre compte 96
Ressources supplémentaires 102
Définition des rôles de base de données à accorder aux utilisateurs fédérés 102
Définition des rôles de base de données 103
Cas d'utilisation pour définir les rôles de base de données à accorder aux utilisateurs fédérés 103
Ressources supplémentaires 105
Identity and Access Management dans Amazon Redshift Serverless 106
Octroi d'autorisations 106
Mise en route avec les informations d'identification IAM 108
Accès aux objets de base de données avec des autorisations de rôle de base de données . 109
Migration à partir d'un cluster provisionné vers Amazon Redshift sans serveur 111
Création d'un instantané de votre cluster alloué 111
Connexion à Amazon Redshift sans serveur à l'aide d'un pilote 112
Utilisation du kit SDK Amazon Redshift sans serveur 118
Groupe de travail et espace de noms 119
Groupes de travail et espaces de noms à l'aide de la console 119
Groupes de travail et espaces de noms utilisant le AWS Command Line Interface et API sans serveur Amazon Redshift 120
Groupes de travail 121
Espaces de noms 128
Surveillance des requêtes et des charges de travail 132
Ajout d'une politique de surveillance des requêtes 134
Octroi d'autorisations de surveillance des requêtes à un utilisateur 136
Octroi d'autorisations de surveillance des requêtes à un rôle 136
Définition des limites d'utilisation 137
Définition des limites des requêtes 138
Configuration des files d'attente de requêtes 138
Vérification des données récapitulatives à l'aide du tableau de bord 143

Journaux d'audit 144
Enregistrez les événements CloudWatch 144
CloudWatch métriques 145
Instantanés et points de récupération 154
AWS Backup intégration 156
Création d'un instantané 156
Création d'un instantané final 157
Partage d'un instantané ou suppression des autorisations relatives aux instantanés 158
Planification d'un instantané 158
Mise à jour d'une période de conservation des instantanés 162
Suppression d'un instantané 162
Restauration d'un instantané 163
Conversion d'un point de récupération 164
Restauration d'un point de récupération 165
Copier des sauvegardes vers un autre Région AWS 165
Restauration d'une table 167
Partage des données 168
Considérations 169
Octroi d'un accès pour afficher des unités de partage des données 169
Enregistrement d'espaces de noms dans le AWS Glue Data Catalog 170
Balisage de ressources 171
Clusters Amazon Redshift alloués 173
Clusters et nœuds 173
Détails de type de nœud 175
Détermination du nombre de nœuds 180
Utiliser EC2 pour créer votre cluster 180
Amazon Virtual Private Cloud (Amazon VPC) 181
Alarme d'espace disque par défaut 181
Statut du cluster 182
Considérations relatives à l'utilisation de clusters alloués 185
Considérations sur les régions et les zones de disponibilité 185
Maintenance du cluster 185
Opérations de cluster 202
Création d'un cluster 202
Création d'une alarme d'espace disque 206
Affichage d'un cluster 206

Modification d’un cluster 207
Redimensionnement d’un cluster 208
Renommer un cluster 227
Mise à niveau de la version d’un cluster 228
Suspension et reprise d’un cluster 229
Redémarrage d’un cluster 231
Relocalisation d’un cluster 232
Définition d'une limite d'utilisation 236
Arrêt et suppression d’un cluster 238
Instantanés et sauvegardes 239
Enregistrement d'un cluster auprès du AWS Glue Data Catalog 267
Multi-AZ déploiement 268
Configuration du Multi-AZ déploiement 268
Configuration Multi-AZ lors de la création d'un nouveau cluster 272
Configuration Multi-AZ d'un entrepôt de données restauré à partir d'un instantané 275
Conversion d'un entrepôt de Single-AZ données en entrepôt Multi-AZ de données 276
Conversion d'un entrepôt de Multi-AZ données en entrepôt Single-AZ de données 278
Redimensionnement d'un entrepôt Multi-AZ de données 279
Échec du Multi-AZ déploiement 280
Affichage des requêtes et des chargements pour les entrepôts Multi-AZ de données 282
Surveillance d'une requête dans un Multi-AZ déploiement 284
Résiliation d’une requête pour un cluster 284
Surveillance des performances de cluster 285
Données de performance 286
Consultation des données de performances 302
Analyse de l’exécution des requêtes 328
Création d'une alarme 330
Arrêt d’une requête en cours d’exécution 331
Statistiques de performance dans la CloudWatch console 331
Profileur de requêtes 333
Surveillance des requêtes et des bases de données 344
View-based Requêtes système et surveillance des bases de données 351
Suivis 354
Basculement entre les suivis 355
Suivis et restauration 355
Mise à jour des groupes de travail sans serveur 356

Gestion des versions 357
Déterminer la version du groupe de travail ou du cluster 357
Zero-ETL intégrations 359
Considérations 362
Considérations relatives à l'utilisation du mode historique sur la cible 364
Considérations lorsque la source d'intégration zéro ETL est Aurora ou Amazon RDS 365
Considérations lorsque la source d'intégration zéro ETL est DynamoDB 366
Points à prendre en compte lorsque la source d'intégration zéro ETL est constituée d'applications telles que Salesforce ServiceNow, SAP et Zendesk 367
Considérations à prendre en compte lors de la restauration d'une cible d'intégration Zéro ... 368
Considérations relatives au redimensionnement d'une cible d'intégration Zéro-ETL 369
Bien démarrer avec les intégrations zéro ETL 370
Création et configuration d'un entrepôt des données Amazon Redshift cible 370
Activation de la sensibilité à la casse 371
Configuration de l'autorisation dans Amazon Redshift 373
Création d'une intégration zéro ETL 378
Création de bases de données de destination 391
Interrogation de données répliquées 394
Interrogation de données répliquées avec des vues matérialisées 395
Interrogation des données répliquées à partir de DynamoDB 397
Affichage des intégrations zéro ETL 398
Mode historique 401
Partage de vos données 404
Surveillance des intégrations zéro ETL 405
Surveillance des intégrations zéro ETL aux vues système Amazon Redshift 405
Surveillance des intégrations Zéro ETL avec Amazon EventBridge 405
Métriques pour les intégrations zéro ETL 405
Modification d'une intégration zéro ETL pour DynamoDB 409
Suppression d'une intégration zéro ETL pour DynamoDB 410
Régions prises en charge 412
Aurora MySQL 412
Aurora PostgreSQL 414
Amazon DynamoDB 416
Amazon RDS for MySQL 418
Applications d'entreprise 419
Résolution des problèmes liés aux intégrations zéro ETL 421

Interroger une base de données ... 439
Connexion à Amazon Redshift ... 439
Interrogation d'une base de données à l'aide de Amazon Redshift Query Editor V2 ... 440
Configuration de votre Compte AWS ... 441
Ouverture de l'éditeur de requête v2 ... 449
Connexion à une base de données Amazon Redshift ... 455
Navigation dans une base de données Amazon Redshift ... 457
Création d'objets de base de données ... 459
Afficher l'historique des requêtes et des onglets ... 468
Interaction avec l'assistant SQL génératif Amazon Q ... 469
Chargement de données dans une base de données ... 483
Création de requêtes ... 493
Blocs-notes ... 500
Interrogation du AWS Glue Data Catalog ... 503
Interrogation d'un lac de données ... 507
Unités de partage des données ... 509
Requêtes planifiées ... 513
Visualisation des résultats ... 524
Collaborer et partager en équipe ... 529
Interrogation d'une base de données à l'aide de l'éditeur de requête v1 ... 531
Considérations ... 532
Connection à un entrepôt de données à l'aide des outils client SQL ... 533
Recommandations pour la connexion avec des outils clients ... 533
Configuration des connexions dans Amazon Redshift ... 534
Bonnes pratiques pour découvrir les métadonnées ... 754
Configuration des options de sécurité des connexions ... 762
Connexion à partir d'outils et de codes clients ... 772
Utilisation d'un profil d'authentification pour se connecter à Amazon Redshift ... 822
Résolution des problèmes de connexion dans Amazon Redshift ... 825
Utilisation de l'API de données ... 834
Utilisation de l'API de données ... 835
Considérations relatives à l'appel à l'API de données ... 836
Choix des informations d'authentification de la base de données ... 838
Mappage de types de données JDBC ... 840
Exécution d'instructions SQL avec des paramètres ... 841
Exécution d'instructions SQL avec un jeton d'idempotence ... 843

Exécution d’instructions SQL avec réutilisation de session ... 845
Récupération des résultats ... 846
Autorisation de l’accès ... 849
Propagation d’identité fiable ... 859
Appel à l’API de données ... 862
Résolution des problèmes liés à l’API de données ... 899
Planification des opérations de l'API Data avec Amazon EventBridge ... 900
Surveillance de l’API de données ... 904
Utilisation AWS KMS avec l'API Data ... 906
Utilisation d’Amazon Sagemaker Unified Studio ... 910
Groupes de paramètres ... 911
Valeurs des paramètres par défaut ... 912
Gestion de la charge de travail ... 914
Propriétés WLM dynamiques et statiques ... 915
Propriétés du paramètre de configuration de la gestion de la charge de travail ... 915
Configuration du paramètre WLM à l'aide du AWS CLI ... 923
Création d'un groupe de paramètres ... 931
Modification d'un groupe de paramètres ... 932
Création d’une règle de surveillance de requête ... 937
Suppression d'un groupe de paramètres ... 938
Intégrer avec un AWS partenaire ... 939
Chargement de données avec AWS partenaires ... 940
Nœuds réservés ... 942
Offres relatives aux nœuds réservés ... 942
Comparaison de prix entre les offres de nœuds réservés ... 943
Fonctionnement des nœuds réservés ... 945
Nœuds réservés et facturation consolidée ... 946
Points à prendre en compte avant de modifier le type de nœud sur un cluster qui utilise des instances réservées ... 947
Exemples de nœuds réservés ... 947
Exemple 1 ... 947
Exemple 2 ... 947
Exemple 3 ... 948
Exemple 4 ... 948
Exemple 5 ... 948
Exemple 6 ... 948

Achat d'un nœud réservé ... 949
Sécurité ... 952
Protection des données ... 954
Chiffrement des données ... 955
Création de jetons de données ... 976
Routage du trafic inter-réseaux ... 977
Gestion des identités et des accès ... 977
Authentification par des identités ... 978
Cross-service prévention adjointe confuse ... 979
Contrôle d'accès ... 981
Présentation de la gestion des accès ... 981
Utilisation des politiques basées sur une identité (politiques IAM) ... 989
Fédération de fournisseurs d'identité (IdP) natifs ... 1054
Utilisation des rôles liés à un service ... 1091
Utilisation de l'authentification IAM pour générer des informations d'identification de l'utilisateur de base de données ... 1100
Autoriser l'accès aux services AWS ... 1161
Gestion des mots de passe administrateur ... 1200
Autorisations requises pour AWS Secrets Manager intégration ... 1201
Rotation secrète des mots de passe administrateur ... 1202
Considérations concernant l'utilisation AWS Secrets Manager avec Amazon Redshift ... 1202
Récupération de l'ARN du secret ... 1203
Création d'un secret pour les informations d'identification de connexion à une base de données ... 1204
Journalisation et surveillance ... 1207
Journalisation des audits de base de données ... 1208
Se connecter avec CloudTrail ... 1226
Intégration des tables système avec les tables S3 ... 1238
Validation de conformité ... 1253
Résilience ... 1254
Sécurité de l'infrastructure ... 1255
Isolement de réseau ... 977
Groupes de sécurité ... 1257
Points de terminaison de VPC d'Interface ... 1257
Analyse de la configuration et des vulnérabilités ... 1265
Utilisation de l'authentification Identity Center ... 1266

Conditions préalables 1266
Comment fonctionne l'authentification Identity Center 1267
GetIdentityCenterAuthToken Opérations d'API 1268
GetIdentityCenterAuthToken pour les clusters provisionnés 1268
GetIdentityCenterAuthToken pour les groupes de travail sans serveur 1269
Syntaxe de réponse 1270
Intégration des pilotes 1271
Utilisation directe des jetons 1271
Exemple de code Java 1271
Exigences de la politique IAM 1272
Autorisations d'API 1272
Exemple de politiques IAM 1272
Disponibilité par région 1274
Résolution des problèmes 1274
erreurs d’API 1274
Erreurs de connexion 1275
Tâches de mise en réseau 1277
Noms de domaine personnalisé pour les connexions client 1277
Enregistrement d’un nom de domaine 1278
Demande de certificat pour un nom de domaine 1280
Configuration d’un domaine personnalisé 1281
Connexion à votre cluster alloué ou groupe de travail 1282
Changement de nom d’un cluster auquel un domaine personnalisé a été attribué 1283
Description des associations de domaines personnalisées 1284
Association d’un domaine personnalisé à un autre certificat 1285
Suppression du domaine personnalisé 1286
Redshift-managed Points de terminaison VPC 1287
Considérations 1288
Accès accordé à un VPC 1289
Création d'un point de Redshift-managed terminaison VPC 1290
Ressources Redshift dans un VPC 1291
Création d’un cluster ou d’un groupe de travail dans un VPC 1294
Groupes de sécurité VPC 1295
Configuration des paramètres de sécurité pour un cluster ou un groupe de travail 1297
Sous-réseaux pour les ressources Redshift 1300
Blocage de l’accès public aux VPC et aux sous-réseaux 1303

Contrôle du trafic réseau avec le routage VPC amélioré 1305
Contrôle du trafic de base de données avec les points de terminaison d'un VPC 1307
Activation du routage VPC amélioré 1308
Interrogation de tables de lacs de données avec un routage VPC amélioré 1310
Événements 1317
Abonnements aux notifications d'événements de cluster 1317
Création d'un abonnement aux notifications d'événement 1320
Notifications d'événement d'un cluster alloué 1321
Notifications d'événements Amazon Redshift sans serveur 1347
Zero-ETL notifications d'événements d'intégration 1365
Quotas et limites 1377
Quotas pour les objets Amazon Redshift 1377
Quotas pour les objets Amazon Redshift sans serveur 1389
Quotas pour l'API de données Amazon Redshift 1393
Quotas pour les objets de l'éditeur de requêtes v2 1395
Quotas et limites pour les objets Amazon Redshift Spectrum 1397
Contraintes d'affectation de noms 1398
Balisage des ressources 1402
Balisage des exigences 1403
Gestion des balises de ressources 1403
AWS Backup intégration 1405
Considérations 1406
Limitations 1407
Utilisation AWS Backup avec Amazon Redshift 1407
Versions de cluster 1409
Patch 205 1410
Nouvelles fonctionnalités 1411
Patch 204 1413
Nouvelles fonctionnalités 1413
Patch 203 1417
Nouvelles fonctionnalités 1418
Patch 202 1421
Nouvelles fonctionnalités 1421
Patch 201 1424
Nouvelles fonctionnalités 1424
Patch 200 1426

Nouvelles fonctionnalités 1427
Patch 199 1430
Nouvelles fonctionnalités 1430
Patch 198 1432
Nouvelles fonctionnalités 1433
Patch 197 1434
Nouvelles fonctionnalités 1435
Patch 196 1437
Nouvelles fonctionnalités 1438
Patch 195 1438
Nouvelles fonctionnalités 1438
Patch 194 1439
Nouvelles fonctionnalités 1439
Patch 193 1440
Nouvelles fonctionnalités 1440
Patch 192 1441
Nouvelles fonctionnalités 1441
Patch 191 1441
Nouvelles fonctionnalités 1442
Patch 190 1442
Nouvelles fonctionnalités 1443
Patch 189 1443
Nouvelles fonctionnalités 1444
Patch 188 1444
Nouvelles fonctionnalités 1445
Patch 187 1445
Nouvelles fonctionnalités 1446
Patch 186 1447
Nouvelles fonctionnalités 1448
Patch 185 1449
Nouvelles fonctionnalités 1450
Patch 184 1451
Nouvelles fonctionnalités 1451
Patch 183 1453
Nouvelles fonctionnalités 1453
Patch 182 1454

Nouvelles fonctionnalités 1455
Patch 181 1457
Nouvelles fonctionnalités 1457
Correctif 180 1458
Nouvelles fonctionnalités 1459
Correctif 179 1460
Nouvelles fonctionnalités 1461
Correctif 178 1462
Nouvelles fonctionnalités 1463
Correctif 177 1465
Nouvelles fonctionnalités 1466
Correctif 176 1467
Nouvelles fonctionnalités 1468
Correctif 175 1470
Nouvelles fonctionnalités 1470
Correctif 174 1470
Nouvelles fonctions pour cette version 1470
Nouvelles fonctions pour cette version 1470
Nouvelles fonctions pour cette version 1470
Nouvelles fonctions pour cette version 1470
Nouvelles fonctions pour cette version 1470
Nouvelles fonctions pour cette version 1470
Nouvelles fonctions pour cette version 1470
Correctif 173 1472
Nouvelles fonctions pour cette version 1472
Nouvelles fonctions pour cette version 1472
Nouvelles fonctions pour cette version 1472
Nouvelles fonctions pour cette version 1472
Nouvelles fonctions pour cette version 1472
Nouvelles fonctions pour cette version 1472
Nouvelles fonctions pour cette version 1472
Nouvelles fonctions pour cette version 1472
Nouvelles fonctions pour cette version 1472
Nouvelles fonctions pour cette version 1472
Correctif 172 1473
Nouvelles fonctionnalités 1474

Correctif 171 1475
Nouvelles fonctionnalités 1475
Correctif 170 1475
Nouvelles fonctionnalités 1475
Correctif 169 1475
Nouvelles fonctionnalités 1476
Correctif 168 1476
Nouvelles fonctionnalités 1476
Changements de comportement 1478
Changements de comportement à venir 1478
Amazon Redshift prend des instantanés automatisés des clusters de producteurs de partage de données interrompus à compter du 30 septembre 2026 1479
Le type de données SUPER prend en charge les chaînes individuelles plus grandes à partir du patch 206 1479
AWS KMS application des autorisations clés pour les API Amazon Redshift sans serveur après le 17 août 2026 1481
Amazon Redshift impose le verrouillage des utilisateurs après plusieurs tentatives de connexion infructueuses, à commencer par le patch 208 1482
Modèle de facturation amélioré pour les instantanés manuels sur les instances Amazon Redshift Serverless et Amazon Redshift RG à compter du 8 juin 2026 1483
Les tables Iceberg DELETE on Lake Formation nécessitent l'autorisation DELETE à compter du patch 202 1483
Amazon Redshift Serverless préserve les intégrations d'événements sans ETL et S3 lors de la restauration de snapshots à partir du correctif 202 1484
Fin du support pour le pilote ODBC 1.x Amazon Redshift le 31 décembre 2026 1485
Les fonctions scalaires Python définies par l’utilisateur ne seront plus prises en charge après le 30 juin 2026 1486
Modification du Auto-REFRESH comportement de la vue matérialisée (MV) après le 27 février 2026 1486
Amazon Redshift ne prendra pas en charge les fonctions permettant d’accéder aux informations des consommateurs via l’unité de partage des données après le 16 février 2026 1487
Modifications apportées à la version du protocole TLS (Minimum Transport Layer Security) à compter du 31 octobre 2026 1487
Amazon Redshift ne prendra pas en charge la création de nouvelles fonctions scalaires Python définies par l’utilisateur après le 30 octobre 2025 1488

Changements de comportement récents 1489
Amazon Redshift utilise la base de données de fuseaux horaires IANA à jour après le 26 août 2025 1489
Les modifications apportées aux unités de traitement Redshift (RPU) Amazon Redshift sans serveur entreront en vigueur après le 15 août 2025 1490
Modifications apportées à la journalisation des audits de base de données en vigueur après le 10 août 2025 1490
Modifications apportées au point de terminaison du cloud privé virtuel pour les groupes de travail sans serveur à compter du 27 juin 2025 1491
Les modifications apportées à la surveillance des requêtes entreront en vigueur après le 2 mai 2025 1491
Changements de sécurité en vigueur après le 10 janvier 2025 1492
Exemples de code 1495
Principes de base 1496
Bonjour Amazon Redshift 1496
Principes de base 1502
Actions 1568
Scénarios 1628
Créer une application web pour suivre les données Amazon Redshift 1628
Premiers pas avec les entrepôts de données sans serveur 1629
Commencer à utiliser des clusters d'entrepôts de données provisionnés 1647
Historique du document 1658

Amazon Redshift ne prendra plus en charge l'utilisation des UDF Python après le 30 juin 2026. Nous allons commencer à l'appliquer par étapes. Pour plus d'informations sur les options de fin de vie et de migration de Python, consultez le billet de blog publié le 30 juin 2025.

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.

Qu’est-ce qu’Amazon Redshift ?

Bienvenue dans le Guide de la gestion du cluster Amazon Redshift. Amazon Redshift est un service d’entrepôt des données entièrement géré dans le cloud. Amazon Redshift sans serveur vous permet d’accéder aux données et de les analyser sans toutes les configurations d’un entrepôt des données provisionné. Les ressources sont automatiquement provisionnées et la capacité de l’entrepôt des données est intelligemment mise à l’échelle afin d’offrir des performances rapides, même pour les charges de travail les plus exigeantes et les plus imprévisibles. Vous ne payez pas de frais lorsque l’entrepôt des données est inactif, vous ne payez donc que ce que vous utilisez. Vous pouvez charger des données et commencer à effectuer des requêtes immédiatement dans l’éditeur de requête Amazon Redshift v2 ou dans votre outil d’informatique décisionnelle (BI) préféré. Profitez des meilleures performances en termes de prix et des fonctionnalités SQL habituelles dans un environnement facile à utiliser et sans administration.

Quelle que soit la taille du jeu de données, Amazon Redshift offre des performances de requête rapides en utilisant les mêmes SQL-based outils et applications de business intelligence que ceux que vous utilisez aujourd'hui.

Utilisez-vous pour la première fois Amazon Redshift ?

Si vous utilisez Amazon Redshift pour la première fois, nous vous recommandons de commencer par lire les sections suivantes :

- Éléments principaux du service et tarifs – Fournit la proposition de valeur Amazon Redshift, les éléments principaux du service et la tarification.
- Premiers pas avec les entrepôts de données Amazon Redshift sans serveur : cette rubrique vous guide dans le processus de configuration d’un entrepôt de données sans serveur, de création de ressources et d’interrogation d’exemples de données.
- Manuel du développeur de base de données Amazon Redshift– Si vous êtes un développeur de base de données, ce guide explique comment concevoir, développer, interroger et gérer les bases de données qui constituent votre entrepôt des données.

Si vous préférez gérer manuellement vos ressources Amazon Redshift, vous pouvez créer des clusters provisionnés pour vos besoins en matière d’interrogation de données. Pour plus d’informations, consultez Clusters Amazon Redshift.

En tant que développeur d'applications, vous pouvez utiliser l'API Amazon Redshift ou les bibliothèques du kit de développement AWS logiciel (SDK) pour gérer les clusters par programmation. Si vous utilisez l'API Amazon Redshift, vous devez authentifier chaque requête HTTP ou HTTPS à l'API en vous y connectant. Pour plus d'informations sur la signature des demandes, consultez Signature d'une requête HTTP.

Pour plus d'informations sur l'API, l'interface CLI et les kits SDK, consultez les liens suivants :

- Référence de l'API Amazon Redshift sans serveur
- Référence de l'API Amazon Redshift
- Référence de l'API de données Amazon Redshift
- AWS CLI Référence de commande
- Références SDK dans Outils Amazon Web Services.

Présentation des fonctions d'Amazon Redshift sans serveur

La plupart des fonctionnalités prises en charge par un entrepôt des données mis en service par Amazon Redshift le sont également par Amazon Redshift sans serveur. Voici quelques-unes de ses principales capacités.

Fonctionnalité	Description
Instantanés	Vous pouvez restaurer un instantané d'Amazon Redshift sans serveur ou d'un entrepôt des données approvisionné dans Amazon Redshift sans serveur. Pour plus d'informations, consultez Instantanés et points de récupération.
Points de récupération	Amazon Redshift sans serveur crée automatiquement un point de récupération toutes les 30 minutes. Ces points de récupération sont conservés 24 heures. Vous pouvez les utiliser pour restaurer après des écritures ou des suppressions accidentelles. Lorsque vous restaurez à partir d'un point de récupération, toutes les données de votre base de données Amazon Redshift sans serveur sont restaurées à un point antérieur dans le temps. Vous pouvez également créer un instantané à partir d'un point de récupération si vous devez conserver un point de récupération plus longtemps. Pour plus d'informations, consultez Instantanés et points de récupération.

Fonctionnalité	Description
Capacité des RPU de base	Vous pouvez définir une capacité de base dans les unités de traitement Redshift (RPU). Une RPU fournit 16 Go de mémoire. Ce paramètre vous donne la possibilité de contrôler l'équilibre entre les ressources utilisées et les coûts pour votre charge de travail. Vous pouvez augmenter cette valeur pour accroître les ressources disponibles et améliorer les performances des requêtes, ou la diminuer pour limiter vos dépenses. La valeur par défaut est 128 RPU. Vous pouvez également définir des limites d'utilisation, telles que les RPU utilisés quotidiennement, pour contrôler les coûts. Pour plus d'informations, consultez Facturation pour Amazon Redshift sans serveur.
Limites d'utilisation du partage de données	Vous pouvez limiter la quantité de données transférées d'une région productrice à une région consommatrice en utilisant la console ou l'API. Ces coûts de transfert de données diffèrent et sont mesurés en téraoctets. Région AWS Pour plus d'informations sur le partage de données, consultez Mise en route du partage de données dans le Manuel du développeur de bases de données Amazon Redshift.
User-defined fonctions (UDF)	Vous pouvez exécuter des fonctions définies par l'utilisateur (UDF) dans Amazon Redshift sans serveur. Pour plus d'informations, consultez Création de fonctions définies par l'utilisateur dans le Guide du développeur de bases de données Amazon Redshift.
Procédures stockées	Vous pouvez exécuter des procédures stockées dans Amazon Redshift sans serveur. Pour plus d'informations, consultez Création de procédures stockées dans le Guide du développeur de base de données Amazon Redshift.
Vues matérialisées	Vous pouvez créer des vues matérialisées dans Amazon Redshift sans serveur. Pour plus d'information, consultez Création de vues matérialisées dans le Guide du développeur de base de données Amazon Redshift.
Fonctions spatiales	Vous pouvez exécuter des fonctions spatiales dans Amazon Redshift sans serveur. Pour plus d'informations, consultez Interrogation des données spatiales dans le Guide du développeur de base de données Amazon Redshift.

Fonctionnalité	Description
Requêtes fédérées	Vous pouvez exécuter des requêtes pour joindre des données avec un cluster Aurora DB et Amazon RDS à partir d'Amazon Redshift sans serveur. Pour plus d'informations, consultez Interrogation de données avec requête fédérée dans le Guide du développeur de base de données Amazon Redshift.
Requêtes de lac de données	Vous pouvez exécuter des requêtes pour joindre les données de votre lac de données Amazon S3 avec Amazon Redshift sans serveur. Pour en savoir plus, consultez Interroger un lac de données dans le Guide de gestion des clusters Amazon Redshift.
HyperLogLog	Vous pouvez exécuter des HyperLogLog fonctions dans Amazon Redshift Serverless. Pour plus d'informations, consultez la section Utilisation de HyperLogLog croquis dans le manuel Amazon Redshift Database Developer Guide.
Interrogation des données de plusieurs bases de données	Vous pouvez interroger des données entre bases de données avec Amazon Redshift sans serveur. Pour plus d'informations, consultez Interrogation des données de plusieurs bases de données dans le Guide du développeur de base de données Amazon Redshift.
Partage des données	Vous pouvez accéder aux données sur les clusters mis en service avec Amazon Redshift sans serveur. Pour plus d'informations, consultez Partager des données entre plusieurs clusters dans le Guide du développeur de bases de données Amazon Redshift.
Semi-structured interrogation de données	Vous pouvez intégrer et stocker des données semi-structurées avec le type de données SUPER, à l'aide de Amazon Redshift sans serveur. Pour plus d'informations, consultez Ingestion et interrogation de données semi-structurées dans le Guide du développeur de base de données Amazon Redshift.
Balisage des ressources	Vous pouvez utiliser l'API Amazon Redshift Serverless AWS CLI ou l'API Amazon Redshift pour baliser les ressources avec des métadonnées associées à la ressource. Pour plus d'informations, consultez Balisage de vos ressources.

Fonctionnalité	Description
Machine learning	Vous pouvez utiliser le machine learning d'Amazon Redshift avec Amazon Redshift sans serveur. Pour plus d'informations, consultez Utilisation du machine learning dans le Guide du développeur de base de données Amazon Redshift.
Commandes et fonctions SQL	À quelques exceptions près (comme pour `REBOOT_CLUSTER`), vous pouvez utiliser les commandes et fonctions SQL d'Amazon Redshift avec Amazon Redshift sans serveur. Pour plus d'informations, consultez Référence SQL du Guide du développeur de bases de données Amazon Redshift.
CloudFormationressources	À l'aide CloudFormation de modèles, vous pouvez déployer et mettre à jour les ressources Amazon Redshift Serverless. Grâce à cette intégration, vous pouvez consacrer moins de temps à la gestion des ressources et vous concentrer sur vos applications. Pour plus d'informations sur les CloudFormation ressources d'Amazon Redshift Serverless, consultez la référence des types de ressources Amazon Redshift Serverless.
CloudTrail resources	Amazon Redshift Serverless est intégré à Amazon Redshift Serverless AWS CloudTrail pour fournir un enregistrement des actions effectuées dans Amazon Redshift Serverless. CloudTrail capture tous les appels d'API pour Amazon Redshift Serverless sous forme d'événements. Pour plus d'informations, consultez CloudTrail Amazon Redshift Serverless.

Vue d'ensemble des clusters provisionnés Amazon Redshift

Le service Amazon Redshift gère toutes les tâches de configuration, d'exploitation et de mise à l'échelle d'un entrepôt des données. Ces tâches incluent la capacité d'allocation, de surveillance et de sauvegarde du cluster, ainsi que l'application de correctifs et de mises à niveau au moteur Amazon Redshift.

La vidéo suivante explique comment créer un cluster et interroger des données à l'aide de l'éditeur de requêtes Amazon Redshift v2.

Gestion du cluster

Un cluster Amazon Redshift est un ensemble de nœuds qui se compose d'un nœud principal et d'un ou de plusieurs nœuds de calcul. Le type et le nombre de nœuds de calcul dont vous avez besoin dépend de la taille de vos données, du nombre de requêtes que vous exécutez et des performances d'exécution des requêtes dont vous avez besoin.

Création et gestion de clusters

En fonction de vos besoins en entrepôt des données, vous pouvez commencer par un petit cluster à un seul nœud et facile à agrandir en un cluster plus grand et à plusieurs nœuds, au fur et à mesure que vos besoins évoluent. Vous pouvez ajouter des nœuds de calcul au cluster ou en supprimer sans interrompre le service. Pour plus d'informations, consultez Clusters Amazon Redshift provisionnés.

Réservation de nœuds de calcul

Si vous souhaitez que votre cluster s'exécute pendant un an ou plus, vous pouvez économiser de l'argent en réservant des nœuds de calcul pour une période d'un an ou de trois ans. La réservation de nœuds de calcul offre des économies importantes par rapport aux taux horaires que vous payez lorsque vous mettez en service des nœuds de calcul à la demande. Pour plus d'informations, consultez Nœuds réservés.

Création d'instantanés de cluster

Les instantanés sont des sauvegardes du cluster à un instant donné. Il existe deux types d'instantanés : automatiques et manuels. Amazon Redshift stocke ces instantanés en interne dans Amazon Simple Storage Service (Amazon S3) à l'aide d'une connexion chiffrée Secure Sockets Layer (SSL). Si vous devez restaurer à partir d'un instantané, Amazon Redshift crée un nouveau cluster et importe les données à partir de l'instantané que vous spécifiez. Pour plus d'informations sur les instantanés, consultez Instantanés et sauvegardes Amazon Redshift.

Accès et sécurité des clusters

Il existe plusieurs fonctions liées à l'accès au cluster et à la sécurité dans Amazon Redshift. Ces fonctionnalités vous permettent de contrôler l'accès à votre cluster, de définir des règles de connectivité et de chiffrer les données et les connexions. Ces fonctions viennent en complément des fonctions liées à l'accès aux bases de données et à leur sécurité dans Amazon Redshift. Pour plus d'informations sur la sécurité de la base de données, consultez Gestion de la sécurité de la base de données du Manuel du développeur de base de données Amazon Redshift.

AWS comptes et informations d'identification IAM

Par défaut, un cluster Amazon Redshift n'est accessible que par le AWS compte qui le crée. Le cluster est verrouillé afin que personne d'autre n'y ait accès. Dans votre AWS compte, vous utilisez le service Gestion des identités et des accès AWS (IAM) pour créer des comptes utilisateurs et gérer les autorisations pour ces comptes afin de contrôler les opérations du cluster. Pour de plus amples informations, veuillez consulter Sécurité dans Amazon Redshift. Pour plus d'informations sur la gestion des identités IAM, y compris les conseils et les bonnes pratiques pour les rôles IAM, consultez Identity and Access Management dans Amazon Redshift.

Groupes de sécurité

Par défaut, les clusters que vous créez sont privés. Les informations d'identification IAM contrôlent uniquement l'accès aux API-related ressources Amazon Redshift : la console Amazon Redshift, l'interface de ligne de commande (CLI), l'API et le SDK. Pour autoriser l'accès au cluster à partir d'outils clients SQL via ODBC ou JDBC, vous utilisez des groupes de sécurité :

- Si vous utilisez la EC2-VPC plate-forme pour votre cluster Amazon Redshift, vous devez utiliser des groupes de sécurité VPC. Nous vous recommandons de lancer votre cluster sur une EC2-VPC plateforme.

  Vous ne pouvez pas déplacer un cluster vers un VPC après son lancement avec EC2-Classic. Vous pouvez toutefois restaurer un EC2-Classic instantané d'un EC2-VPC cluster à l'aide de la console Amazon Redshift. Pour de plus amples informations, veuillez consulter Restauration d'un cluster à partir d'un instantané.
- Si vous utilisez la EC2-Classic plateforme pour votre cluster Amazon Redshift, vous devez utiliser les groupes de sécurité Amazon Redshift.

Dans les deux cas, vous ajoutez des règles au groupe de sécurité pour accorder un accès entrant explicite à une plage d' CIDR/IP adresses spécifique ou à un groupe de sécurité Amazon Elastic Compute Cloud (Amazon EC2) si votre client SQL s'exécute sur une instance Amazon EC2. Pour de plus amples informations, veuillez consulter Groupes de sécurité Amazon Redshift.

Outre les règles de l'accès entrant, vous créez des utilisateurs de base de données pour fournir les informations d'identification afin de s'authentifier auprès de la base de données au sein du cluster lui-même. Pour plus d'informations, consultez Bases de données dans cette rubrique.

Chiffrement

Lorsque vous mettez en service le cluster, vous pouvez choisir, le cas échéant, de chiffrer le cluster pour plus de sécurité. Lorsque vous activez le chiffrement, Amazon Redshift stocke toutes les données des tables créées par l'utilisateur en un format chiffré. Vous pouvez utiliser AWS Key Management Service (AWS KMS) pour gérer vos clés de chiffrement Amazon Redshift.

Le chiffrement est une propriété immuable du cluster. Le seul moyen de passer d'un cluster chiffré à un cluster non chiffré consiste à décharger les données et à les recharger dans un nouveau cluster. Le chiffrement s'applique au cluster et à toutes les sauvegardes. Lors de la restauration d'un cluster à partir d'un instantané chiffré, le nouveau cluster est également chiffré.

Pour plus d'informations sur le chiffrement, les clés et les modules de sécurité matérielle, consultez Chiffrement de base de données Amazon Redshift.

Connexions SSL

Vous pouvez utiliser le chiffrement SSL (Secure Sockets Layer) pour chiffrer la connexion entre votre client SQL et votre cluster. Pour plus d'informations, consultez Configuration des options de sécurité des connexions.

Surveillance des clusters

Il existe plusieurs fonctions liées à la surveillance dans Amazon Redshift. Vous pouvez utiliser la journalisation d'audit afin de générer des journaux d'activités, de configurer des événements et des abonnements aux notifications pour suivre les informations intéressantes. Utilisez les statistiques d'Amazon Redshift et d'Amazon CloudWatch pour en savoir plus sur l'état et les performances de vos clusters et bases de données.

Journalisation des audits de base de données

Vous pouvez utiliser la journalisation des audits de base de données pour suivre les informations sur les tentatives d'authentification, les connexions, les déconnexions, les modifications apportées aux définitions des utilisateurs de la base de données et les requêtes s'exécutant dans la base de données. Ces informations sont utiles pour la sécurité et le dépannage d'Amazon Redshift. Les journaux sont stockés dans des compartiments Amazon S3. Pour plus d'informations, consultez Journalisation des audits de base de données.

Événements et notifications

Amazon Redshift suit les événements et conserve les informations les concernant pendant plusieurs semaines sur votre AWS compte. Pour chaque événement, Amazon Redshift prend en charge les informations telles que la date à laquelle l'événement s'est produit, une description, la source de l'événement (un cluster, un groupe de paramètres ou un instantané, par exemple) et l'ID source. Vous pouvez créer des abonnements aux notifications d'événements Amazon Redshift qui spécifient un ensemble de filtres d'événement. Quand se produit un événement qui correspond aux critères de filtre, Amazon Redshift utilise Amazon Simple Notification Service pour vous informer que l'événement a eu lieu. Pour plus d'informations sur les événements et les notifications, consultez Événements Amazon Redshift.

Performance

Amazon Redshift fournit les métriques de performance et les données de telle sorte que vous puissiez suivre l'état et les performances de vos clusters et bases de données. Amazon Redshift utilise CloudWatch les métriques Amazon pour surveiller les aspects physiques du cluster, tels que l'utilisation du processeur, la latence et le débit. Amazon Redshift fournit également des données de performances de requête et de chargement pour vous aider à surveiller l'activité de la base de données dans votre cluster. Pour plus d'informations sur les métriques de performance et leur surveillance, consultez Surveiller les performances de cluster Amazon Redshift.

Bases de données

Amazon Redshift crée une base de données lorsque vous allouez un cluster. Il s'agit de la base de données que vous utilisez pour charger les données et exécuter des requêtes sur vos données. Vous pouvez créer des bases de données supplémentaires en fonction des besoins en exécutant une commande SQL. Pour plus d'informations, consultez Étape 1 : Création d'une base de données dans le Manuel du développeur de base de données Amazon Redshift.

Lorsque vous allouez un cluster, vous spécifiez un utilisateur administrateur qui a accès à toutes les bases de données créées au sein du cluster. Cet utilisateur administrateur est un super-utilisateur, qui est le seul utilisateur ayant accès initialement à la base de données, même si cet utilisateur peut créer des utilisateurs et des super-utilisateurs supplémentaires. Pour plus d'informations, consultez Super-utilisateurs et Utilisateurs dans le Manuel du développeur de base de données Amazon Redshift.

Amazon Redshift utilise les groupes de paramètres pour définir le comportement de toutes les bases de données d'un cluster, comme le style de présentation des dates et la précision en virgule flottante.

Si vous ne spécifiez pas un groupe de paramètres lorsque vous allouez votre cluster, Amazon Redshift associe un groupe de paramètres par défaut au cluster. Pour plus d'informations, consultez Groupes de paramètres Amazon Redshift.

Pour plus d'informations sur les bases de données dans Amazon Redshift, consultez le Manuel du développeur de base de données Amazon Redshift.

Comparaison entre Amazon Redshift sans serveur et un entrepôt des données mis en service par Amazon Redshift sans serveur

Pour Amazon Redshift sans serveur, certains concepts et fonctionnalités sont différents de la fonctionnalité correspondante pour un entrepôt des données mis en service par Amazon Redshift. Par exemple, une comparaison contrastée est qu'Amazon Redshift sans serveur ne comprend pas le concept de cluster ou de nœud. La table suivante décrit les fonctions et le comportement d'Amazon Redshift sans serveur et explique en quoi ils diffèrent d'une fonction équivalente dans un entrepôt des données mis en service.

Fonctionnalité	Description	sans serveur	Alloué
Groupe de travail et espace de noms	Pour isoler les charges de travail et gérer différentes ressources dans Amazon Redshift sans serveur, vous pouvez créer des espaces de noms et des	Un espace de noms est une collection d'objets de base de données et d'utilisateurs. Un groupe de travail est une collection de ressources informatiques.	Un cluster provisionné est un ensemble de nœuds de calcul et un nœud principal, que vous gérez directement. Pour plus d'informations, consultez Clusters Amazon Redshift provisionnés.

Fonctionnalité	Description	sans serveur	Alloué
	groupes de travail afin de gérer séparément les ressources de stockage et de calcul.	Pour plus d'informations, consultez Amazon Redshift sans serveur pour comprendre la conception d'Amazon Redshift sans serveur.	

Fonctionnalité	Description	sans serveur	Alloué
Types de nœud	Lorsque vous utilisez Amazon Redshift sans serveur, vous ne choisissez pas les types de nœuds ou ne spécifiez pas le nombre de nœuds comme vous le faites avec un cluster Amazon Redshift mis en service.	Amazon Redshift sans serveur met en service et gère automatiquement les capacités pour vous. Vous pouvez éventuellement spécifier la capacité de l'entrepôt de données de base afin de sélectionner le bon price/performance équilibre pour vos charges de travail. Vous pouvez également	Vous créez un cluster avec des types de nœuds qui répondent à vos spécifications en matière de coûts et de performances. Pour plus d'informations, consultez Clusters Amazon Redshift provisionnés.

Fonctionnalité	Description	sans serveur	Alloué
		spécifier un nombre maximum d'heures de RPU pour définir des contrôles de coûts afin de garantir la prévisibilité des coûts. Pour plus d'informations, consultez Capacité de calcul pour Amazon Redshift sans serveur.	

Fonctionnalité	Description	sans serveur	Alloué
Gestion de la charge de travail et évolutivité de la simultanéité	Amazon Redshift peut s'adapter aux périodes de forte charge. Amazon Redshift sans serveur peut également évoluer pour répondre aux périodes intermittentes de forte charge.	Amazon Redshift sans serveur gère automatiquement les ressources de manière efficace et évolue, en fonction des charges de travail, dans le respect des seuils de contrôle des coûts. Pour plus d'informations, consultez Facturation de la capacité de calcul.	Avec un entrepôt des données provisionné, vous activez la mise à l'échelle de la simultanéité sur votre cluster pour gérer les périodes de lourdes charges. Pour plus d'informations, consultez Évolutivité de la simulanéité.

Fonctionnalité	Description	sans serveur	Alloué
Port	Le numéro de port que vous utilisez pour vous connecter.	Avec Amazon Redshift sans serveur, vous pouvez passer à un autre port dans la plage de ports 5431–5455 ou 8191–8215. Pour plus d'informations, consultez Connexion à Amazon Redshift sans serveur.	Avec un cluster provisionné, vous pouvez choisir n'importe quel port pour la conenxion.

Fonctionnalité	Description	sans serveur	Alloué
Redimensionnement	Ajoutez ou supprimez des ressources de calcul pour optimiser les performances de la charge de travail.	Le redimensionnement n'est pas applicable dans Amazon Redshift sans serveur. Vous pouvez toutefois modifier la capacité RPU de l'entrepôt des données de base, en fonction de vos exigences en matière de prix et de performances. Pour plus d'informations, consultez Capacité	Avec un cluster mis en service, vous effectuez un redimensionnement du cluster pour ajouter ou supprimer des nœuds. Pour plus d'informations, consultez Présentation de la gestion des clusters dans Amazon Redshift.

Fonctionnalité	Description	sans serveur	Alloué
		de calcul pour Amazon Redshift sans serveur.	
Suspension et reprise	Vous pouvez suspendre un cluster provisionné lorsque vous n'avez pas de charges de travail à exécuter, afin de réduire les coûts.	Avec Amazon Redshift sans serveur, vous ne payez que lors de l'exécution des requêtes, il n'est donc pas nécessaire de faire une pause ou de reprendre. Pour plus d'informations, consultez Facturation de la capacité de calcul.	Vous mettez en pause et reprenez votre cluster manuellement, en fonction d'une évaluation de votre charge de travail à différents moments. Pour plus d'informations, consultez Présentation de la gestion des clusters dans Amazon Redshift.

Fonctionnalité	Description	sans serveur	Alloué
Interrogation de données externes	Vous pouvez interroger des données dans des compartiments Amazon S3, dans différents formats, tels que JSON, Parquet ou Iceberg.	Amazon Redshift Serverless inclut un moteur de requête de lac de données intégré qui s'exécute sur les ressources de calcul du groupe de travail et permet d'interroger les données Amazon S3 au sein d'une AWS région ou entre différentes régions. AWS Pour optimiser les performances des requêtes du lac de	Avec les clusters provisionnés RA3 et DC2, les requêtes des lacs de données s'exécutent sur Redshift Spectrum à l'aide de serveurs dédiés indépendants de votre cluster. Redshift Spectrum nécessite que le compartiment Amazon S3 se trouve dans la même AWS région que le cluster. Pour plus d'informations, consultez Interroger les données externes à l'aide d'Amazon Redshift Spectrum. Les clusters provisionnés par RG incluent un moteur de requêtes de lac de données intégré. Les requêtes de lac de données s'exécutent directement sur les ressources de calcul du cluster, de la même manière que Redshift Serverless, et permettent d'interroger des données Amazon S3 dans la même AWS région ou dans une région différente. AWS Pour plus d'informations, voir Interroger votre lac de données.

Fonctionnalité	Description	sans serveur	Alloué
		données, ajustez la capacité RPU de base de votre groupe de travail.	

Fonctionnalité	Description	sans serveur	Alloué
Compute-resourcefacturation	Comment s’accumule la facturation entre Amazon Redshift et Amazon Redshift sans serveur.	Avec Amazon Redshift Serverless, vous payez les charges de travail que vous exécutez, à RPU-hours la seconde, avec un minimum de 60 secondes. Cela inclut les requêtes qui accèdent aux données dans des formats de fichiers ouverts dans Amazon S3. Pour plus d’informations, consultez	Avec un cluster provisionné, la facturation s’effectue à la seconde lorsque le cluster n’est pas suspendu. Pour les clusters RG, les requêtes sur les lacs de données sont incluses dans la tarification du calcul par heure de nœud, sans frais Spectrum distincts. Pour les clusters RA3 et DC2, les requêtes de lac de données entraînent des frais de spectre Redshift supplémentaires.

Fonctionnalité	Description	sans serveur	Alloué
		Facturation de la capacité de calcul.	
Fenêtre de maintenance	Comment fonctionne la maintenance des serveurs.	Avec Amazon Redshift sans serveur, il n'y a pas de fenêtre de maintenance. Les mises à jour sont gérées sans problème Pour plus d'informations, consultez Qu'est-ce qu'Amazon Redshift sans serveur ?	Avec un cluster provisionné, vous spécifiez une fenêtre de maintenance lorsque le correctif est appliqué sur votre cluster. (En règle générale, vous choisissez une période récurrente de faible utilisation.)

Fonctionnalité	Description	sans serveur	Alloué
Chiffrement	Vous pouvez activer le chiffrement des bases de données.	Amazon Redshift Serverless est toujours chiffré avec AWS KMS, avec des clés AWS gérées ou gérées par le client.	Les données d'un entrepôt de données provisionné peuvent être chiffrées AWS KMS (avec des clés AWS gérées ou gérées par le client) ou non chiffrées. Consultez Chiffrement de base de données Amazon Redshift.
Facturation du stockage	Comment fonctionne la facturation du stockage	Pour Amazon Redshift sans serveur. Le tarif est calculé en fonction du nombre de Go par mois. Consultez Facturation de la capacité de calcul.	Le stockage est facturé séparément des ressources de calcul pour un cluster provisionné avec des nœuds RG ou RA3.

Fonctionnalité	Description	sans serveur	Alloué
Gestion des utilisateurs	La façon dont les utilisateurs sont gérés.	Pour Amazon Redshift sans serveur, les utilisateurs sont des utilisateurs IAM ou Redshift. Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift Serverless. Pour plus d'informations sur la gestion des identités IAM, y compris les bonnes pratiques pour les	Pour un entrepôt de données alloué, les utilisateurs sont des utilisateurs IAM ou Redshift. Pour plus d'informations, consultez Gestion de la sécurité de la base de données dans le Guide du développeur de base de données Amazon Redshift. Pour plus d'informations sur la gestion des identités IAM, y compris les bonnes pratiques pour les rôles IAM, consultez Identity and Access Management dans Amazon Redshift.

Fonctionnalité	Description	sans serveur	Alloué
		rôles IAM, consultez Identity and Access Management dans Amazon Redshift.	

Fonctionnalité	Description	sans serveur	Alloué
Outils JDBC et ODBC et compatibilité	Comment fonctionnent les connexions client.	Amazon Redshift sans serveur est compatible avec n'importe quel outil ou application cliente compatible JDBC ou ODBC. Pour plus d'informations sur les pilotes, consultez Configuration des connexions dans le Guide de la gestion du cluster Amazon Redshift. Pour plus d'informations sur la connexion à Amazon Redshift	Un cluster alloué Amazon Redshift est compatible avec n'importe quel outil ou application cliente compatible JDBC ou ODBC. Pour plus d'informations sur les pilotes, consultez Configuration des connexions dans le Guide de la gestion du cluster Amazon Redshift. Pour plus d'informations sur la connexion aux clusters, consultez Connexion à un entrepôt de données Amazon Redshift à l'aide des outils client SQL.

Fonctionnalité	Description	sans serveur	Alloué
		sans serveur, consultez Connexion à Redshift sans serveur.	
Exigences relatives aux informations d'identification lors de la connexion	Comment les informations d'identification sont gérées.	Pour Amazon Redshift sans serveur, vous n'avez pas besoin de saisir les informations d'identification dans chaque instance. Pour plus d'informations, consultez Connexion à Amazon Redshift sans serveur.	L'accès à Amazon Redshift nécessite les informations de connexion d'un utilisateur associé à un rôle IAM. Le rôle IAM est associé à des autorisations spécifiques pour un entrepôt des données provisionné. Une fois authentifié, l'utilisateur peut directement se connecter à la base de données, à la console Redshift et à l'éditeur de requête v2.

Fonctionnalité	Description	sans serveur	Alloué
API de données	Vous pouvez accéder aux données des services Web et d'autres applications.	Amazon Redshift sans serveur prend en charge l'API de données Amazon Redshift. Avec Amazon Redshift sans serveur, vous utilisez le paramètre `workgroup-name` à la place du paramètre `cluster-identity` lorsque vous exécutez une commande. Pour plus d'informations sur	Un cluster alloué Amazon Redshift prend en charge l'API de données Amazon Redshift. Avec les clusters Amazon Redshift, vous utilisez le paramètre `cluster-identity` à la place du paramètre `workgroup-name` lorsque vous exécutez une commande. Pour plus d'informations sur l'appel de l'API Data, consultez Utilisation de l'API de données Amazon Redshift.

Fonctionnalité	Description	sans serveur	Alloué
		l'appel de l'API Data, consultez Utilisation de l'API de données Amazon Redshift.	

Fonctionnalité	Description	sans serveur	Alloué
Instantanés	Assure une restauration à un instant dans le passé.	Amazon Redshift sans serveur prend en charge les instantanés et les points de récupération. Pour plus d'informations sur les instantanés et les points de récupération pour un espace de noms, consultez Instantanés et points de récupération.	Les clusters provisionnés prennent en charge les instantanés. Pour plus d'informations, consultez Gestion des instantanés à l'aide de la console.

Fonctionnalité	Description	sans serveur	Alloué
Partage des données	Permet de partager des données entre des bases de données d'un même compte ou de comptes différents.	Amazon Redshift sans serveur prend en charge toutes les fonctionnalités de partage de données d'un entrepôt des données provisionné. Il prend également en charge le partage de données entre Amazon Redshift sans serveur et un entrepôt des données provisionné, un outil ou une	Les clusters provisionnés prennent en charge plusieurs bases de données, plusieurs comptes, plusieurs régions et le partage de AWS Data Exchange données. Pour plus d'informations, consultez Partager des données entre plusieurs clusters dans Amazon Redshift.

Fonctionnalité	Description	sans serveur	Alloué
		application client.	
Suivis	Fournit un calendrier pour les mises à jour logicielles.	Amazon Redshift sans serveur n'utilise pas le concept de piste. Les versions et les mises à jour sont gérées par le service. Pour plus d'informations sur la facturation sans serveur, consultez Instantanés et points de récupération.	Les clusters provisionnés prennent en charge le basculement entre les pistes courantes et les pistes de fin.

Fonctionnalité	Description	sans serveur	Alloué
Tables et vues système	Permet de surveiller vos ressources et les métadonnées de votre système.	Amazon Redshift sans serveur prend en charge les nouvelles tables et vues système. Pour plus d'informations sur les tables système, consultez Surveillance des requêtes et des charges de travail avec Amazon Redshift sans serveur. Pour plus d'informations sur la façon de migrer vos requêtes depuis les	Un entrepôt des données provisionné prend en charge l'ensemble existant de tables et de vues système pour la surveillance des clusters et d'autres tâches nécessitant des métadonnées système.

Fonctionnalité	Description	sans serveur	Alloué
		anciennes tables et vues système provisionnées vers les nouvelles vues, consultez Migration vers les vues de surveillance SYS.	

Fonctionnalité	Description	sans serveur	Alloué
Groupes de paramètres	Groupe de paramètres qui s'appliquent à toutes les bases de données que vous créez dans un cluster. Ces paramètres configurent les paramètres de base de données tels que le délai de requête et le style de date.	Amazon Redshift sans serveur n'utilise pas le concept de groupe de paramètres.	Les entrepôts des données provisionnés supportent les groupes de paramètres. Pour plus d'informations sur les groupes de paramètres pour un cluster provisionné, consultez Groupes de paramètres Amazon Redshift.

Fonctionnalité	Description	sans serveur	Alloué
Surveillance des requêtes	Fournit une vue temporelle des requêtes exécutées.	Le suivi des requêtes dans Amazon Redshift sans serveur nécessite que les utilisateurs se connectent à la base de données pour utiliser les tables système. Ainsi, la surveillance des requêtes et des tables système sont synchronisées. Les requêtes des tables système dans	La surveillance des requêtes dans les clusters mis en service n’affiche pas toutes les données des tables du système.

Fonctionnalité	Description	sans serveur	Alloué
		Amazon Redshift sans serveur utilisent l'utilisateur de la base de données mappé à l'utilisateur IAM pour utiliser la surveillance des requêtes. Pour plus d'informations sur la surveillance des requêtes, consultez Surveillance des requêtes et des charges de travail avec Amazon Redshift sans serveur.	

Fonctionnalité	Description	sans serveur	Alloué
Journaux d’audit	Fournit des informations sur les connexions et les activités de l’utilisateur dans votre base de données.	Avec Amazon Redshift Serverless, CloudWatch c'est une destination pour les journaux d'audit. La fourniture des journaux d’audit basée sur Amazon S3 n’est pas prise en charge par Amazon Redshift sans serveur. Pour plus d’informations, consultez Journalisation de l’audit pour Amazon Redshift	Pour un cluster provisionné, la livraison du journal S3-based d'audit Amazon est devenue la norme. Désormais, la livraison des journaux d'audit à CloudWatch est étendue pour couvrir les entrepôts de données provisionnés.

Fonctionnalité	Description	sans serveur	Alloué
		sans serveur.	

Fonctionnalité	Description	sans serveur	Alloué
Notifications d’événements	Amazon EventBridge est un service de bus d'événements sans serveur que vous pouvez utiliser pour connecter vos applications à des données d'événements provenant de diverses sources.	Amazon Redshift Serverless utilise Amazon EventBridge pour gérer les notifications d'événements afin de vous tenir informé des modifications apportées à votre entrepôt de données. Pour de plus amples informations, veuillez consulter Notifications d'événements Amazon	Pour un cluster provisionné, vous gérez les notifications d’événements à l’aide de la console Amazon Redshift afin de créer des abonnements aux événements. Pour plus d’informations, consultez Création d'un abonnement aux notifications d'événement.

Fonctionnalité	Description	sans serveur	Alloué
		Redshift sans serveur avec Amazon EventBridge.	
Contraintes du curseur	Amazon Redshift applique les contraintes sur la taille de tous les ensembles de résultats du curseur.	Amazon Redshift sans serveur dispose d'un curseur d'une taille totale maximale de 150 000 Mo pour l'ensemble de résultats.	Pour un cluster alloué, la taille totale maximale de l'ensemble de résultats du curseur dépend du type de cluster. Pour plus d'informations, consultez Contraintes de curseur.

Utilisation des interfaces de gestion Amazon Redshift pour les clusters alloués

> **Note**
>
> Cette rubrique se concentre sur les interfaces de gestion Amazon Redshift pour les clusters alloués. Il existe des interfaces de gestion similaires pour Amazon Redshift sans serveur et l'API de données Amazon Redshift.

Amazon Redshift prend en charge plusieurs interfaces de gestion que vous pouvez utiliser pour créer, gérer et supprimer des clusters Amazon Redshift : les SDK, AWS le AWS CLI() et AWS Command Line Interface l'API de gestion Amazon Redshift.

L'API Amazon Redshift – Vous pouvez appeler cette API de gestion Amazon Redshift en soumettant une requête. Les requêtes sont des requêtes HTTP ou HTTPS qui utilisent les verbes HTTP `GET` ou `POST` avec un paramètre nommé `Action`. Appeler l'API Amazon Redshift est le moyen le plus direct d'accéder au service Amazon Redshift. Toutefois, cela exige que votre application traite des détails de bas niveau tels que le traitement des erreurs et la génération d'un hachage pour signer la demande.

- Pour plus d'informations sur la création et la signature d'une demande d'API Amazon Redshift, consultez Signature d'une requête HTTP.
- Pour plus d'informations sur les actions d'API Amazon Redshift et les types de données pour Amazon Redshift, consultez la référence d'API Amazon Redshift.

AWS SDK : vous pouvez utiliser les AWS SDK pour effectuer des opérations liées au cluster Amazon Redshift. Plusieurs bibliothèques de kits SDK regroupent l'API Amazon Redshift sous-jacente. Elles intègrent les fonctionnalités de l'API dans le langage de programmation spécifique et gèrent un grand nombre des détails de bas niveau, tels que le calcul des signatures, la gestion des nouvelles tentatives de demande et la gestion des erreurs. L'appel des fonctions du wrapper dans les bibliothèques de kits SDK peut simplifier considérablement le processus d'écriture d'une application pour gérer un cluster Amazon Redshift.

- Amazon Redshift est pris en charge par les AWS kits SDK pour Java, .NET, PHP, Python, Ruby et. Node.js Les fonctions du wrapper pour Amazon Redshift sont documentées dans le manuel

de référence pour chaque kit SDK. Pour obtenir la liste des AWS SDK et des liens vers leur documentation, consultez la section Outils pour Amazon Web Services.

- Ce manuel fournit des exemples d'utilisation d'Amazon Redshift à l'aide du kit SDK Java. Pour des exemples de code AWS SDK plus généraux, consultezExemples de code pour Amazon Redshift à l'aide de AWS Kits SDK.

AWS CLI— La CLI fournit un ensemble d'outils de ligne de commande que vous pouvez utiliser pour gérer les AWS services à partir d'ordinateurs Windows, Mac et Linux. L' AWS CLI inclut des commandes basées sur les actions d'API Amazon Redshift.

- Pour plus d'informations sur l'installation et la configuration de l'interface de ligne de commande Amazon Redshift, consultez Configuration de la CLI Amazon Redshift.
- Pour obtenir des documents de référence sur les commandes de la CLI Amazon Redshift, consultez la section Amazon Redshift de la référence AWS CLI .

L'utilisation de ce service avec un AWS Kit SDK

AWS des kits de développement logiciel (SDK) sont disponibles pour de nombreux langages de programmation populaires. Chaque kit SDK fournit une API, des exemples de code et de la documentation qui facilitent la création d'applications par les développeurs dans leur langage préféré.

Documentation SDK	Exemples de code
AWS SDK pour C++	AWS SDK pour C++ exemples de code
AWS CLI	AWS CLI exemples de code
AWS SDK pour Go	AWS SDK pour Go exemples de code
AWS SDK pour Java	AWS SDK pour Java exemples de code
AWS SDK pour JavaScript	AWS SDK pour JavaScript exemples de code
AWS SDK pour Kotlin	AWS SDK pour Kotlin exemples de code
AWS SDK pour .NET	AWS SDK pour .NET exemples de code
AWS SDK pour PHP	AWS SDK pour PHP exemples de code

Documentation SDK	Exemples de code
Outils AWS pour PowerShell	Outils AWS pour PowerShell exemples de code
AWS SDK pour Python v4	AWS Exemples de code SDK pour Python v4
AWS SDK pour Python (Boto3)	AWS SDK pour Python (Boto3) exemples de code
AWS SDK pour Ruby	AWS SDK pour Ruby exemples de code
AWS SDK pour Rust	AWS SDK pour Rust exemples de code
AWS SDK pour SAP ABAP	AWS SDK pour SAP ABAP exemples de code
AWS SDK pour Swift	AWS SDK pour Swift exemples de code

> **Exemple de disponibilité**
>
> Vous n’avez pas trouvé ce dont vous avez besoin ? Demandez un exemple de code en utilisant le lien Faire un commentaire en bas de cette page.

Signature d'une requête HTTP

Amazon Redshift exige que chaque demande que vous envoyez à l'API de gestion soit authentifiée avec une signature. Cette rubrique explique comment signer vos demandes.

Si vous utilisez l'un des kits de développement AWS logiciel (SDK) ou le AWS Command Line Interface, la signature des demandes est gérée automatiquement et vous pouvez ignorer cette section. Pour plus d'informations sur l'utilisation AWS des kits SDK, consultezUtilisation des interfaces de gestion Amazon Redshift pour les clusters alloués. Pour plus d'informations sur l'utilisation de l'interface de ligne de commande Amazon Redshift, consultez la référence des commandes en ligne Amazon Redshift.

Pour signer une demande, vous calculez une signature numérique à l'aide d'une fonction de hachage de chiffrement. Un hachage de chiffrement est une fonction qui renvoie une valeur de hachage unique basée sur l'entrée. L'entrée de la fonction de hachage contient le texte de la demande et votre clé d'accès secrète que vous pouvez obtenir dans les informations d'identification temporaires. La

fonction de hachage renvoie une valeur de hachage que vous incluez dans la demande comme votre signature. La signature fait partie de l'en-tête `Authorization` de votre demande.

> **Note**
>
> Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec des AWS personnes extérieures au Console de gestion AWS. La manière d'accorder l'accès par programmation dépend du type d'utilisateur qui accède AWS.
> Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Recommandé) Utilisez les informations d'identification de la console comme informations d'identification temporaires pour signer les AWS CLI demandes programmatiques adressées aux AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, consultez la section Connexion pour le développement AWS local dans le Guide de AWS Command Line Interface l'utilisateur. • Pour les AWS kits de développement, consultez la section Connexion pour le développement AWS local dans le Guide de référence AWS des kits de développement logiciel et des outils.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
Identité de la main-d'œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, reportez-vous AWS CLI à la section Configuration de l'utilisation AWS IAM Identity Center dans le Guide de AWS Command Line Interface l'utilisateur. • Pour les AWS kits de développement logiciel, les outils et les AWS API, consultez la section Authentification IAM Identity Center dans le Guide de référence AWS des kits de développement logiciel et des outils.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de la section Utilisation des informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer des demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, consultez la section Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS kits de développement logiciel et les outils, consultez la section Authentification à l'aide d'informations d'identification à long terme dans le Guide de référence AWS des kits de développement logiciel et des outils. • Pour les AWS API, consultez la section Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Après qu'Amazon Redshift a reçu votre demande, il recalcule la signature en utilisant la même fonction de hachage et la même entrée que celles que vous avez utilisées pour signer la demande. Si

la signature résultante correspond à la signature de la demande, Amazon Redshift traite la demande ; sinon, la demande est rejetée.

Amazon Redshift prend en charge l'authentification à l'aide d'AWS Signature Version 4. Le processus de calcul d'une signature se compose de trois tâches. Ces tâches sont illustrées dans l'exemple qui suit.

- Tâche 1 : créer une demande canonique

  Réorganisez votre demande HTTP sous forme canonique. L'utilisation d'une forme canonique est nécessaire, car Amazon Redshift utilise la même forme canonique pour calculer la signature qu'il compare à celle que vous avez envoyée.

- Tâche 2 : créer une chaîne de connexion

  Créez une chaîne que vous utiliserez comme une des valeurs d'entrée pour votre fonction de hachage cryptographique. La chaîne, appelée la chaîne de connexion, est une concaténation du nom de l'algorithme de hachage, de la date de la demande, d'une chaîne d'informations d'identification et de la demande convertie sous forme canonique de la tâche précédente. La chaîne d'informations d'identification elle-même est une concaténation de date, de région et d'informations de service.

- Tâche 3 : calculer une signature

  Calculez une signature pour votre demande à l'aide d'une fonction de hachage cryptographique qui accepte deux chaînes en entrée : votre chaîne de signature et une clé dérivée. La clé dérivée est calculée en commençant par votre clé d'accès secrète et en utilisant la chaîne d'étendue des informations d'identification pour créer une série de codes d'authentification des messages basés sur le hachage ()HMAC-SHA256.

Exemple de calcul de signature

L'exemple suivant explique en détail comment créer une signature pour une CreateCluster demande. Vous pouvez utiliser cet exemple comme référence pour vérifier votre propre méthode de calcul de signature. D'autres calculs de référence sont inclus dans la section Demander des exemples de signature du Guide de l'utilisateur IAM.

Vous pouvez utiliser une requête GET ou POST pour envoyer des demandes à Amazon Redshift. La différence entre les deux requêtes est que pour la requête GET, vos paramètres sont envoyés

comme paramètres de chaîne de requête. Pour la requête POST, ils sont inclus dans le corps de la demande. L'exemple suivant illustre une requête POST.

Dans cet exemple il est supposé que :

- L'horodatage de la demande est `Fri, 07 Dec 2012 00:00:00 GMT`.
- Le point de terminaison est la région USA Est (Virginie du Nord), `us-east-1`.

La syntaxe générale de la demande est :

```
https://redshift.us-east-1.amazonaws.com/
   ?Action=CreateCluster
   &ClusterIdentifier=examplecluster
   &MasterUsername=masteruser
   &MasterUserPassword=12345678Aa
   &NumberOfNode=2
   &NodeType=dc2.large
   &Version=2012-12-01
   &x-amz-algorithm=AWS4-HMAC-SHA256
   &x-amz-credential=AKIAIOSFODNN7EXAMPLE/20121207/us-east-1/redshift/aws4_request
   &x-amz-date=20121207T000000Z
   &x-amz-signedheaders=content-type;host;x-amz-date
```

La forme canonique de la demande calculée pour Tâche 1 : Créer une demande canonique est :

```
POST
/

content-type:application/x-www-form-urlencoded; charset=utf-8
host:redshift.us-east-1.amazonaws.com
x-amz-date:20121207T000000Z

content-type;host;x-amz-date
55141b5d2aff6042ccd9d2af808fdf95ac78255e25b823d2dbd720226de1625d
```

La dernière ligne de la demande canonique est le hachage du corps de la demande. La troisième ligne de la requête canonique est vide, car il n'y a pas de paramètres d'interrogation pour cette API.

La chaîne de connexion de Tâche 2 : Créer une chaîne de connexion est :

```
AWS4-HMAC-SHA256
```

```
20121207T000000Z
20121207/us-east-1/redshift/aws4_request
06b6bef4f4f060a5558b60c627cc6c5b5b5a959b9902b5ac2187be80cbac0714
```

La première ligne de la chaîne de connexion est l'algorithme, la deuxième ligne est l'horodatage, la troisième ligne est les informations d'identification, et la dernière ligne est un hachage de la demande canonique issu de la tâche 1 : créer une demande canonique. Le nom du service à utiliser dans les informations d'identification est `redshift`.

Pour Tâche 3 : calculer une signature, la clé dérivée peut être représentée comme suit :

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20121207"),"us-
east-1"),"redshift"),"aws4_request")
```

La clé dérivée est calculée en tant que série de fonctions de hachage. À partir de l'instruction HMAC interne de la formule ci-dessus, vous concaténez l'expression « **AWS4** » et votre clé d'accès secrète, puis utilisez le résultat obtenu comme clé de hachage des données « us-east-1 ». Le résultat de ce hachage devient la clé de la fonction de hachage suivante.

Après que vous avez calculé la clé dérivée, vous l'utilisez dans une fonction de hachage qui accepte deux chaînes en entrée, votre chaîne de connexion et la clé dérivée. Par exemple, si vous utilisez la clé d'accès secrète `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY` et la chaîne de connexion fournie précédemment, la signature calculée est la suivante :

```
9a6b557aa9f38dea83d9215d8f0eae54100877f3e0735d38498d7ae489117920
```

L'étape finale consiste à construire l'en-tête `Authorization`. Pour la clé d'accès de la démonstration `AKIAIOSFODNN7EXAMPLE`, l'en-tête (avec les sauts de ligne ajoutés pour faciliter la lecture) est :

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20121207/us-east-1/
redshift/aws4_request,
SignedHeaders=content-type;host;x-amz-date,
Signature=9a6b557aa9f38dea83d9215d8f0eae54100877f3e0735d38498d7ae489117920
```

Configuration de la CLI Amazon Redshift

Cette section explique comment configurer et exécuter les outils de ligne de AWS CLI commande à utiliser pour gérer Amazon Redshift. Les outils de ligne de commande Amazon Redshift

s'exécutent sur le AWS Command Line Interface (AWS CLI), qui utilise à son tour Python (https://www.python.org/). Il AWS CLI peut être exécuté sur n'importe quel système d'exploitation supportant Python.

Installation de la AWS Command Line Interface

Pour commencer à utiliser les outils de ligne de commande Amazon Redshift, vous devez d'abord configurer AWS CLI, puis ajouter des fichiers de configuration qui définissent les options de la CLI Amazon Redshift.

Si vous l'avez déjà installé et configuré AWS CLI pour un autre AWS service, vous pouvez ignorer cette procédure.

Pour installer la AWS Command Line Interface

1. Accédez à Installer ou mettre à jour vers la dernière version du AWS CLI, puis suivez les instructions d'installation du AWS CLI.

   Pour accéder à la CLI, vous avez besoin d'un ID de clé d'accès et d'une clé d'accès secrète. Utilisation des informations d'identification temporaires au lieu des clés d'accès à long terme si possible. Les informations d'identification temporaires incluent un ID de clé d'accès, une clé d'accès secrète et un jeton de sécurité qui indique la date d'expiration des informations d'identification. Pour plus d'informations, consultez la section Utilisation d'informations d'identification temporaires avec AWS des ressources dans le Guide de l'utilisateur IAM.
2. Créez un fichier contenant des informations de configuration telles que vos clés d'accès, la région par défaut et le format de sortie de commande. Puis définissez la variable d'environnement `AWS_CONFIG_FILE` pour faire référence à ce fichier. Pour obtenir des instructions détaillées, reportez-vous à la section Configuration de l'interface de ligne de AWS commande dans le guide de AWS Command Line Interface l'utilisateur.
3. Exécutez une commande de test pour vérifier que l' AWS CLI interface fonctionne. Par exemple, la commande suivante devrait afficher des informations d'aide pour l' AWS CLI :

   ```
   aws help
   ```

   La commande suivante devrait afficher des informations d'aide pour Amazon Redshift :

   ```
   aws redshift help
   ```

Pour obtenir des documents de référence sur les commandes de la CLI Amazon Redshift, consultez la section Amazon Redshift dans la référence de l' AWS CLI .

Amazon Redshift sans serveur

Amazon Redshift sans serveur facilite l'exécution et la mise à l'échelle des analyses sans avoir à provisionner ni à gérer d'entrepôt de données sur site. Avec Amazon Redshift sans serveur, les analystes de données, les développeurs et les scientifiques des données peuvent désormais utiliser Amazon Redshift pour obtenir des informations à partir de données en quelques secondes en chargeant des données dans l'entrepôt des données et en interrogeant des enregistrements à partir de l'entrepôt de données dans le cloud. Amazon Redshift approvisionne et met à l'échelle automatiquement la capacité de l'entrepôt des données afin de fournir des performances rapides pour les charges de travail exigeantes et imprévisibles. Vous payez uniquement en fonction de la capacité que vous utilisez. Vous pouvez bénéficier de cette simplicité sans apporter de modifications à vos applications existantes d'analyse et d'aide à la décision.

Pour plus d'informations sur les contrats de niveau de service Amazon Redshift sans serveur, consultez Accord de niveau de service Amazon Redshift.

Qu'est-ce qu'Amazon Redshift sans serveur ?

Amazon Redshift sans serveur alloue automatiquement la capacité de l'entrepôt des données et met intelligemment à l'échelle les ressources sous-jacentes. Amazon Redshift sans serveur ajuste la capacité en quelques secondes pour fournir des performances élevées et des opérations simplifiées, même pour les charges de travail les plus exigeantes et les plus volatiles.

Avec Amazon Redshift sans serveur, vous pouvez bénéficier des fonctions suivantes :

- Accédez aux données et analyse-les sans avoir besoin de configurer, de régler et de gérer des clusters alloués Amazon Redshift.
- Utilisez les capacités SQL supérieures d'Amazon Redshift, les performances de pointe et l'intégration des lacs de données pour effectuer des requêtes de manière transparente dans un entrepôt des données, un lac de données et des sources de données opérationnelles.
- Offrez des performances élevées et des opérations simplifiées en toutes circonstances, pour les charges de travail les plus exigeantes et les plus volatiles, avec une scalabilité automatique et intelligente.
- Utilisez les groupes de travail et les espaces de noms pour organiser les ressources informatiques et les données avec des contrôles de coûts granulaires.
- Ne payez que lorsque l'entrepôt des données est utilisé.

Avec Amazon Redshift sans serveur, vous utilisez une interface de console pour accéder à un entrepôt des données sans serveur ou à des API pour créer des applications. Grâce à l'entrepôt des données, vous pouvez accéder à votre stockage géré Amazon Redshift et à votre lac de données Amazon S3.

Cette vidéo vous montre comment Amazon Redshift sans serveur facilite l'exécution et la mise à l'échelle des analyses sans avoir à gérer une infrastructure d'entrepôts des données :

Console Amazon Redshift sans serveur

Pour commencer à utiliser la console Amazon Redshift sans serveur, regardez la vidéo suivante : Premiers pas avec Amazon Redshift sans serveur.

Tableau de bord sans serveur

Dans la page Serverless dashboard (Tableau de bord sans serveur), vous pouvez afficher un résumé de vos ressources et des graphiques de votre utilisation.

- Namespace overview (Vue d'ensemble des espaces de noms) : cette section indique la quantité d'instantanés et de données dans votre espace de noms.
- Workgroups (Groupes de travail) : cette section présente tous les groupes de travail d'Amazon Redshift sans serveur.
- Queries metrics (Métriques des requêtes) : cette section montre l'activité des requêtes pour la dernière heure.
- RPU capacity used (Capacité utilisée par RPU) : cette section présente la capacité utilisée au cours de la dernière heure.
- Essai gratuit — Cette section indique les crédits d'essai gratuits restants sur votre AWS compte. Cela couvre toute utilisation des ressources et des opérations d'Amazon Redshift sans serveur, y compris les instantanés, le stockage, les groupes de travail, et plus encore, sous le même compte.
- Alarms (Alarmes) : cette section présente les alarmes que vous avez configurées dans Amazon Redshift sans serveur.

Sauvegarde des données

Dans l'onglet Data backup(Sauvegarde des données), vous pouvez utiliser les éléments suivants :

- Snapshots (Instantanés) : vous pouvez créer, supprimer et gérer des instantanés de vos données Amazon Redshift sans serveur. La période de conservation par défaut est `indefinitely`, mais

vous pouvez configurer la période de conservation pour qu'elle corresponde à n'importe quelle valeur comprise entre 1 et 3 653 jours. Vous pouvez autoriser la restauration Comptes AWS des espaces de noms à partir d'un instantané.

- Recovery points (Points de récupération) : affiche les points de récupération créés automatiquement afin que vous puissiez effectuer une récupération après une écriture ou une suppression accidentelle au cours des dernières 24 heures. Pour récupérer des données, vous pouvez restaurer un point de récupération dans n'importe quel espace de noms disponible. Vous pouvez créer un instantané à partir d'un point de récupération si vous souhaitez conserver un point de récupération plus longtemps. La période de conservation par défaut est `indefinitely`, mais vous pouvez configurer la période de conservation pour qu'elle corresponde à n'importe quelle valeur comprise entre 1 et 3 653 jours.

Accès aux données

Dans l'onglet Data access (Accès aux données), vous pouvez utiliser les éléments suivants :

- Paramètres réseau et de sécurité : vous pouvez consulter VPC-related les valeurs, les valeurs de AWS KMS chiffrement et les valeurs de journalisation des audits. Vous pouvez uniquement mettre à jour la journalisation de l'audit.
- AWS KMS key — la valeur AWS KMS key utilisée pour chiffrer les ressources dans Amazon Redshift sans serveur.
- Permissions (Autorisations) : vous pouvez gérer les rôles IAM qu'Amazon Redshift sans serveur peut assumer pour utiliser des ressources en votre nom. Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Redshift Serverless.
- Redshift-managed Points de terminaison VPC : vous pouvez accéder à votre instance Amazon Redshift Serverless depuis un autre VPC ou sous-réseau. Pour de plus amples informations, veuillez consulter Connexion à Amazon Redshift sans serveur depuis d'autres points de terminaison d'un VPC.

Restrictions

Dans l'onglet Limits (Limites), vous pouvez utiliser les éléments suivants :

- paramètres Base capacity in Redshift processing units (RPUs) (Capacité de base dans les unités de traitement Redshift (RPU)) : vous pouvez définir la capacité de base utilisée pour traiter votre charge de travail. Pour améliorer les performances des requêtes, augmentez la valeur de votre RPU.

- Usage limits (Limites d'utilisation) : les ressources de calcul maximales que votre instance Amazon Redshift sans serveur peut utiliser dans un laps de temps avant qu'une action ne soit lancée. Vous limitez la quantité de ressources qu'Amazon Redshift sans serveur utilise pour exécuter votre charge de travail. L'utilisation est mesurée en heures d'unité de traitement Redshift (RPU). Une heure RPU désigne le nombre de RPU utilisées en une heure. Vous déterminez une action à effectuer lorsqu'un seuil défini est atteint, comme suit :
  - Envoyez une alerte.
  - Journaliser une entrée dans une table système.
  - Désactivez les requêtes des utilisateurs.

  Vous pouvez configurer jusqu'à quatre limites.
- Query limits (Limites des requêtes) : vous pouvez ajouter une limite pour contrôler les performances et les limites. Pour plus d'informations sur les limites de surveillance de requête, consultez Règles de surveillance de requête WLM.

Pour de plus amples informations, veuillez consulter Capacité de calcul pour Amazon Redshift sans serveur.

Unités de partage des données

Dans l'onglet Unités de partage des données, vous pouvez utiliser les éléments suivants :

- Paramètres Unités de partage des données créées dans mon espace de noms : vous pouvez créer une unité de partage des données et la partager avec d'autres espaces de noms et Comptes AWS.
- Partages de données provenant d'autres espaces de noms et Comptes AWS : vous pouvez créer une base de données à partir d'une unité de partage des données, à partir d'un autre espace de noms et de Comptes AWS.

Pour plus d'informations sur le partage de données, consultez Partage de données dans Amazon Redshift sans serveur.

Surveillance des requêtes et des bases de données

Sur la page Query and database monitoring (Surveillance des requêtes et des bases de données), vous pouvez afficher des graphiques de votre historique des requêtes et de vos performance de base de données.

Sur l’onglet Query history (Historique des requêtes), vous voyez les graphiques suivants (vous pouvez choisir entre Query list (Liste des requêtes) et Resource metrics) (Métriques de ressources) :

- Query runtime (Exécution de requête) : ce graphique montre les requêtes qui sont en cours d’exécution pendant la même période. Choisissez une barre du graphique pour afficher plus de détails sur l’exécution de la requête.
- Queries and loads (Requêtes et charges) : cette section répertorie les requêtes et les charges effectuées par ID de requête.
- RPU capacity used (Capacité de RPU utilisée) : ce graphique montre la capacité globale des unités de traitement Redshift (RPU).
- Database connections (Connexions à la base de données) : ce graphique indique le nombre de connexions actives à la base de données.

Performances des bases de données

Sur l’onglet Database performance (Performance de base de données), vous voyez les graphiques suivants :

- Queries completed per second (Requêtes terminées par seconde) : ce graphique montre le nombre moyen de requêtes terminées par seconde.
- Queries duration (Durée de la requête) : le temps moyen nécessaire pour exécuter une requête.
- Database connections (Connexions à la base de données) : ce graphique indique le nombre de connexions actives à la base de données.
- Running queries (Requêtes en cours d’exécution) : ce graphique montre le nombre total de requêtes en cours d’exécution à un moment donné.
- Queued queries (Requêtes en file d’attente) : ce graphique montre le nombre total de requêtes mises en file d’attente à un moment donné.
- Query run time breakdown (Ventilation du temps d’exécution des requêtes) : ce graphique montre la durée totale des requêtes exécutées par type de requête.

Surveillance des ressources

Sur la page Resource monitoring (Surveillance des ressources), vous pouvez afficher les graphiques de vos ressources consommées. Vous pouvez filtrer les données en fonction de plusieurs facettes.

- Metric filter (Filtre de métrique) : vous pouvez utiliser des filtres de métriques pour sélectionner des filtres pour un groupe de travail spécifique, ainsi que pour choisir la plage de temps et l'intervalle de temps.
- RPU capacity used (Capacité de RPU utilisée) : ce graphique montre la capacité globale des unités de traitement Redshift (RPU).
- Utilisation du calcul : ce graphique montre l'utilisation d'heures de RPU par période pour la plage de temps sélectionnée. Pour les plages de temps inférieures à 6 heures, les heures de RPU sont affichées avec le temps exact. Pour les plages de temps de 6 heures ou plus, les heures de RPU sont affichées sous forme de moyennes.
- Calcul supplémentaire pour les optimisations automatiques facturées en secondes : ce graphique indique le nombre de transactions RPU-seconds facturées pour les optimisations automatiques de base de données pour la plage de temps sélectionnée. Les optimisations automatiques vous sont facturées lorsque Amazon Redshift utilise des ressources de calcul supplémentaires pour les exécuter. Pour plus d'informations, consultez la section Allocation de ressources de calcul supplémentaires pour l'optimisation automatique des bases de données.

Unités de partage des données

Sur la page Unités de partage des données, vous pouvez gérer des unités de partage des données dans mon compte et depuis d'autres comptes. Pour plus d'informations sur le partage de données, consultez Partage de données dans Amazon Redshift sans serveur.

AWS Glue Data Catalog

Dans l'onglet AWS Glue Data Catalog, vous pouvez consulter le statut d'enregistrement de votre espace de noms auprès du AWS Glue Data Catalog. Cet onglet n'apparaît qu'une fois que vous avez entamé le processus d'enregistrement. Pour plus d'informations sur l'enregistrement des espaces de noms dans le AWS Glue Data Catalog, consultez la section Compatibilité d'Apache Iceberg pour Amazon Redshift dans le Amazon Redshift Database Developer Guide.

Considérations relatives à l'utilisation d'Amazon Redshift sans serveur

Pour obtenir la liste des Régions AWS endroits où Amazon Redshift Serverless est disponible, consultez les points de terminaison répertoriés pour l'API Redshift Serverless dans le. Référence générale d'Amazon Web Services

Certaines ressources utilisées par Amazon Redshift sans serveur sont soumises à des quotas. Pour de plus amples informations, veuillez consulter Quotas pour les objets Amazon Redshift sans serveur.

Lorsque vous DÉCLAREZ un curseur, les spécifications de taille du jeu de résultats pour Amazon Redshift sans serveur sont spécifiées dans DECLARE. Amazon Redshift sans serveur dispose d'un curseur d'une taille totale maximale de 150 000 Mo pour l'ensemble de résultats.

Application de correctifs en ligne : Amazon Redshift Serverless propose des mises à jour logicielles automatiques sans nécessiter de fenêtres de maintenance traditionnelles. Lorsqu'une nouvelle mise à jour est disponible, le système l'applique dans les 14 jours suivant sa publication pendant les périodes d'inactivité. Le processus de mise à jour prend généralement jusqu'à 15 minutes. Si aucune période d'inactivité de 15 minutes ne se produit dans les 14 jours, votre terminal sans serveur peut connaître une brève indisponibilité. Pendant cette période, les connexions des applications aux terminaux peuvent échouer. Vous pouvez suivre les versions de correctifs Redshift dans la documentation « Versions de cluster pour Amazon Redshift ». Pour plus d'informations sur les contrats de niveau de service Amazon Redshift sans serveur, consultez Accord de niveau de service Amazon Redshift.

Suivi : lorsque Amazon Redshift publie une nouvelle version de groupe de travail, votre groupe de travail est automatiquement mis à jour. Vous pouvez vérifier si votre groupe de travail est mis à jour par rapport à la dernière version approuvée ou à la précédente. Pour plus d'informations sur le suivi, consultez Suivi des clusters alloués Amazon Redshift et des groupes de travail sans serveur.

ID de zone de disponibilité : lorsque vous configurez votre instance Amazon Redshift sans serveur, ouvrez Considérations supplémentaires et assurez-vous que les ID de sous-réseau fournis dans le champ Sous-réseau contiennent au moins deux des ID de zone de disponibilité pris en charge.

- Pour les groupes de travail sans routage VPC amélioré (EVR), vous avez besoin de deux zones de disponibilité (AZ).
- Pour les groupes de travail avec routage VPC amélioré, vous avez besoin de trois trois zones de disponibilité.

Pour voir le mappage du sous-réseau à l'ID de zone de disponibilité, accédez à la console VPC et choisissez Subnets (Sous-réseaux) pour afficher la liste des ID de sous-réseau avec leurs ID de zone de disponibilité. Vérifiez que votre sous-réseau est mappé à un ID de zone de disponibilité pris en charge. Pour créer un sous-réseau, consultez Créer un sous-réseau dans votre VPC dans le Guide de l'utilisateur Amazon VPC.

Trois sous-réseaux (sans routage VPC amélioré) : vous devez avoir trois sous-réseaux minimum et ils doivent être répartis sur trois zones de disponibilité.

Trois sous-réseaux (avec routage VPC amélioré UNIQUEMENT) : vous devez avoir trois sous-réseaux minimum quand vous utilisez le routage VPC amélioré et ils doivent être répartis sur trois zones de disponibilité ou plus.

Exigences relatives aux adresses IP libres : lorsque vous utilisez Redshift sans serveur sans que le routage VPC amélioré soit activé, vous devez disposer d'au moins trois adresses IP libres dans chaque sous-réseau. Il s'agit d'une exigence du bon fonctionnement du service.

Lors de la mise à jour des RPU pour le déploiement de Redshift sans serveur, au moins trois adresses IP libres doivent être disponibles dans chaque sous-réseau pour répondre aux exigences opérationnelles du service.

Pour plus d'informations sur l'attribution d'adresses IP et la compréhension de l'adressage IP dans Amazon VPC, consultez Adressage IP pour vos VPC et sous-réseaux dans le Guide de l'utilisateur Amazon VPC.

Without EVR

Si vous n'utilisez pas le routage VPC amélioré, vous devez disposer d'au moins trois adresses IP libres pour chaque sous-réseau, quelle que soit la taille de la RPU de base (4 à 1 024 RPU) ou l'utilisation de la RPU par votre ou vos groupes de travail. La nécessité d'une adresse IP 3 s'applique également aux groupes de travail dont les fonctionnalités de mise à AI-driven l'échelle et d'optimisation sont activées.

With Enhanced VPC Routing (EVR)

Si vous utilisez un routage VPC amélioré avec Redshift sans serveur, le nombre minimum d'adresses IP requises lors de la création d'un groupe de travail est le suivant :

Unités de traitement Redshift (RPU)	Adresses IP libres requises	Taille minimum du CIDR
4	9	/27
8	9	/27
16	13	/27

Unités de traitement Redshift (RPU)	Adresses IP libres requises	Taille minimum du CIDR
32	13	/27
64	21	/27
128	37	/26
256	69	/25
512	133	/24
1 024	261	/23

Avec le routage VPC amélioré, vous avez également besoin d'adresses IP libres lorsque vous mettez à jour votre groupe de travail afin d'utiliser davantage de RPU. Le nombre minimum d'adresses IP libres requises lors de la mise à jour des sous-réseaux d'un groupe de travail est le suivant :

Unités de traitement Redshift (RPU)	Unités de traitement Redshift (RPU) mises à jour	Adresses IP libres requises
4	8	10
8	16	10
16	32	13
32	64	16
64	128	28
128	256	52
256	512	100
512	1 024	197

> **Note**
>
> La capacité RPU de base maximale de 1 024 n'est disponible que dans les Régions AWS suivantes :
>
> - USA Est (Virginie du Nord)
> - USA Est (Ohio)
> - USA Ouest (Oregon)
> - Europe (Irlande)
> - Europe (Londres)

Pour plus d'informations sur l'allocation d'adresses IP, consultez Adressage IP dans le Guide de l'utilisateur Amazon VPC.

Storage space after migration (Espace de stockage après migration) : lors de la migration de petits clusters provisionnés Amazon Redshift vers Amazon Redshift sans serveur, vous pouvez constater une augmentation de l'allocation d'espace de stockage après la migration. Ceci est le fruit d'une allocation optimisée de l'espace de stockage, qui se traduit par un espace de stockage pré-alloué. Cet espace est utilisé au fur et à mesure de la croissance des données dans Amazon Redshift sans serveur.

Datasharing between Amazon Redshift sans serveur and Amazon Redshift provisioned clusters (Partage des données entre des clusters provisionnés Amazon Redshift sans serveur et Amazon Redshift) : lors du partage des données, où Amazon Redshift sans serveur est le producteur et un cluster provisionné est le consommateur, le cluster provisionné doit disposer d'une version de cluster supérieure à 1.0.38214. Si vous utilisez une version de cluster antérieure à celle-ci, une erreur se produit lorsque vous exécutez une requête. Vous pouvez consulter la version du cluster sur la console Amazon Redshift dans l'onglet Maintenance. Vous pouvez également exécuter `SELECT version();`.

Max query execution time (Délai d'exécution maximale des requêtes) : temps écoulé pour l'exécution d'une requête (en secondes). Le délai d'exécution n'inclut pas le temps d'attente dans une file d'attente. Si une requête dépasse le délai d'exécution défini, Amazon Redshift sans serveur arrête la requête. Les valeurs valides sont comprises entre 0 et 86 399.

Migration vers des tables dotées de clés de tri entrelacées : lors de la migration de clusters provisionnés par Amazon Redshift vers Amazon Redshift sans serveur, Redshift convertit les tables

comportant des clés de tri entrelacées et DISTSTYLE KEY en clés de tri composées. Le DISTSTYLE ne change pas. Pour en savoir plus sur les styles de distribution, consultez Utilisation des styles de distribution de données dans le Guide du développeur Amazon Redshift. Pour en savoir plus sur les clés de tri, consultez Utilisation des clés de tri.

Partage de VPC : vous pouvez créer des groupes de travail Amazon Redshift sans serveur dans un VPC partagé. Dans ce cas, nous vous recommandons de ne pas supprimer le partage des ressources, car cela pourrait rendre le groupe de travail indisponible.

Support IPv6 :

Amazon Redshift Serverless prend en charge la configuration de vos groupes de travail Amazon Redshift avec des adresses IPv4 et IPv6 (double pile) ou des IPv4-only configurations au sein de vos clouds privés AWS virtuels (VPC). Vous pouvez activer la prise en charge IPv6 lors de la création de nouveaux groupes de travail Amazon Redshift Serverless ou modifier des groupes de travail existants pour prendre en charge l'adressage IPv6. Grâce à cette fonctionnalité, vous pouvez déployer des entrepôts Amazon Redshift Serverless dans des sous-réseaux IPv6-enabled VPC et configurer les paramètres réseau pour prendre en charge les besoins croissants en espace d'adressage de vos applications. Vos applications peuvent désormais communiquer avec les entrepôts Amazon Redshift Serverless à l'aide des protocoles IPv4 ou IPv6, garantissant ainsi la compatibilité avec les architectures réseau existantes et futures.

Capacité de calcul pour Amazon Redshift sans serveur

Avec Amazon Redshift sans serveur, la capacité de calcul se met automatiquement à l’échelle pour répondre aux exigences de votre charge de travail. La capacité de calcul fait référence à la puissance de traitement et à la mémoire allouées à vos charges de travail Amazon Redshift sans serveur. Les cas d’utilisation courants incluent la gestion des périodes de pointe, l’exécution d’analyses complexes ou le traitement efficace de gros volumes de données. Les conditions suivantes fournissent des informations sur la manière dont Amazon Redshift gère la capacité de calcul.

RPU

Amazon Redshift sans serveur mesure la capacité de l’entrepôt des données en unités de traitement Redshift (RPU). Les RPU sont des ressources utilisées pour traiter les charges de travail. Une RPU fournit 16 Go de mémoire.

Capacité de base

Ce paramètre spécifie la capacité de l'entrepôt des données de base qu'Amazon Redshift utilise pour servir les requêtes. La capacité de base est spécifiée en RPU. Vous pouvez définir une capacité de base dans les unités de traitement Redshift (RPU). La définition d'une capacité de base plus élevée améliore les performances des requêtes, notamment pour les tâches de traitement des données qui exigent beaucoup de ressources. La capacité de base par défaut pour Amazon Redshift sans serveur est de 128 RPU. Vous pouvez régler le paramètre Capacité de base de 4 à 512 RPU. Vous pouvez définir cette valeur sur 4 RPU, ou en unités de 8 à 8 RPU ou plus (8, 16, 24... 512). Vous pouvez définir cette valeur à l'aide de la AWS console, de l'opération `UpdateWorkgroup` API ou de `update-workgroup` l'opération dans le AWS CLI.

Avec une capacité de base minimale de 8 RPU, vous disposez d'une certaine flexibilité pour exécuter des charges de travail plus simples ou plus complexes en fonction des coûts et des exigences de capacité de votre entrepôt de données. La capacité de base de 4 RPU est destinée aux entrepôts contenant moins de 32 To de données, et les capacités de base de 8, 16 et 24 RPU sont destinées aux charges de travail nécessitant moins de 128 To de données. Si vos besoins en données sont supérieurs à 128 To, vous devez utiliser un minimum de 32 RPU de base. Par ailleurs, pour les charges de travail comportant des tables avec un grand nombre de colonnes et une forte simultanéité, nous vous recommandons d'utiliser 32 RPU de base ou plus.

Les RPU de base maximum disponibles, 1 024, ajoutent le plus haut niveau de ressources informatiques à vos charges de travail. Cela offre une plus grande flexibilité pour prendre en charge des charges de travail très complexes et accélère le chargement et l'interrogation des données.

> **Note**
>
> Une capacité RPU de base maximale étendue de 1024 est disponible dans les versions suivantes Régions AWS. Dans les autres régions, la capacité de base maximale est de 512 RPU.
>
> - USA Est (Virginie du Nord)
> - USA Est (Ohio)
> - USA Ouest (Oregon)
> - Europe (Irlande)
> - Europe (Francfort)

Vous pouvez incrémenter ou décrémenter les RPU en unités de 32 lorsque vous définissez une capacité de base comprise entre 512 et 1 024 RPU.

Si vous gérez des charges de travail plus importantes et plus complexes, envisagez d'augmenter la taille de votre entrepôt de données Redshift sans serveur. Les grands entrepôts ont accès à davantage de ressources informatiques, ce qui leur permet de traiter les requêtes plus efficacement.

Voici quelques exemples dans lesquels il est avantageux de disposer d'une capacité de base plus élevée :

- Vous avez des requêtes complexes dont l'exécution prend beaucoup de temps
- Vos tableaux comportent un grand nombre de colonnes.
- Vos requêtes comportent un nombre élevé de JOIN.
- Vos requêtes regroupent ou analysent de grandes quantités de données provenant d'une source externe, telle qu'un lac de données.

Pour de plus amples informations sur les quotas et limites d'Amazon Redshift sans serveur, consultez Quotas pour les objets Amazon Redshift sans serveur.

Considérations et limitations relatives à la capacité d'Amazon Redshift sans serveur

Vous trouverez ci-après des considérations et des limitations concernant la capacité d'Amazon Redshift sans serveur. Pour les considérations générales relatives à Redshift sans serveur, consultez Considérations relatives à l'utilisation d'Amazon Redshift sans serveur.

- Les configurations de 4 RPU de base prennent en charge une capacité de stockage allant jusqu'à 32 To. Si vous utilisez plus de 32 To de stockage géré, vous ne pouvez pas passer à moins de 8 RPU de base.
- Les configurations de 8 ou 16 RPU de base prennent en charge une capacité de stockage gérée par Redshift allant jusqu'à 128 To. Si vous utilisez plus de 128 To de stockage géré, vous ne pouvez pas passer à moins de 32 RPU de base.
- La modification de la capacité de base de votre groupe de travail peut annuler certaines requêtes exécutées sur votre groupe de travail.

- Redshift sans serveur met à l'échelle les RPU pour votre entrepôt de données en utilisant les incréments suivants :
  - 4 à 8 RPU : augmentation par paliers de 4 RPU.
  - 8 à 512 RPU : augmentation par paliers de 8 RPU.
  - 512 à 1 024 RPU : augmentation par paliers de 32 RPU.
- Vacuum Boost n'est pris en charge que pour 8 RPU et plus. Pour 8 RPU ou moins, utilisez plutôt la commande suivante :

```
VACUUM [FULL | SORT ONLY | DELETE ONLY | REINDEX | RECLUSTER] [table_name] [TO
 threshold PERCENT]
```

Redshift sans serveur avec capacité de 4 unités de traitement Redshift (RPU)

Redshift sans serveur avec une capacité de 4 RPU de base est idéal pour les charges de travail plus petites ou moins exigeantes. Ce point d'entrée offre une solution flexible et rentable. Cette configuration d'entrée prend en charge les entrepôts de données dotés des ressources suivantes au maximum :

- Jusqu'à 32 To de stockage géré par Redshift.
- Un maximum de 100 colonnes par table
- 64 Go de mémoire

Si vous devez dépasser ces limites, vous devez augmenter votre capacité de base manuellement, plutôt que de vous fier à l'autoscaling. Une fois que vous aurez étendu votre entrepôt de données au-delà de 4 RPU, votre entrepôt de données continuera à utiliser davantage de RPU, et Amazon Redshift ne réduira pas votre entrepôt de données à 4 RPU.

> **Note**
>
> Vous pouvez créer des tables de plus de 100 colonnes lorsque vous utilisez 4 RPU de base, mais nous vous recommandons de limiter les tables à 100 colonnes. Le dépassement de cette limite peut entraîner l'épuisement de la mémoire de votre entrepôt de données lors de l'exécution des requêtes, ce qui réduit les performances.

Vous pouvez créer des entrepôts de données utilisant 4 RPU comme suit : Régions AWS

- USA Est (Ohio)
- USA Est (Virginie du Nord)
- USA Ouest (Californie du Nord)
- USA Ouest (Oregon)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asia Pacific (Tokyo)
- Europe (Irlande)
- Europe (Stockholm)

AI-driven mise à l'échelle et optimisation

> **Note**
>
> AI-driven le dimensionnement et l'optimisation sont disponibles dans toutes les AWS régions où Amazon Redshift Serverless est disponible.

Amazon Redshift Serverless propose une fonctionnalité avancée de mise à AI-driven l'échelle et d'optimisation pour répondre aux diverses exigences en matière de charge de travail. Les entrepôts de données peuvent rencontrer les problèmes de provisionnement suivants :

- Les entrepôts de données peuvent être suralloués pour améliorer les performances des requêtes gourmandes en ressources
- Les entrepôts de données peuvent être sous-alloués pour réduire les coûts.

Il est difficile de trouver le juste équilibre entre performance et coût pour les charges de travail des entrepôts de données, en particulier en cas de requêtes ad hoc et de volumes de données croissants. Lorsque vous exécutez des charges de travail mixtes, comprenant à la fois des requêtes peu ou fortement gourmandes en ressources, une mise à l’échelle intelligente est nécessaire. La fonctionnalité de mise à l' AI-driven échelle et d'optimisation adapte automatiquement le calcul sans serveur ou les RPU en réponse à la croissance des données. Cette fonctionnalité permet également de maintenir les performances des requêtes dans le respect des objectifs de performance et de prix

ciblés. La AI-driven mise à l'échelle et l'optimisation allouent dynamiquement les ressources de calcul à mesure que les volumes de données augmentent, garantissant ainsi que les requêtes continuent d'atteindre les objectifs de performance. AI-driven la mise à l'échelle et l'optimisation permettent au service de s'adapter facilement à l'évolution des exigences en matière de charge de travail, sans intervention manuelle ni planification complexe des capacités.

Amazon Redshift sans serveur fournit une solution de mise à l'échelle plus complète et plus réactive basée sur des facteurs tels que la complexité des requêtes et le volume de données. Cette fonctionnalité permet d'optimiser le rapport prix/performances des charges de travail tout en conservant la flexibilité nécessaire pour gérer efficacement des charges de travail variables et des jeux de données croissants. Amazon Redshift Serverless peut appliquer automatiquement le AI-driven dimensionnement et l'optimisation à votre point de terminaison Amazon Redshift Serverless afin d'atteindre les objectifs de prix/performances que vous avez spécifiés pour votre groupe de travail sans serveur. Cette optimisation automatique du rapport prix/performances est particulièrement utile si vous ne savez pas quelle capacité de base définir pour vos charges de travail, ou si certaines parties de votre charge de travail peuvent profiter d'un plus grand nombre de ressources allouées.

Exemple

Si votre organisation exécute des charges de travail qui nécessitent uniquement 32 RPU mais qu'elle introduit soudainement une requête plus complexe, vous ne connaissez peut-être pas la capacité de base approprié. La définition d'une capacité de base plus élevée permet d'obtenir de meilleures performances, mais elle entraîne également des coûts plus élevés, de sorte que le coût risque de ne pas correspondre à vos attentes. Grâce AI-driven à la mise à l'échelle et à l'optimisation, Amazon Redshift Serverless ajuste automatiquement les RPU pour atteindre vos objectifs de prix-performance tout en optimisant les coûts pour votre entreprise. Cette optimisation automatique est utile quelle que soit la taille de la charge de travail. L'optimisation automatique peut vous aider à atteindre les rapports prix/performances cible de votre organisation en cas de requêtes complexes.

> **Note**
>
> Price-performance les cibles sont un paramètre spécifique au groupe de travail. Les différents groupes de travail peuvent avoir des rapports prix/performances cible différents.

Pour configurer les objectifs de rapport prix/performances, utilisez la AWS console. L'objectif prix-performance est activé par défaut pour tous les nouveaux groupes de travail sans serveur et est

défini sur Équilibré. Vous pouvez modifier l'objectif de prix/performances après avoir créé le groupe de travail Serverless.

Pour modifier l’objectif prix/performances pour votre groupe de travail

1. Dans la console Amazon Redshift sans serveur, choisissez Configuration de groupe de travail.
2. Choisissez le groupe de travail pour lequel vous souhaitez modifier le rapport prix/performances cible. Choisissez l’onglet Performances, puis choisissez Modifier.
3. Choisissez Price-performancela cible et réglez le curseur selon les paramètres souhaités.
4. Cliquez sur Enregistrer les modifications.
5. Pour mettre à jour le nombre maximal de RPU qu’Amazon Redshift sans serveur peut allouer à votre charge de travail, choisissez l’onglet Limites de la section Configuration du groupe de travail.

Vous pouvez utiliser le curseur Price-performance cible pour définir l'équilibre souhaité entre le coût et les performances. En déplaçant le curseur, vous pouvez choisir l’une des options suivantes :

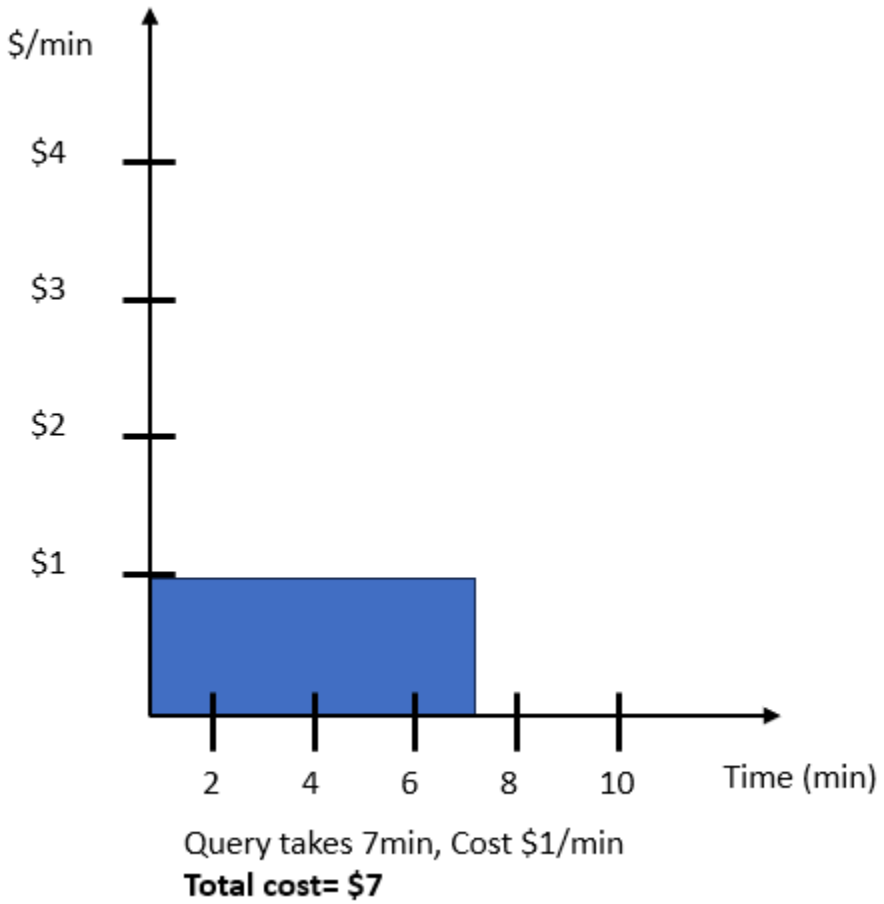
- Optimisation pour les coûts : ce paramètre donne la priorité aux économies de coûts. Amazon Redshift Serverless tente d'augmenter automatiquement la capacité de calcul uniquement lorsque cela est susceptible de réduire les coûts. Amazon Redshift sans serveur tente également de réduire les ressources de calcul à moindre coût, ce qui peut augmenter le temps d’exécution des requêtes.
- Équilibré : ce paramètre crée un équilibre entre les performances et les coûts. Amazon Redshift Serverless évolue en fonction des performances et peut entraîner une augmentation ou une diminution modérée des coûts. Il s’agit du paramètre recommandé pour la plupart des entrepôts de données Amazon Redshift sans serveur.
- Optimisation pour les performances : ce paramètre donne la priorité aux performances. Amazon Redshift met à l’échelle de manière agressive pour atteindre des performances élevées, ce qui peut entraîner des coûts plus élevés.
- Positions intermédiaires : vous pouvez également placer le curseur sur l’une des deux positions intermédiaires entre Équilibré et Optimisation pour les coûts ou Optimisation pour les performances. Utilisez ces paramètres si l’optimisation complète pour les coûts ou de performances est trop extrême.

Considérations lors du choix de votre objectif prix/performances

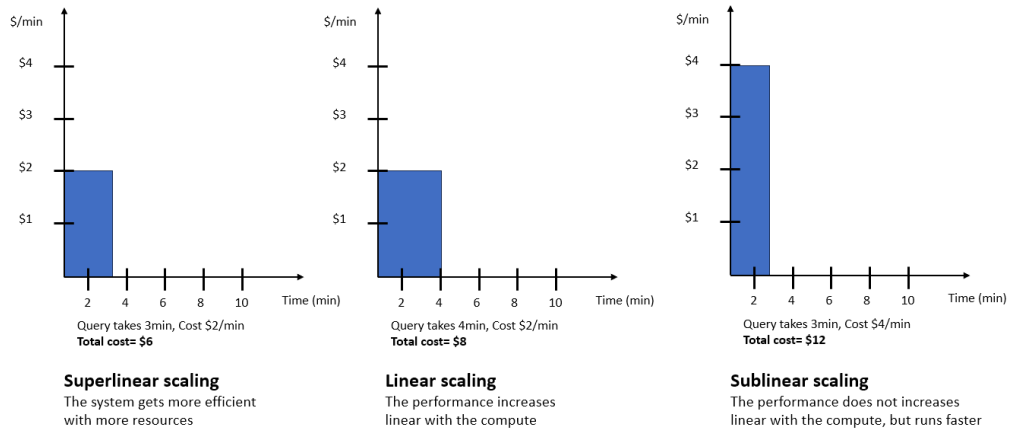
Vous pouvez utiliser le curseur de prix/performance pour choisir l’objectif prix/performance souhaité pour votre charge de travail. L'algorithme de AI-driven dimensionnement et d'optimisation apprend au fil du temps à partir de l'historique de votre charge de travail et améliore la précision des prévisions et des décisions.

Exemple

Pour cet exemple, supposons une requête qui prend sept minutes et coûte 7 $. La figure suivante montre les temps d’exécution et le coût des requêtes sans mise à l’échelle.



Une requête donnée peut être mise à l’échelle de différentes manières, comme indiqué ci-dessous. Sur la base de l'objectif prix/performance que vous avez choisi, le AI-driven dimensionnement et l'optimisation prédisent la manière dont la requête équilibre les performances et les coûts, et l'ajustent en conséquence. Le choix des différentes options du curseur donne les résultats suivants :



- Optimisation pour les coûts : avec l'option Optimisation pour les coûts, votre entrepôt de données évolue en privilégiant les choix qui réduisent vos coûts. Dans l'exemple précédent, l'approche de mise à l'échelle super linéaire montre ce comportement. La mise à l'échelle n'aura lieu que si elle peut être réalisée de manière rentable conformément aux prédictions modélisées de mise à l'échelle. Si les modèles de mise à l'échelle prédisent qu'une mise à l'échelle optimisée pour les coûts n'est pas possible pour une charge de travail donnée, l'entrepôt de données ne sera pas évolutif.
- Équilibré : avec l'option Équilibré, le système met à l'échelle tout en équilibrant les considérations de coût et de performance, avec une augmentation potentielle limitée des coûts. L'option Équilibré effectue une mise à l'échelle de la charge de travail superlinéaire, linéaire et éventuellement sublinéaire.
- Optimisation pour les performances : avec l'option Optimisation pour les performances, outre les méthodes précédentes d'amélioration des performances, le système met à l'échelle même si les coûts sont plus élevés, et ce n'est peut-être pas proportionnel à l'amélioration du temps d'exécution. Avec Optimisation pour les performances, le système effectue une mise à l'échelle superlinéaire, une mise à l'échelle linéaire et une mise à l'échelle sublinéaire si possible. Plus la position du curseur est proche de la position Optimisation pour les performances, plus Amazon Redshift sans serveur autorise le mise à l'échelle sublinéaire.

Lorsque vous réglez le Price-Performancecurseur, tenez compte des points suivants :

- Vous pouvez modifier le paramètre de prix/performances à tout moment, mais le mise à l'échelle de la charge de travail ne changera pas immédiatement. La mise à l'échelle change au fil du temps à mesure que le système prend connaissance de la charge de travail actuelle. Nous vous conseillons de surveiller un groupe de travail sans serveur pendant 1 à 3 jours afin de vérifier l'impact du nouveau paramètre.

- Les options du curseur prix/performance Max capacity et Max fonctionnent ensemble. RPU-hours La capacité maximale et la valeur maximale RPU-hours sont les commandes permettant de limiter le nombre maximal de RPU qu'Amazon Redshift Serverless permet à l'entrepôt de données de faire évoluer, ainsi que le nombre maximum d'heures de RPU qu'Amazon Redshift Serverless permet à l'entrepôt de données de consommer. Amazon Redshift sans serveur respecte et applique toujours ces paramètres, quel que soit l'objectif prix/performances fixé.

Surveillance de l'autoscaling des ressources

Vous pouvez contrôler la AI-driven mise à l'échelle et l'optimisation des manières suivantes :

- Consultez le graphique de capacité RPU utilisée sur la console Amazon Redshift.
- Surveillez la `ComputeCapacity` métrique en dessous `AWS/Redshift-Serverless` et `Workgroup` en aval CloudWatch.
- Interrogez la vue SYS_QUERY_HISTORY. Fournissez l'ID de requête ou le texte de la requête spécifique pour identifier la période. Utilisez cette période pour interroger la vue système SYS_SERVERLESS_USAGE afin de trouver la valeur `compute_capacity`. Le champ `compute_capacity` indique les RPU redimensionnées pendant l'exécution de la requête.

Utilisez l'exemple suivant pour interroger la vue `SYS_QUERY_HISTORY`. Remplacez les exemples de valeur par le texte de votre requête.

```
select query_id,query_text,start_time,end_time, elapsed_time/1000000.0
 duration_in_seconds
from sys_query_history
where query_text like '<query_text>'
and query_text not like '%sys_query_history%'
order by start_time desc
```

Exécutez la requête suivante pour voir comment `compute_capacity` a été mise à l'échelle au cours de la période allant de `start_time` à `end_time`. Remplacez `start_time` et `end_time` dans la requête suivante par le résultat de la requête précédente :

```
select * from sys_serverless_usage
where end_time >= 'start_time'
and end_time <= DATEADD(minute,1,'end_time')
order by end_time asc
```

Pour obtenir des instructions détaillées sur l'utilisation de ces fonctionnalités, consultez Configurer la surveillance, les limites et les alarmes dans Amazon Redshift sans serveur afin de garantir la prévisibilité des coûts.

Considérations relatives à l'utilisation du AI-driven dimensionnement et de l'optimisation

Lorsque vous utilisez la mise à l' AI-driven échelle et l'optimisation, tenez compte des points suivants :

- Pour les charges de travail existantes sur Amazon Redshift Serverless nécessitant de 8 à 512 RPU de base, AI-driven utilisez le dimensionnement et l'optimisation pour obtenir des résultats optimaux. Nous déconseillons d'utiliser cette fonctionnalité pour les charges de travail inférieures ou supérieures à cette plage de RPU.
- Price-performance les cibles optimisent automatiquement la charge de travail, même si les résultats peuvent varier. Utilisez cette fonctionnalité au fil du temps afin que le système puisse apprendre vos modèles spécifiques en exécutant une charge de travail représentative.
- AI-driven le dimensionnement et l'optimisation utilisent des moments optimaux pour appliquer des optimisations aux groupes de travail sans serveur en fonction de la charge de travail exécutée sur votre instance Amazon Redshift Serverless.

Pour en savoir plus sur la AI-driven mise à l'échelle et l'optimisation, regardez la vidéo suivante.

Facturation pour Amazon Redshift sans serveur

Facturation de la capacité de calcul

Vous pouvez acheter de la capacité pour Amazon Redshift sans serveur de deux façons :

- Vous pouvez acheter de la capacité à la demande : lorsque vous optez pour une capacité de calcul à la demande, vous payez les ressources au fur et à mesure. C'est le meilleur choix si vous commencez tout juste à utiliser Amazon Redshift Serverless ou si vous n'avez pas encore une idée précise de vos habitudes d'utilisation régulières. On-demand offre la plus grande flexibilité. Pour plus d'informations, consultez Facturation de la capacité de calcul à la demande.
- Vous pouvez acheter des réservations : une réservation offre une remise lorsque vous achetez une quantité prédéfinie de ressources informatiques pour une durée spécifique, par exemple pendant un an. C'est une bonne idée si vous savez que vous allez utiliser régulièrement une certaine

quantité de capacité. Il est utile d'économiser de l'argent lorsque vous pouvez prévoir certains de vos besoins en matière de capacité. Pour plus d'informations, consultez Facturation pour les réservations sans serveur.

Vous pouvez utiliser conjointement les réservations et les ressources à la demande. Il n'est pas nécessaire d'utiliser l'un ou l'autre.

Pour obtenir des informations détaillées sur la tarification, consultez Tarification Amazon Redshift.

Facturation de la capacité de calcul à la demande

La capacité de base et son incidence sur la facturation

Lorsque les requêtes sont exécutées, vous êtes facturé en fonction de la capacité utilisée pendant une durée donnée, en heures RPU sur une base par seconde. Lorsqu'aucune requête n'est en cours, vous n'êtes pas facturé pour la capacité de calcul. Vous êtes également facturé pour le stockage géré par Redshift sur la base de la quantité de données stockées.

Lorsque vous créez votre groupe de travail, vous avez la possibilité de définir la Capacité de base pour le calcul. Pour répondre aux price/performance exigences de votre charge de travail au niveau d'un groupe de travail, ajustez la capacité de base à la hausse ou à la baisse pour un groupe de travail existant. Sélectionnez le groupe de travail dans Configuration de groupe de travail et choisissez l'onglet Limites pour modifier la capacité de base à l'aide de la console.

À mesure que le nombre de requêtes augmente, Amazon Redshift sans serveur se met automatiquement à l'échelle pour assurer des performances constantes.

Limite d'utilisation maximale d'heures de RPU

Pour que les coûts restent prévisibles pour Amazon Redshift sans serveur, vous pouvez définir la valeur Maximum RPU hours (Nombre maximal d'heures RPU) utilisées par jour, par semaine ou par mois. Vous pouvez définir ce paramètre à l'aide de la console ou de l'API. Lorsqu'une limite est atteinte, vous pouvez configurer l'écriture d'une entrée de journal dans une table système, la réception d'une alerte ou la désactivation des requêtes de l'utilisateur. La fixation d'un nombre maximum d'heures RPU permet de maîtriser vos coûts. Les paramètres relatifs au nombre maximal d'heures RPU s'appliquent à votre groupe de travail pour les requêtes qui accèdent aux données de votre entrepôt des données et pour les requêtes qui accèdent à des données externes, par exemple dans une table externe d'Amazon S3.

Voici un exemple :

Supposons que vous définissiez une limite de 100 heures par semaine. Pour faire cela sur la console, procédez comme suit :

1. Choisissez votre groupe de travail, puis choisissez Gérer les limites d'utilisation sous l'onglet Limites.
2. Ajoutez une limite d'utilisation, en choisissant la fréquence Toutes les semaines, une durée de 100 heures et en définissant l'action Désactiver les requêtes utilisateur.

Dans cet exemple, si vous atteignez la limite de 100 heures de RPU par semaine, les requêtes sont désactivées.

Le fait de définir le nombre maximum d'heures de RPU pour le groupe de travail ne limite pas les performances ni les ressources de calcul pour le groupe de travail. Vous pouvez ajuster ces paramètres à tout moment sans affecter le traitement des requêtes. L'objectif de la définition du nombre maximum d'heures de RPU est de vous aider à répondre à vos exigences en matière de prix et de performances. Pour plus d'informations sur la facturation sans serveur, consultez Tarification Amazon Redshift.

Un autre moyen de garantir la prévisibilité du coût d'Amazon Redshift Serverless consiste à utiliser la détection des anomalies de AWS coût afin de réduire les risques de surprises liées à la facturation et de renforcer le contrôle.

> **Note**
>
> Le calculateur de tarification Amazon Redshift est utile pour estimer les tarifs. Vous saisissez les ressources de calcul dont vous avez besoin et il fournit un aperçu du coût.

Définition d'une capacité maximale pour contrôler les coûts des ressources de calcul

Le paramètre de capacité maximale sert de plafond de RPU qu'Amazon Redshift sans serveur peut atteindre. Il permet de contrôler le coût des ressources de calcul. D'une manière similaire à la manière dont la capacité de base définit une quantité minimale de ressources de calcul disponibles, la capacité maximale définit un plafond d'utilisation de RPU. De cette façon, elle permet à vos dépenses de rester conformes à vos plans. La capacité maximale s'applique spécifiquement à chaque groupe de travail et limite l'utilisation du calcul à tout moment.

En quoi la capacité maximale diffère-t-elle des limites d’utilisation d’heures de RPU ?

Les limites d'heures maximales de RPU et de capacité maximale peuvent vous aider à contrôler les coûts, mais elles fonctionnent de différentes manières. Les points suivants expliquent la différence :

- Capacité maximale : ce paramètre définit le nombre maximal de RPU qu'Amazon Redshift Serverless peut utiliser à des fins de dimensionnement automatique.
- Limite d’utilisation maximale d’heures de RPU : contrairement à la capacité maximale, ce paramètre ne définit pas un plafond de capacité. Mais il effectue d’autres actions pour vous aider à limiter les coûts. Elles incluent notamment l’ajout d’une entrée dans un journal, une notification ou l’arrêt de l’exécution des requêtes, si vous le souhaitez.

Vous pouvez utiliser exclusivement la capacité maximale ou la compléter par des actions correspondant aux limites d'utilisation maximale d'heures de RPU.

Cas d’utilisation de la capacité maximale

Chaque groupe de travail peut avoir une valeur de capacité maximale différente. Elle vous aide à faire respecter les exigences budgétaires. Pour illustrer ce fonctionnement, prenons l’exemple suivant :

- Vous disposez d’un groupe de travail dont la capacité de base est définie à 256 RPU. Vous avez des charges de travail régulières dépassant de justesse 256 RPU pendant la majeure partie du mois.
- La capacité maximale est définie sur 512 RPU.

Supposons que vous ayez un taux d’utilisation élevé inattendu sur une période de trois jours pour générer des rapports statistiques ponctuels. Dans ce cas, la capacité maximale est définie pour éviter des coûts de calcul supérieurs à ceux de 512 RPU. Avec cela, vous pouvez être sûr que la capacité de calcul ne dépassera pas cette limite supérieure.

Notes d’utilisation de la capacité maximale

Ces notes peuvent vous aider à définir la capacité maximale de manière appropriée :

- Chaque groupe de travail Amazon Redshift sans serveur peut avoir un paramètre de capacité maximale différent.

- Si vous traversez une période d'utilisation très élevée des ressources et que la capacité maximale est définie sur un faible niveau de RPU, cela peut retarder le traitement des charges de travail et entraîner une expérience utilisateur qui n'est pas optimale.
- Vous pouvez visualiser la capacité utilisée sur une période donnée sur le tableau de bord d'Amazon Redshift sans serveur. Pour plus d'informations sur l'affichage des données récapitulatives, consultez Vérification des données récapitulatives d'Amazon Redshift sans serveur à l'aide du tableau de bord.
- Les modifications de capacité maximale ne perturbent généralement pas l'exécution des requêtes. Toutefois, si vous définissez une capacité maximale en dessous de votre capacité de base actuelle, Amazon Redshift Serverless réduira immédiatement la capacité. Cela peut affecter votre charge de travail courante.
- La valeur maximale de la capacité maximale est de 5 632 RPU.

Comment définir la capacité maximale

Vous pouvez définir la capacité maximale dans la console. Pour un groupe de travail existant, vous pouvez modifier ce paramètre sous Configuration de groupe de travail. Vous pouvez également utiliser la CLI pour le définir à l'aide d'une commande, comme dans l'exemple suivant :

```
aws redshift-serverless update-workgroup --workgroup-name myworkgroup --max-capacity
 512
```

Cela définit le paramètre Capacité maximale pour le groupe de travail portant le nom spécifié. Après l'avoir définie, vous pouvez vérifier la valeur dans la console. Vous pouvez également vérifier la valeur à l'aide de la CLI en exécutant la commande `get-workgroup`.

Vous pouvez désactiver le paramètre Capacité maximale en lui affectant la valeur `-1`, comme suit :

```
aws redshift-serverless update-workgroup --workgroup-name myworkgroup --max-capacity -1
```

Surveillance de l'utilisation et des coûts d'Amazon Redshift sans serveur

Il existe plusieurs façons d'estimer l'utilisation et la facturation d'Amazon Redshift sans serveur. Les vues du système peuvent être utiles car les métadonnées du système, y compris les données de requête et d'utilisation, sont disponibles en temps opportun et vous n'avez aucune configuration à effectuer pour les interroger. CloudWatch peut également être utile pour surveiller l'utilisation de votre

instance Amazon Redshift Serverless, et possède des fonctionnalités supplémentaires pour fournir des informations et définir des actions.

Visualisation de l'utilisation en interrogeant une vue système

Interrogez la table système SYS_SERVERLESS_USAGE pour suivre l'utilisation et obtenir les frais des requêtes :

```
select trunc(start_time) "Day",
(sum(charged_seconds)/3600::double
precision) * <Price for 1 RPU> as cost_incurred
from sys_serverless_usage
group by 1
order by 1
```

Cette requête fournit le coût journalier d'Amazon Redshift sans serveur, en fonction de l'utilisation.

Notes d'utilisation pour déterminer l'utilisation et le coût

- Vous payez les charges de travail que vous exécutez à RPU-hours la seconde, avec une charge minimale de 60 secondes.
- Les enregistrements de la table système sys_serverless_usage indiquent les frais encourus par intervalles d'une minute. Il est important de comprendre les colonnes suivantes :

  La colonne charged_seconds :

  - Fournit les secondes d'unité de calcul (RPU) qui ont été facturées pendant l'intervalle de temps. Les résultats incluent tous les frais minimum dans Amazon Redshift sans serveur.
  - Contient des informations sur l'utilisation des ressources informatiques une fois les transactions terminées. La valeur de cette colonne peut donc être 0 si les transactions ne sont pas terminées.

  La colonne compute_seconds :

  - Fournit des informations en temps réel sur l'utilisation du calcul. Les résultats n'incluent pas les frais minimum dans Amazon Redshift sans serveur. Ils peuvent donc différer dans une certaine mesure des secondes facturées pendant l'intervalle.
  - Affiche les informations d'utilisation au cours de chaque transaction (même si une transaction n'est pas terminée) et les données fournies sont donc en temps réel.
- Il existe des situations où compute_seconds est égal à 0 mais où charged_seconds est supérieur à 0, ou vice versa. Il s'agit d'un comportement normal résultant de la manière dont

les données sont enregistrées dans la vue système. Pour une représentation plus précise des détails de l'utilisation sans serveur, nous recommandons d'agréger les données dans SYS_SERVERLESS_USAGE.

Pour plus d'informations sur la surveillance des tables et des vues, consultez Surveillance des requêtes et des charges de travail avec Amazon Redshift sans serveur.

Visualisation de l'utilisation avec CloudWatch

Vous pouvez utiliser les statistiques disponibles dans CloudWatch pour suivre l'utilisation. CloudWatch Les `ComputeSeconds` métriques générées pour indiquent le nombre total de secondes RPU utilisées dans la minute en cours et `ComputeCapacity` la capacité de calcul totale pour cette minute. Les métriques d'utilisation figurent également dans la console Redshift, sur le tableau de bord Redshift sans serveur. Pour plus d'informations CloudWatch, consultez Qu'est-ce qu'Amazon CloudWatch ?

Facturation pour les réservations sans serveur

Amazon Redshift sans serveur vous permet d'exécuter et de mettre à l'échelle des analyses sans avoir à provisionner ni à gérer des clusters avec un modèle de tarification à l'usage. Désormais, avec les réservations sans serveur, vous pouvez optimiser davantage vos coûts de calcul et améliorer la prévisibilité des coûts des charges de travail existantes et nouvelles sur Redshift sans serveur.

Amazon Redshift gère les réservations sans serveur au niveau du compte AWS payeur, et les réservations peuvent être partagées entre plusieurs AWS comptes, ce qui vous permet de réduire vos coûts de calcul jusqu'à 24 % sur toutes les charges de travail Redshift sans serveur de votre compte. AWS Amazon Redshift facture les réservations sans serveur toutes les heures et mesure les réservations par seconde, offrant ainsi un modèle de facturation cohérent, 24 heures sur 24, sept jours sur sept, tout en conservant la flexibilité offerte par Redshift sans serveur. Amazon Redshift facture toute utilisation dépassant le niveau de RPU spécifié au tarif standard à la demande.

> **Note**
>
> Si vous souhaitez limiter l'utilisation à la demande, vous pouvez utiliser le paramètre Capacité max. pour définir des limites d'utilisation des ressources pour vos groupes de travail. Pour plus d'informations, consultez Facturation pour Amazon Redshift sans serveur.

Avantages des réserves sans serveur

Les réservations sans serveur constituent une option tarifaire à prix réduit pour Amazon Redshift sans serveur. Les réservations sans serveur vous permettent de vous engager à utiliser un certain nombre d'unités de traitement Redshift (RPU) pendant un an à un prix remisé par rapport aux tarifs à la demande (OD), sans paiement initial. Vous pouvez bénéficier d'une réduction plus importante avec un paiement initial. Avec les réservations sans serveur, vous pouvez optimiser vos coûts de calcul et améliorer la prévisibilité des coûts des charges de travail existantes et nouvelles sur Redshift sans serveur.

Chaque réservation sans serveur est achetée au niveau du AWS compte et peut être partagée entre plusieurs groupes de travail Amazon Redshift Serverless au sein du même compte payeur. Cela vous donne une certaine flexibilité dans la manière dont la remise est appliquée. Plusieurs groupes de travail ayant des modèles de charge de travail différents peuvent partager la réservation.

Comment fonctionne une réservation sans serveur

La réservation de RPU est un processus simple qui ne dure que quelques minutes. Cela inclut la spécification du niveau de RPU à réserver et du type de paiement. Amazon Redshift Serverless utilise l'outil standard de AWS facturation et de gestion des coûts qui vous aide à déterminer le niveau de réservation dont vous avez besoin et à surveiller votre utilisation en permanence. Les réservations sans serveur sont gérées au niveau du compte AWS payeur et peuvent être partagées sous le même compte payeur, ce qui vous permet de réduire vos coûts de calcul jusqu'à 24 % sur toutes les charges de travail Redshift Serverless de votre compte. AWS Les réservations sans serveur sont facturées à l'heure et mesurées à la seconde, offrant ainsi un modèle de facturation cohérent, 24 heures sur 24, sept jours sur sept, tout en conservant la flexibilité offerte par Redshift sans serveur. Toute utilisation dépassant le niveau de RPU spécifié est facturée aux tarifs à la demande standard de Redshift sans serveur.

Vous pouvez effectuer plusieurs réservations sans serveur sur le même AWS compte. Lorsque vous achetez des réservations sans serveur supplémentaires, elles se superposent. Par exemple, si vous achetez deux réservations et que vous choisissez 100 RPU pour chacune, vous obtenez un total de 200 RPU à un tarif réduit.

> **Note**
>
> Si vous souhaitez définir une limite d'utilisation à la demande, vous pouvez définir le maximum de RPU dans la console Amazon Redshift sans serveur pour un groupe de travail en choisissant l'onglet Limites, puis en sélectionnant Gérer les limites d'utilisation.

Une fois que vous avez acheté une réservation sans serveur, elle entre en vigueur immédiatement et apparaît dans la console Redshift dans le tableau de bord des réservations sans serveur.

Analyse de votre utilisation de RPU (unité de traitement Redshift) pour déterminer le niveau de réservation dont vous avez besoin

Les réservations Redshift sans serveur vous permettent de bénéficier de coûts de calcul prévisibles et réduits en vous engageant à utiliser un nombre spécifique d'unités de traitement Redshift (RPU) pendant un an, ce qui vous permet de bénéficier de remises par rapport aux tarifs à la demande. Ces remises peuvent aller jusqu'à 20 % avec l'option sans paiement initial, ou jusqu'à 24 % lorsque vous payez d'avance. Vous achetez Redshift Serverless Reservations au niveau du AWS compte payeur, et vos économies s'appliquent automatiquement à n'importe quel groupe de travail Redshift Serverless sur n'importe quel compte AWS associé. Vous pouvez ainsi gérer les budgets de manière centralisée tout en soutenant plusieurs équipes. Redshift sans serveur mesure l'utilisation selon une granularité par seconde, arrondie chaque heure, puis facturée à l'heure, afin que vous ne payiez que pour la capacité que vous utilisez. Les réservations Redshift sans serveur associent une application flexible pour tous les comptes à des économies basées sur les termes, vous offrant ainsi des prix d'analyse prévisibles sans sacrifier l'agilité de Redshift sans serveur.

Analyse de l'utilisation de RPU pour les réservations

Vous pouvez déterminer vos niveaux d'utilisation de RPU de deux manières : vous pouvez utiliser le tableau de bord Redshift sans serveur pour une vue sur sept jours ou utiliser Cost Explorer pour une analyse à long terme. Les procédures suivantes montrent comment analyser votre utilisation de RPU :

Méthode 1 : Tableau de bord Redshift sans serveur (affichage sur 7 jours)

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Ouvrez le Tableau de bord sans serveur.

3. Choisissez votre groupe de travail.
4. Consultez votre utilisation de la capacité RPU sur une période allant de la dernière heure à une semaine.

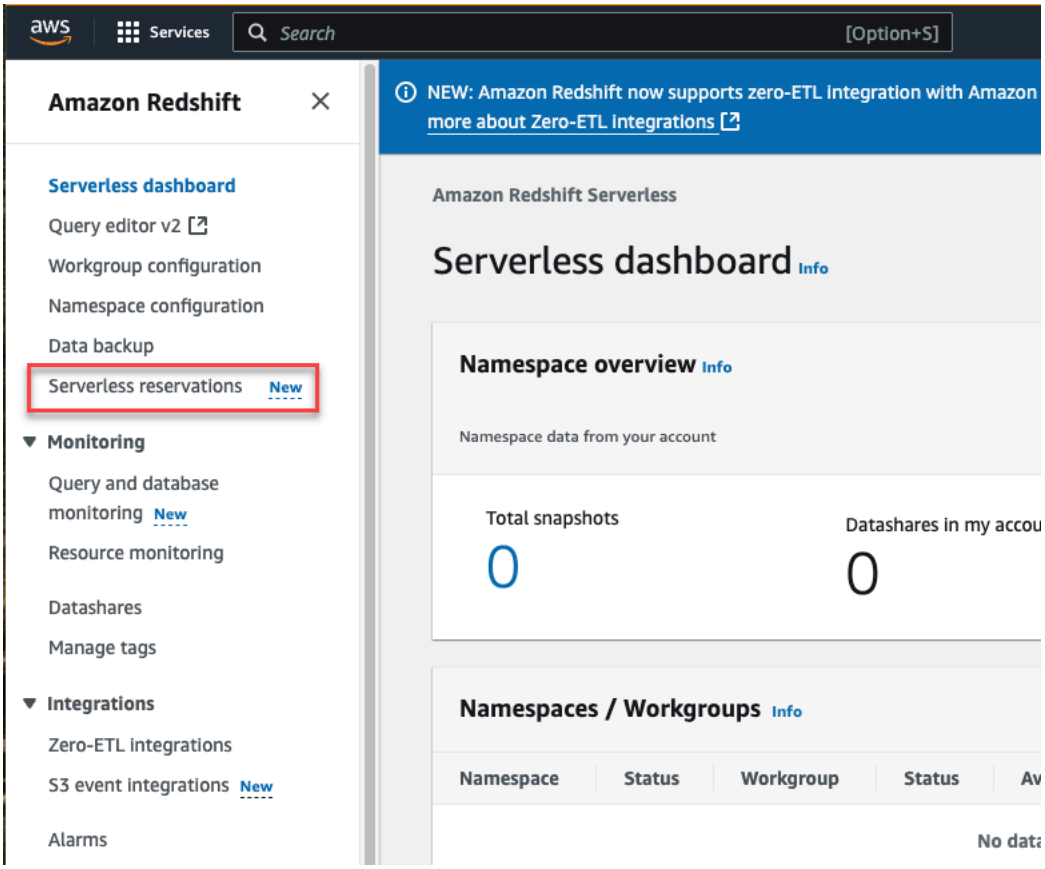
Méthode 2 : AWS Cost Explorer (Long-term analyse)

1. Connectez-vous à la console Cost Explorer Console de gestion AWS et ouvrez-la à l'adresse https://console.aws.amazon.com/costmanagement/.
2. Réglez la granularité sur Horaire
3. Regroupez par Type d’utilisation
4. Appliquez les filtres suivants :
   - Service : Redshift
   - Région : votre région locale
   - Type d'utilisation : Filtre pour Redshift:ServerlessUsage
5. Consultez le graphique des coûts et de l’utilisation pour l’utilisation horaire sans serveur dans la région que vous avez choisie

Acheter une réservation sans serveur à l’aide de la console

Lorsque vous achetez une réservation, vous choisissez le niveau de RPU qui sera remisé. Avant de sélectionner votre niveau de RPU, il est préférable de connaître votre capacité de base et la capacité à la demande que vous utilisez au fil du temps. Cette section explique comment déterminer votre capacité et réserver une réservation sans serveur.

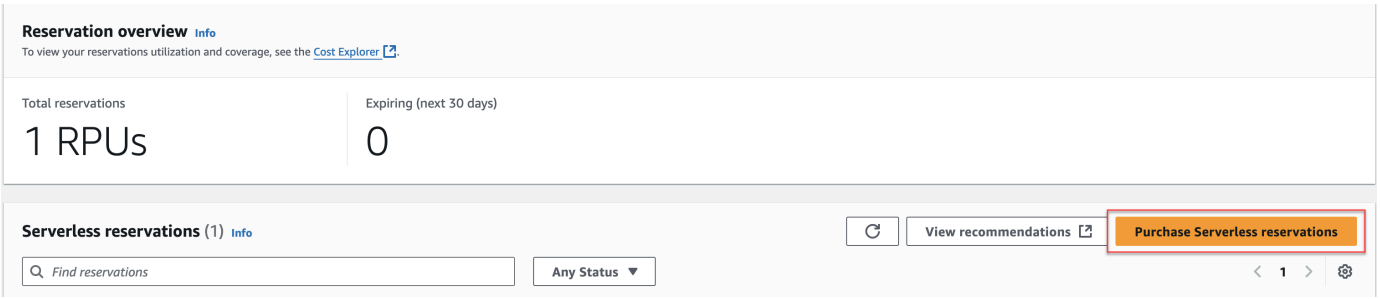
Pour commencer, dans la console Redshift, choisissez Sans serveur, puis Réservations sans serveur dans le menu.



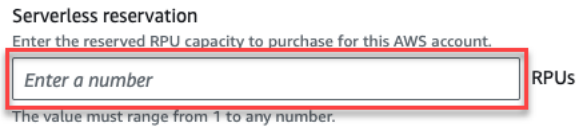
La console affiche une description de la fonctionnalité et une liste des réservations existantes. De là, vous pouvez acheter une réservation ou utiliser les rapports et les outils de surveillance disponibles pour vérifier votre consommation actuelle. Ils vous aident à déterminer vos niveaux de RPU et le nombre de RPU qu'il convient de réserver.

Pour acheter une réservation, procédez comme suit :

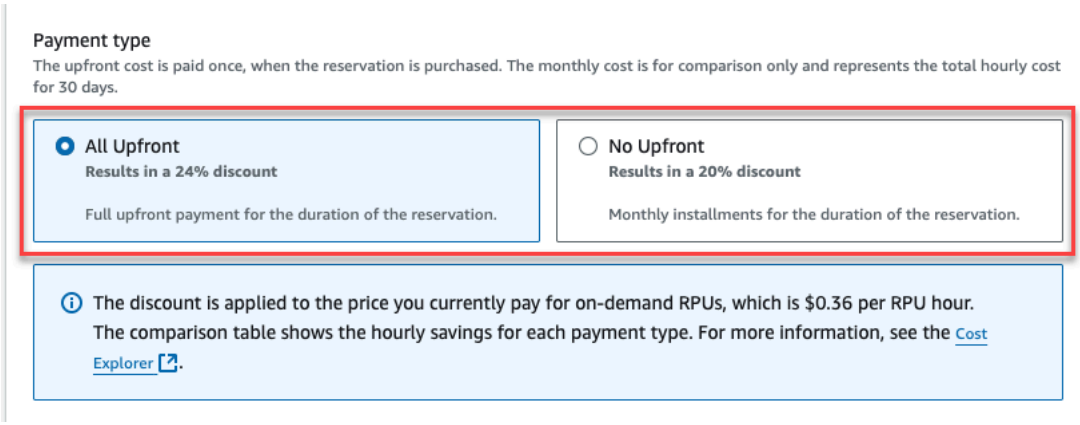
1. Choisissez Acheter des réservations sans serveur.



2. Une visite guidée contenant une série de sélections apparaît. Entrez le niveau de RPU de réservation sans serveur à réserver. Si vous ne savez pas quel doit être ce niveau, vous pouvez utiliser les outils décrits plus loin dans cette section.

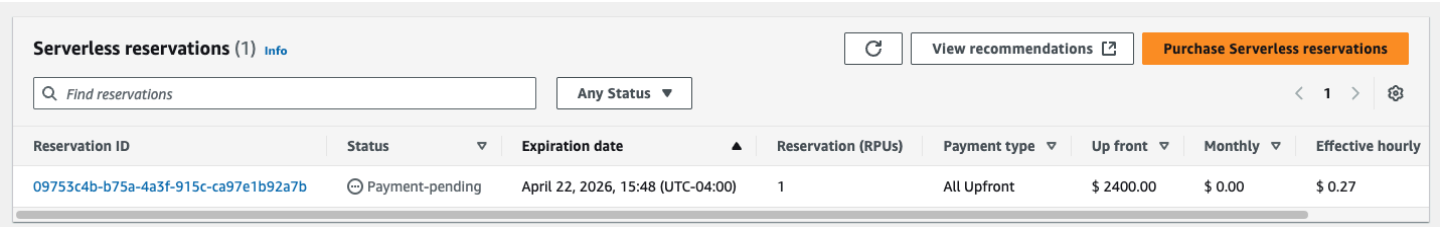


3. Définissez le type de paiement. Vous pouvez choisir de payer d'avance pour vos RPU réservés ou de payer mensuellement. Si vous choisissez de payer d'avance, vous bénéficiez d'une réduction plus importante.



4. Lorsque vous avez terminé vos sélections, choisissez Acheter des réservations sans serveur, puis Confirmer.

Une fois que vous avez confirmé la réservation, elle apparaît dans la liste des réservations.



Notes d'utilisation

- Vous ne pouvez pas modifier ni supprimer une réservation. Mais vous pouvez créer des réservations supplémentaires pour bénéficier d'une meilleure couverture.
- Redshift sans serveur utilise des RPU réservées pour une charge de travail avant d'utiliser des RPU à la demande, afin de garantir des économies de coûts. Si vous dépassez le nombre de RPU que vous avez réservées, vous commencez à accumuler les frais pour ces RPU supplémentaires au tarif à la demande de Redshift sans serveur.

- Les crédits gratuits pour Amazon Redshift sans serveur ne sont pas appliqués aux réservations sans serveur, mais uniquement aux RPU facturées à la demande.

Exemples de réservation sans serveur

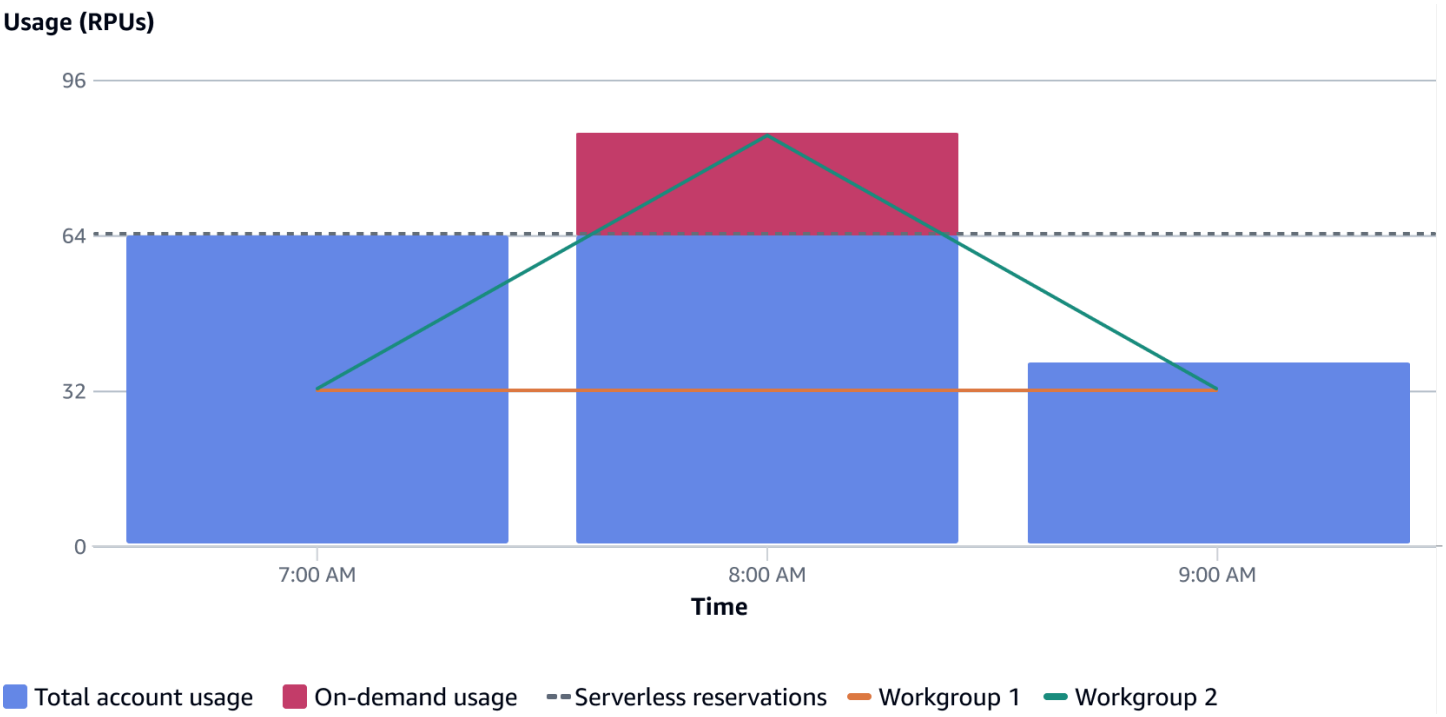
Dans ce scénario, votre AWS payeur/compte lié possède deux groupes de travail Amazon Redshift :

- Le groupe de travail 1 a un état d'utilisation stable, par exemple pour une équipe de veille commerciale.
- Le groupe de travail 2 a des charges de travail imprévisibles avec des pics d'utilisation, par exemple pour les opérations ETL.

Vous souhaitez optimiser les coûts de ces groupes de travail, c'est pourquoi vous achetez une réservation sans serveur d'un an. Sur la base des données historiques, vous déterminez que les deux groupes de travail consomment 64 RPU à un état stable. Cependant, le groupe de travail 2 passe parfois de 32 RPU à 48 RPU et chute à 24 RPU pendant de courtes périodes. Vous définissez le niveau de RPU de votre réservation à 64 RPU pour commencer, conformément aux tendances historiques. Les détails de facturation par heure sont les suivants :

- Pendant la première heure, comme dans le cas des tendances d'utilisation historiques, les deux groupes de travail utilisent 32 RPU pour une utilisation totale du compte de 64 RPU. Pour cette heure, toutes les RPU sont facturées au tarif réduit pour les réservations sans serveur. Cela est dû au fait que le niveau d'utilisation de 64 RPU est égal à la réservation sans serveur de 64 RPU.
- Pendant la deuxième heure, le groupe de travail 1 continue d'utiliser 32 RPU. Cependant, le groupe de travail 2 atteint 48 RPU, pour une utilisation totale du compte de 80 RPU. Pour cette heure, 64 RPU sont facturées au tarif réduit pour les réservations sans serveur, et 16 RPU sont facturées au tarif Redshift sans serveur à la demande.
- Pendant la troisième heure, le groupe de travail 1 continue de consommer 32 RPU et le groupe de travail 2 diminue à 8 RPU. Pendant cette heure, le compte est débité au tarif de réservation sans serveur de 64 RPU, même si le total du compte est de 40 RPU.

Consultez le schéma suivant pour connaître l'évolution de l'utilisation des groupes de travail et les détails de facturation des tarifs de réservation à la demande et sans serveur :



Acheter une réservation sans serveur à l'aide du AWS CLI ou API Amazon Redshift

Vous utilisez `create-reservation` pour créer une réservation RPU. La commande est illustrée ci-dessous.

```
create-reservation
--capacity
--offering-id
```

Vous définissez `capacity` sur le nombre de RPU que vous souhaitez réserver.

Facturation pour stockage

La capacité de stockage principale est facturée en tant que stockage géré Redshift (RMS). Le stockage est facturé par Go / mois. Le stockage et la capacité de calcul font l'objet d'une facturation distincte. Le stockage utilisé pour les instantanés manuels est facturé sur la base du nombre total de blocs de données uniques pour tous les instantanés manuels actifs aux taux de facturation des sauvegardes standard. Les points de récupération conservés pendant moins de 24 heures ne sont pas facturés.

Les coûts de transfert de données et de machine learning (ML) s'appliquent séparément, de la même manière que les clusters alloués. La réplication de snapshots et le partage de données entre

les AWS régions sont facturés aux taux de transfert indiqués sur la page de tarification. Pour plus d'informations, consultez Tarification d'Amazon Redshift.

Visualisation de l'utilisation de la facturation avec CloudWatch

La métrique`ServerlessUniqueSnapshotStorage`, qui suit l'utilisation du stockage des instantanés, est générée et envoyée à CloudWatch. Pour plus d'informations CloudWatch, consultez Qu'est-ce qu'Amazon CloudWatch ?

Utilisation de l'essai gratuit d'Amazon Redshift sans serveur

Amazon Redshift sans serveur propose un essai gratuit. Si vous participez à l'essai gratuit, vous pouvez voir le solde du crédit de l'essai gratuit dans la console Redshift et vérifier l'utilisation de l'essai gratuit dans la vue système SYS_SERVERLESS_USAGE. Notez que les détails de facturation pour l'utilisation de l'essai gratuit n'apparaissent pas dans la console de facturation. Vous ne pouvez visualiser l'utilisation dans la console de facturation qu'après la fin de la période d'essai gratuite. Pour en savoir plus sur l'essai gratuit d'Amazon Redshift sans serveur, consultez Essai gratuit d'Amazon Redshift sans serveur.

Notes d'utilisation de facturation

- Utilisation de l'enregistrement : une requête ou une transaction n'est mesurée et enregistrée qu'une fois la transaction terminée, annulée ou arrêtée. Par exemple, si une transaction s'exécute pendant deux jours, l'utilisation des RPU est enregistrée une fois que cette transaction est terminée. Vous pouvez surveiller l'utilisation continue en temps réel en interrogeant `sys_serverless_usage`. L'enregistrement des transactions peut refléter une variation d'utilisation des RPU et affecter les coûts pour des heures spécifiques et pour une utilisation quotidienne.
- Rédaction de transactions explicites : il est important de respecter la bonne pratique consistant à mettre fin aux transactions. Si vous ne mettez pas fin ou si vous n'annulez pas une transaction ouverte, Amazon Redshift sans serveur continue d'utiliser des RPU. Par exemple, si vous écrivez un texte `BEGIN TRAN` explicite, il est important d'avoir des instructions `COMMIT` et `ROLLBACK`correspondantes.
- Requêtes annulées : si vous exécutez une requête et que vous l'annulez avant la fin de son exécution, vous êtes toujours facturé pour la durée de l'exécution de la requête.
- Scaling (Mise à l'échelle) : l'instance Amazon Redshift sans serveur peut initier une mise à l'échelle pour gérer les périodes de charge plus élevée, afin de maintenir des performances cohérentes. Votre facturation Amazon Redshift sans serveur comprend à la fois le calcul de base et la capacité mise à l'échelle au même taux de RPU.

- Scaling down (Réduction de l’échelle) : Amazon Redshift sans serveur augmente sa capacité RPU de base pour gérer les périodes de charge plus élevée. Dans certains cas, la capacité de la RPU peut rester à un niveau plus élevé pendant un certain temps après la baisse de la charge des requêtes. Nous vous recommandons de définir le nombre maximum d’heures RPU dans la console afin de vous prémunir contre les coûts inattendus.
- Tables système : lorsque vous interrogez une table système, la durée de requête est facturée.
- Redshift Spectrum : lorsque vous utilisez Amazon Redshift sans serveur et que vous exécutez des requêtes, il n’y a pas de frais distincts pour les requêtes liées à un lac de données. Pour les requêtes sur des données stockées dans Amazon S3, les frais sont identiques, par temps de transaction, comme les requêtes sur des données locales.
- Requêtes fédérées : les requêtes fédérées sont facturées en termes de RPU utilisées sur un intervalle de temps spécifique, de la même manière que les requêtes sur l’entrepôt des données ou le lac de données.
- Stockage : le stockage est facturé séparément, par Go / mois.
- Forfait minimum : le tarif minimum est fixé à 60 secondes d’utilisation des ressources, facturées à la seconde.
- Facturation d’instantané : la facturation d’instantané ne change pas. Il est facturé en fonction du stockage, sur la base d’un tarif de Go / mois. Vous pouvez restaurer gratuitement votre entrepôt des données à des points spécifiques au cours des dernières 24 heures à une granularité de 30 minutes. Pour plus d’informations, consultez Tarification d’Amazon Redshift.
- Optimisations automatiques exécutées à l'aide de ressources de calcul supplémentaires - Amazon Redshift Serverless exécute généralement des opérations d'optimisation automatiques parallèlement aux requêtes des utilisateurs. Ces opérations sont appelées autonomes, et elles ne vous sont pas facturées.

  Si vous activez l'allocation de ressources informatiques supplémentaires, Amazon Redshift exécutera des systèmes autonomes si nécessaire, même en période de forte activité des utilisateurs. Dans de tels cas, le temps passé à utiliser des systèmes autonomes peut vous être facturé. Pour plus d'informations, consultez la section Allocation de ressources de calcul supplémentaires pour l'optimisation automatique des bases de données dans le manuel Amazon Redshift Database Developer Guide.

Les bonnes pratiques d'Amazon Redshift sans serveur pour une facturation prévisible

Vous trouverez ci-dessous les bonnes pratiques ainsi que les paramètres intégrés qui permettent d'assurer la cohérence de votre facturation.

- Veillez à mettre fin à chaque transaction. Lorsque vous utilisez `BEGIN` pour commencer une transaction, il est important d'y mettre fin (`END`) également.
- Suivez les bonnes pratiques en matière de gestion des erreurs pour répondre convenablement aux erreurs et mettre fin à chaque transaction. Le fait de minimiser le nombre de transactions ouvertes permet d'éviter l'utilisation inutile de RPU.
- Utilisez `SESSION TIMEOUT` pour mettre fin aux transactions ouvertes et aux sessions inactives. Ce paramètre fait expirer toute session restée inactive pendant plus de 3 600 secondes (1 heure). Il fait expirer toute transaction restée ouverte et inactive pendant plus de 21 600 secondes (6 heures). Ce paramètre de délai peut être modifié explicitement pour un utilisateur spécifique, par exemple lorsque vous souhaitez maintenir une session ouverte pour une requête de longue durée. La rubrique CREATE USER (CRÉER UN UTILISATEUR) montre comment adapter `SESSION TIMEOUT` à un utilisateur.
  - Dans la plupart des cas, nous vous recommandons de ne pas allonger la valeur `SESSION TIMEOUT`, sauf si vous avez un cas d'utilisation qui le requiert spécifiquement. Si la session reste inactive, avec une transaction ouverte, il peut en résulter un cas où les RPU sont utilisées jusqu'à ce que la session soit fermée. Cela entraînera des coûts inutiles.
  - Amazon Redshift sans serveur dispose d'une durée maximale de 86 399 secondes (24 heures) pour une requête en cours d'exécution. La période maximale d'inactivité pour une transaction ouverte est de six heures avant qu'Amazon Redshift sans serveur ne mette fin à la session associée à la transaction. Pour plus d'informations, consultez Quotas pour les objets Amazon Redshift sans serveur.

Amazon Redshift sans serveur avec regroupement des connexions

Amazon Redshift sans serveur traite toutes les requêtes entrantes comme des activités facturables des utilisateurs, y compris les requêtes légères de surveillance de l'état envoyées par des groupes de connexions. Ce comportement s'applique indépendamment du fait que la requête provient d'une application, d'un JDBC/ODBC pilote ou d'un framework de regroupement de connexions. Chaque requête de surveillance de l'état déclenche l'utilisation du calcul, et des frais sont facturés quel que soit le but ou l'origine de la requête. Par conséquent, le maintien de groupes de connexions

ouverts peut générer des coûts même lorsqu'aucune charge de travail utilisateur réelle n'est en cours d'exécution.

Le regroupement de connexions gère un groupe de connexions persistantes entre les applications et le point de terminaison Amazon Redshift sans serveur. Pour garantir que ces connexions restent saines et disponibles, les mécanismes de regroupement envoient souvent des requêtes légères ou vides (par exemple, `SELECT 1`) à intervalles réguliers. Ces requêtes automatisées vérifient l'état de la connexion.

Lorsque vous utilisez le regroupement de connexions, tenez compte des bonnes pratiques suivantes afin de minimiser les frais imprévus :

- Ajustez la fréquence des surveillances de l'état en passant en revue et en optimisant la fréquence des requêtes de surveillance de l'état ou de conservation dans votre configuration de regroupement de connexions.
- Optimisez les paramètres du système inactif en configurant le regroupement des connexions afin de minimiser les pertes de connexion inutiles ou les requêtes en arrière-plan pendant les périodes d'inactivité du système.
- Mettez en œuvre le regroupement au niveau des applications ou une meilleure gestion du cycle de vie des connexions si cela peut réduire les frais généraux.
- Désactivez les requêtes de pulsation ou de validation si votre configuration de regroupement de connexions le permet. Vérifiez les paramètres de votre chaîne de connexion ou vos fichiers de configuration spécifiques pour ajuster ces paramètres.
- Fine-tune Paramètres TCP keepalive : si vous ne pouvez pas désactiver les mécanismes internes du rythme cardiaque du pilote, ajustez les paramètres TCP (Transmission Control Protocol) keepalive au niveau du système d'exploitation ou de l'application pour résoudre les problèmes de délai de connexion. Reportez-vous à la documentation de votre système d'exploitation, de votre JDBC/ODBC pilote ou de votre pool de connexions pour plus de détails.
- Optimisez le regroupement des connexions aux bases de données : configurez votre groupe de connexions (HikariCP, Apache Database Connection Pool) pour gérer les connexions et minimiser les frais de connexion. Concentrez-vous sur des paramètres tels que le nombre maximal de connexions, le délai d'inactivité et les requêtes de validation (si nécessaire). Cette optimisation permet d'aligner l'utilisation du calcul d'Amazon Redshift sans serveur sur la demande de charge de travail réelle, ce qui peut réduire les coûts.

Optimisation des coûts pour Amazon Redshift sans serveur zéro ETL

Pour optimiser les coûts lors de l'exécution d'intégrations zéro ETL sur Amazon Redshift sans serveur, vous pouvez dimensionner correctement vos environnements et ajuster vos paramètres d'actualisation en fonction des besoins de charge de travail. Pensez à effectuer les ajustements suivants :

- Utilisez la capacité RPU de base inférieure de 8 RPU lorsqu'elle est disponible pour les charges de travail.
- Configurez le REFRESH_INTERVAL de votre instance Redshift cible pour équilibrer actualisation et coût. Des intervalles plus courts garantissent des mises à jour en temps quasi réel, mais augmentent les coûts de calcul. Des intervalles plus longs (5 minutes ou plus) réduisent les frais liés aux charges de travail pour lesquelles l'actualisation immédiate n'est pas essentielle, comme les rapports ou les analyses historiques. Pour modifier votre REFRESH_INTERVAL Redshift cible, consultez la clause d'intervalle d'actualisation dans la description d'ALTER DATABASE.
- Optimisez l'utilisation de votre environnement Amazon Redshift sans serveur en exécutant simultanément des charges de travail d'analyse alors que des données zéro ETL sont ingérées. Cela garantit que la capacité de calcul répond activement à de multiples objectifs commerciaux.

Connexion à Amazon Redshift sans serveur

Une fois que vous avez configuré votre instance Amazon Redshift sans serveur, vous pouvez vous y connecter selon différentes méthodes, décrites ci-dessous. Si vous avez plusieurs équipes ou projets et que vous souhaitez gérer les coûts séparément, vous pouvez utiliser des Comptes AWS distincts.

Pour obtenir la liste des Régions AWS endroits où Amazon Redshift Serverless est disponible, consultez les points de terminaison répertoriés pour l'API Redshift Serverless dans le. Référence générale d'Amazon Web Services

Amazon Redshift Serverless se connecte à l'environnement sans serveur de votre Compte AWS environnement actuel. Région AWS Amazon Redshift sans serveur s'exécute dans un VPC au sein des plages de ports 5431-5455 et 8191-8215. La valeur par défaut est 5439. Actuellement, vous ne pouvez modifier les ports qu'à l'aide de l'opération API `UpdateWorkgroup` et de l' AWS CLI opération`update-workgroup`.

Connexion à Amazon Redshift sans serveur

Vous pouvez vous connecter à une base de données (nommée dev) dans Amazon Redshift sans serveur avec la syntaxe suivante.

```
workgroup-name.account-number.aws-region.redshift-serverless.amazonaws.com:port/dev
```

Par exemple, la chaîne de connexion suivante spécifie la région us-east-1.

```
default.123456789012.us-east-1.redshift-serverless.amazonaws.com:5439/dev
```

Connexion à Amazon Redshift sans serveur via des pilotes JDBC

Vous pouvez utiliser l'une des méthodes suivantes pour vous connecter à Amazon Redshift Serverless avec votre client SQL préféré à l'aide du pilote Amazon Redshift-provided JDBC version 2.x.

Pour se connecter avec des informations d'identification pour l'authentification de la base de données en utilisant le pilote JDBC version 2.x, utilisez la syntaxe suivante. Le numéro de port est facultatif. S'il n'est pas inclus, Amazon Redshift sans serveur utilise par défaut le numéro de port 5439. Vous pouvez passer à un autre port dans la plage de ports 5431-5455 ou 8191-8215. Pour modifier le port par défaut d'un point de terminaison sans serveur, utilisez l' AWS CLI API Amazon Redshift.

```
jdbc:redshift://workgroup-name.account-number.aws-region.redshift-
serverless.amazonaws.com:5439/dev
```

Par exemple, la chaîne de connexion suivante spécifie l'ID de compte 123456789012 dans la région us-east-2.

```
jdbc:redshift://default.123456789012.us-east-2.redshift-serverless.amazonaws.com:5439/
dev
```

Pour vous connecter à IAM à l'aide du pilote JDBC version 2.x, utilisez la syntaxe suivante. Le numéro de port est facultatif. S'il n'est pas inclus, Amazon Redshift sans serveur utilise par défaut le numéro de port 5439. Vous pouvez passer à un autre port dans la plage de ports 5431-5455 ou 8191-8215. Pour modifier le port par défaut d'un point de terminaison sans serveur, utilisez l' AWS CLI API Amazon Redshift.

```
jdbc:redshift:iam://workgroup-name.account-number.aws-region.redshift-
serverless.amazonaws.com:5439/dev
```

Par exemple, la chaîne de connexion suivante spécifie l'ID de compte 123456789012 dans la région us-east-2.

```
jdbc:redshift:iam://default.123456789012.us-east-2.redshift-
serverless.amazonaws.com:5439/dev
```

Pour ODBC, utilisez la syntaxe suivante.

```
Driver={Amazon Redshift (x64)}; Server=workgroup-name.account-number.aws-
region.redshift-serverless.amazonaws.com; Database=dev
```

Si vous utilisez une version du pilote JDBC antérieure à 2.1.0.9 et que vous vous connectez avec IAM, vous devrez utiliser la syntaxe suivante.

```
jdbc:redshift:iam://redshift-serverless-<name>:aws-region/database-name
```

Par exemple, la chaîne de connexion suivante spécifie la valeur par défaut du groupe de travail et la valeur Région AWS us-east-1.

```
jdbc:redshift:iam://redshift-serverless-default:us-east-1/dev
```

Pour plus d'informations sur les pilotes, consultez Configuration des connexions dans Amazon Redshift.

Trouver votre chaîne de connexion JDBC et ODBC

Pour vous connecter à votre groupe de travail avec votre outil client SQL, vous devez disposer de la chaîne de connexion JDBC ou ODBC. Vous pouvez trouver la chaîne de connexion dans la console Amazon Redshift sans serveur, sur la page des détails d'un groupe de travail.

Pour trouver la chaîne de connexion d'un groupe de travail

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Redshift sans serveur.

3. Dans le menu de navigation, choisissez Configuration du groupe de travail, puis sélectionnez le nom du groupe de travail dans la liste pour ouvrir ses détails.
4. Les chaînes de connexion JDBC URL et ODBC URL sont disponibles, ainsi que des détails supplémentaires dans la section Informations générales. Chaque chaîne est basée sur la AWS région dans laquelle s'exécute le groupe de travail. Cliquez sur l'icône en regard de la chaîne de connexion appropriée pour la copier.

Connexion à Amazon Redshift sans serveur avec l'API de données

Vous pouvez également utiliser l'API de données Amazon Redshift pour vous connecter à Amazon Redshift sans serveur. Utilisez le `workgroup-name` paramètre à la place du `cluster-identifier` paramètre dans vos AWS CLI appels.

Pour plus d'informations sur l'API de données, consultez Utilisation de l'API de données Amazon Redshift. Pour obtenir des exemples de code appelant l'API Data en Python et d'autres exemples, consultez la section Getting Started with Redshift Data API et consultez les `use-cases` dossiers `quick-start` et de GitHub.

Se connecter avec SSL à Amazon Redshift sans serveur

Configuration d'une connexion sécurisée à Amazon Redshift sans serveur

Pour prendre en charge les connexions SSL, Redshift sans serveur crée et installe un certificat SSL émis par AWS Certificate Manager (ACM) sur chaque groupe de travail. Les certificats ACM sont publiquement approuvés par la plupart des systèmes d'exploitation, des navigateurs web et des clients. Vous pourriez devoir télécharger une solution groupée de certificats si vos clients ou applications SQL se connectent à Redshift sans serveur en utilisant SSL avec l'option de connexion `sslmode` définie sur `require`, `verify-ca` ou `verify-full`. Si votre client a besoin d'un certificat, Redshift sans serveur fournit un certificat de solution groupée comme suit :

- Téléchargez le bundle depuis https://s3.amazonaws.com/redshift-downloads/amazon-trust-ca-bundle.crt.
  - Le numéro de total de contrôle MD5 prévu est 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - Le numéro de total de contrôle sha256 est 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

  N'utilisez pas la solution groupée de certificats précédente qui se trouvait à l'adresse `https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt`.

- En Chine Région AWS, téléchargez le bundle depuis https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt.
  - Le numéro de total de contrôle MD5 prévu est 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - Le numéro de total de contrôle sha256 est 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

  N'utilisez pas les solutions groupées de certificats antérieures qui se trouvait à l'adresse `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt` et `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem`.

> **Important**
>
> Redshift sans serveur a changé la méthode de gestion des certificats SSL. Il se peut que vous ayez besoin de mettre à jour vos certificats CA actuels racine approuvés pour pouvoir continuer à vous connecter à vos groupes de travail à l'aide du protocole SSL. Pour de plus amples informations sur les certificats ACM pour les connexions SSL, consultez Transition vers les certificats ACM pour les connexions SSL.

Par défaut, les bases de données du groupe de travail acceptent une connexion qu'elle s'appuie sur le protocole SSL ou non.

Pour créer un nouveau groupe de travail qui accepte uniquement les connexions SSL, utilisez la commande `create-workgroup` et définissez le paramètre `require_ssl` sur `true`. Pour utiliser l'exemple suivant, remplacez *`yourNamespaceName`* par le nom de votre espace de noms et remplacez-le *`yourWorkgroupName`* par le nom de votre groupe de travail.

```
aws redshift-serverless create-workgroup \
--namespace-name yourNamespaceName \
--workgroup-name yourWorkgroupName \
--config-parameters parameterKey=require_ssl,parameterValue=true
```

Pour mettre à jour un groupe de travail existant afin qu'il n'accepte que les connexions SSL, utilisez la commande `update-workgroup` et définissez le paramètre `require_ssl` sur `true`. Notez que Redshift sans serveur redémarrera votre groupe de travail lorsque vous mettrez à jour le paramètre

`require_ssl`. Pour utiliser l'exemple suivant, remplacez *yourWorkgroupName* par le nom de votre groupe de travail.

```
aws redshift-serverless update-workgroup \
--workgroup-name yourWorkgroupName \
--config-parameters parameterKey=require_ssl,parameterValue=true
```

Amazon Redshift prend en charge le protocole d'accord de clé Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). Avec le protocole ECDHE, le client et le serveur disposent chacun d'une paire de clés publiques-privées à courbes elliptiques qui permettent d'établir un secret partagé via un canal non sécurisé. Vous n'avez pas besoin de configurer quoi que ce soit dans Amazon Redshift pour activer ECDHE. Si vous vous connectez à partir d'un outil client SQL qui utilise le protocole ECDHE pour chiffrer les communications entre le client et le serveur, Amazon Redshift utilise la liste de chiffrement fournie pour établir les connexions appropriées. Pour plus d'informations, consultez Elliptic curve diffie—hellman sur Wikipedia et Ciphers sur le site d'OpenSSL.

Configuration d'une connexion FIPS-compliant SSL à Amazon Redshift Serverless

Pour créer un nouveau groupe de travail utilisant une connexion FIPS-compliant SSL, utilisez la `create-workgroup` commande et définissez les `require_ssl` paramètres `use_fips_ssl` et sur`true`. Pour utiliser l'exemple suivant, remplacez *yourNamespaceName* par le nom de votre espace de noms et remplacez-le *yourWorkgroupName* par le nom de votre groupe de travail.

```
aws redshift-serverless create-workgroup \
--namespace-name yourNamespaceName \
--workgroup-name yourWorkgroupName \
--config-parameters '[{"parameterKey": "require_ssl", "parameterValue": "true"},
 {"parameterKey": "use_fips_ssl", "parameterValue": "true"}]'
```

Pour mettre à jour un groupe de travail existant afin qu'il utilise une connexion FIPS-compliant SSL, utilisez la `update-workgroup` commande et définissez les `require_ssl` paramètres `use_fips_ssl` et sur`true`. Notez que Redshift sans serveur redémarrera votre groupe de travail lorsque vous mettrez à jour le paramètre `use_fips_ssl`. Pour utiliser l'exemple suivant, remplacez *yourWorkgroupName* par le nom de votre groupe de travail.

```
aws redshift-serverless update-workgroup \
--workgroup-name yourWorkgroupName \
--config-parameters '[{"parameterKey": "require_ssl", "parameterValue": "true"},
 {"parameterKey": "use_fips_ssl", "parameterValue": "true"}]'
```

Pour plus d'informations sur la configuration de Redshift Serverless pour utiliser des FIPS-compliant connexions, consultez use_fips_ssl dans le manuel Amazon Redshift Database Developer Guide.

Connexion à Amazon Redshift sans serveur à partir d’un point de terminaison de VPC géré par Amazon Redshift

Connexion à Amazon Redshift sans serveur depuis d’autres points de terminaison d’un VPC

Pour plus d'informations sur la configuration ou la configuration d'un point de terminaison VPC géré pour un groupe de travail Amazon Redshift Serverless, consultez la section Utilisation des points de terminaison VPC. Redshift-managed

Connexion à Amazon Redshift Serverless depuis un point de terminaison VPC d'interface (AWS PrivateLink)

Pour en savoir plus la connexion à Amazon Redshift sans serveur à partir d’un point de terminaison d’un VPC d’interface (AWS PrivateLink), consultez Points de terminaison de VPC d’Interface.

Connexion à Amazon Redshift sans serveur à partir d’un point de terminaison d’un VPC Redshift dans un autre compte

Connexion à Amazon Redshift sans serveur à partir d’un point de terminaison entre VPC

Amazon Redshift sans serveur est mis en service dans un VPC. Vous pouvez accorder l’accès à un VPC dans un autre compte pour accéder à Amazon Redshift sans serveur sur votre compte. Cela ressemble à une connexion depuis un point de terminaison de VPC géré, mais dans ce cas, la connexion provient, par exemple, d’un client de base de données dans un autre compte. Vous pouvez effectuer quelques opérations :

- Le propriétaire d’une base de données peut accorder l’accès à un VPC contenant Amazon Redshift sans serveur à un autre compte dans la même région.
- Le propriétaire d’une base de données peut révoquer l’accès à Amazon Redshift sans serveur.

Le principal avantage de l'accès intercompte est de faciliter la collaboration avec les bases de données. Les utilisateurs n'ont pas besoin d'être provisionnés dans le compte contenant la base de données pour y accéder, ce qui réduit les étapes de configuration et fait gagner du temps.

Autorisations requises pour accorder l'accès à un VPC dans un autre compte

Pour accorder l'accès ou modifier l'accès autorisé, le concédant a besoin d'une politique d'autorisations assignée avec les autorisations suivantes :

- redshift sans serveur : PutResourcePolicy
- redshift sans serveur : GetResourcePolicy
- redshift sans serveur : DeleteResourcePolicy
- EC2 : CreateVpcEndpoint
- EC2 : ModifyVpcEndpoint

Vous pourriez avoir besoin d'autres autorisations spécifiées dans la politique AWS gérée AmazonRedshiftFullAccess. Pour plus d'informations, consultez Octroi d'autorisations à Amazon Redshift sans serveur.

Le bénéficiaire a besoin d'une politique d'autorisations assignée avec les autorisations suivantes :

- redshift sans serveur : ListWorkgroups
- redshift sans serveur : CreateEndpointAccess
- redshift sans serveur : UpdateEndpointAccess
- redshift sans serveur : GetEndpointAccess
- redshift sans serveur : ListEndpointAccess
- redshift sans serveur : DeleteEndpointAccess

Il est recommandé d'associer des politiques d'autorisation à un rôle IAM, puis de l'attribuer à des utilisateurs et à des groupes, le cas échéant. Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift.

Voici un exemple de politique de ressources utilisé pour configurer l'accès entre VPC :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccountCrossVPCAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "123456789012",
                    "234567890123"
                ]
            },
            "Action": [
                "redshift-serverless:CreateEndpointAccess",
                "redshift-serverless:UpdateEndpointAccess",
                "redshift-serverless:DeleteEndpointAccess",
                "redshift-serverless:GetEndpointAccess"
            ],
            "Resource": "arn:aws:redshift-serverless:*:*:*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": "us-east-1"
                },
                "StringLike": {
                    "aws:SourceVpc": [
                       "vpc-11223344556677889",
                       "vpc-12345678"
                    ]
                }
            }
        }
    ]
}
```

Les procédures décrites dans cette section supposent que l'utilisateur qui les exécute dispose des autorisations appropriées, par exemple au moyen d'un rôle IAM attribué dont les autorisations sont répertoriées. Les procédures supposent également que le groupe de travail possède un rôle IAM attaché avec les autorisations de ressources appropriées.

Octroi d’un accès VPC à d’autres comptes, à l’aide de la console

Cette procédure indique les étapes à suivre pour configurer l’accès à la base de données lorsque vous êtes le propriétaire de la base de données et que vous souhaitez autoriser l’accès à celle-ci.

Octroi d’accès depuis le compte du propriétaire

1. Dans les propriétés du groupe de travail Amazon Redshift sans serveur, dans l’onglet Accès aux données, figure une liste appelée Comptes accordés. Elle indique les comptes et les VPC autorisés à accéder au groupe de travail. Recherchez la liste et choisissez Accorder l’accès pour ajouter un compte à la liste.
2. Une fenêtre apparaît dans laquelle vous pouvez ajouter les informations du bénéficiaire. Entrez l’ID du compte AWS , qui représente l’ID à 12 chiffres du compte auquel vous souhaitez accorder l’accès.
3. Accordez au bénéficiaire l’accès à tous les VPC ou à des VPC spécifiques. Si vous accordez l’accès uniquement à des VPC spécifiques, vous pouvez ajouter les identifiants correspondants en entrant chacun d’eux et en choisissant Ajouter un VPC.
4. Enregistrez les modifications lorsque vous avez terminé.

Lorsque vous enregistrez les modifications, le compte apparaît dans la liste Comptes accordés. L’entrée indique l’ID du compte et la liste des VPC autorisés à y accéder.

Le propriétaire de la base de données peut également révoquer l’accès à un compte. Le propriétaire peut révoquer l’accès à tout moment.

Révocation de l’accès à un compte

1. Vous pouvez commencer à partir de la liste des comptes accordés. Sélectionnez d’abord un ou plusieurs comptes.
2. Choisissez Révoquer l’accès.

Une fois l’accès accordé, un administrateur de base de données du bénéficiaire peut vérifier la console pour déterminer s’il y a accès.

Utilisation de la console pour confirmer que l’accès vous est accordé pour accéder à un autre compte

1. Dans les propriétés du groupe de travail Amazon Redshift sans serveur, sous l’onglet Accès aux données, se trouve une liste intitulée Comptes autorisés. Il montre les comptes accessibles

depuis ce groupe de travail. Le bénéficiaire ne peut pas utiliser l'URL du point de terminaison du groupe de travail pour accéder directement au groupe de travail. Pour accéder au groupe de travail, vous, en tant que bénéficiaire, accédez à la section point de terminaison et choisissez créer un point de terminaison.

2. Ensuite, en tant que bénéficiaire, vous fournissez un nom de point de terminaison et un VPC pour accéder au groupe de travail.
3. Une fois le point de terminaison créé avec succès, il apparaît dans la section point de terminaison et une URL de point de terminaison lui correspond. Vous pouvez utiliser cette URL de point de terminaison pour accéder au groupe de travail.

Octroi d'un accès à d'autres comptes à l'aide des commandes CLI

Le compte accordant l'accès doit d'abord accorder l'accès à un autre compte pour se connecter en utilisant `put-resource-policy`. Le propriétaire de la base de données peut appeler `put-resource-policy` pour autoriser un autre compte à créer des connexions au groupe de travail. Le compte bénéficiaire peut ensuite utiliser `create-endpoint-authorization` pour créer des connexions au groupe de travail via ses VPC autorisés.

Vous trouverez ci-dessous les propriétés pour `put-resource-policy`, que vous pouvez appeler pour autoriser l'accès à un compte et à un VPC spécifiques.

```
aws redshift-serverless put-resource-policy
--resource-arn <value>
--policy <value>
```

Après avoir appelé la commande, vous pouvez appeler `get-resource-policy`, en spécifiant l'élément `resource-arn` pour voir quels comptes et VPC sont autorisés à accéder à la ressource.

L'appel suivant peut être effectué par le bénéficiaire. Il affiche des informations sur l'accès accordé. Plus précisément, il renvoie une liste contenant les VPC auxquels l'accès est accordé.

```
aws redshift-serverless list-workgroups
--owner-account <value>
```

L'objectif est de permettre au bénéficiaire d'obtenir des informations sur les autorisations des points de terminaison auprès du compte qui les a accordées. L'élément `owner-account` est le compte de partage. Lorsque vous exécutez ce code, il renvoie `CrossAccountVpcs` pour chaque groupe de

travail, qui correspond à la liste des VPC autorisés. À titre de référence, voici toutes les propriétés disponibles pour un groupe de travail :

```
Output: workgroup (Object)
workgroupId String,
workgroupArn String,
workgroupName String,
status: String,
namespaceName: String,
baseCapacity: Integer, (Not-applicable)
enhancedVpcRouting: Boolean,
configParameters: List,
securityGroupIds: List,
subnetIds: List,
endpoint: String,
publiclyAccessible: Boolean,
creationDate: Timestamp,
port: Integer,
CrossAccountVpcs: List
```

> **Note**
>
> Pour rappel, la relocalisation du cluster n'est pas une condition préalable à la configuration de fonctionnalités de mise en réseau Redshift supplémentaires. Il n'est pas non plus obligatoire de l'activer pour activer les fonctionnalités suivantes :
>
> - Connexion à Redshift depuis un VPC multicompte ou interrégional : vous pouvez vous connecter d'un cloud privé AWS virtuel (VPC) à un autre contenant une base de données Redshift, comme décrit dans cette section.
> - Configuration d'un nom de domaine personnalisé : vous pouvez créer un nom de domaine personnalisé, également appelé URL personnalisée, pour votre cluster Amazon Redshift ou votre groupe de travail Amazon Redshift sans serveur, afin de rendre le nom du point de terminaison plus facile à mémoriser et plus simple. Pour plus d'informations, consultez Utilisation d'un nom de domaine personnalisé pour les connexions client.

Ressources supplémentaires

Les instructions pour configurer vos paramètres de trafic réseau sont disponibles dans Accessibilité publique avec une configuration de groupe de sécurité par défaut ou personnalisée. Cela inclut un cas d'utilisation où le cluster est accessible publiquement.

Les instructions pour configurer vos paramètres de trafic réseau sont disponibles dans Accessibilité privée avec une configuration de groupe de sécurité par défaut ou personnalisée. Cela inclut les cas d'utilisation où le cluster n'est pas disponible sur Internet.

Pour plus d'informations sur les connexions sécurisées à Amazon Redshift sans serveur, y compris l'octroi d'autorisations, l'autorisation d'accès à des services supplémentaires et la création de rôles IAM, consultez Identity and Access Management dans Amazon Redshift Serverless.

Définition des rôles de base de données à accorder aux utilisateurs fédérés dans Amazon Redshift sans serveur

Lorsque vous faites partie d'une organisation, vous avez un ensemble de rôles associés. Par exemple, vous avez des rôles liés à votre fonction, comme programmeur et responsable. Vos rôles déterminent les applications et les données auxquelles vous avez accès. La plupart des organisations utilisent un fournisseur d'identité, tel que Microsoft Active Directory, pour attribuer des rôles aux utilisateurs et aux groupes. L'utilisation des rôles pour contrôler l'accès aux ressources s'est développée, car les organisations n'ont plus à gérer autant d'utilisateurs individuels.

Récemment, le contrôle d'accès basé sur les rôles a été introduit dans Amazon Redshift sans serveur. Les rôles de base de données vous permettent de sécuriser l'accès aux données et aux objets, tels que les schémas ou les tables, par exemple. Vous pouvez également utiliser les rôles pour définir un ensemble d'autorisations élevées, par exemple pour un moniteur système ou un administrateur de base de données. Mais après avoir accordé des autorisations de ressources aux rôles de la base de données, il y a une étape supplémentaire qui consiste à connecter les rôles d'un utilisateur de l'organisation aux rôles de la base de données. Vous pouvez affecter chaque utilisateur à son rôle dans la base de données lors de la première connexion en exécutant des instructions SQL, mais cela demande beaucoup d'efforts. Un moyen plus simple consiste à définir les rôles de base de données à accorder et à les transmettre à Amazon Redshift sans serveur. Cela a l'avantage de simplifier la procédure d'inscription initiale.

Vous pouvez transmettre des rôles à Amazon Redshift sans serveur à l'aide de `GetCredentials`. Lorsqu'un utilisateur se connecte pour la première fois à une base de données Amazon Redshift sans

serveur, un utilisateur de base de données associé est créé et mappé aux rôles de base de données correspondants. Cette rubrique détaille le mécanisme de transmission des rôles à Amazon Redshift sans serveur.

La transmission des rôles de la base de données a deux utilisations principales :

- Lorsqu'un utilisateur se connecte par l'intermédiaire d'un fournisseur d'identité tiers, généralement avec une fédération configurée, et transmet les rôles au moyen d'une balise de session.
- Lorsqu'un utilisateur s'identifie à l'aide des informations d'identification d'IAM, ses rôles sont transmis au moyen d'une clé et d'une valeur de balise.

Pour plus d'informations sur le contrôle d'accès basé sur les rôles, consultez la section Contrôle Role-based d'accès (RBAC).

Définition des rôles de base de données

Avant de pouvoir transmettre des rôles à Amazon Redshift sans serveur, vous devez configurer des rôles de base de données dans votre base de données et leur accorder les autorisations appropriées sur les ressources de la base de données. Par exemple, dans un scénario simple, vous pouvez créer un rôle de base de données appelé ventes et lui accorder l'accès aux tables de requêtes contenant des données sur les ventes. Pour plus d'informations sur la création de rôles de base de données et l'octroi d'autorisations, consultez CREATE ROLE et GRANT.

Cas d'utilisation pour définir les rôles de base de données à accorder aux utilisateurs fédérés

Ces sections présentent quelques cas d'utilisation où le fait de transmettre des rôles de base de données à Amazon Redshift sans serveur peut simplifier l'accès aux ressources de la base de données.

Connexion à l'aide d'un fournisseur d'identité

Le premier cas d'utilisation suppose que votre organisation dispose d'identités d'utilisateurs dans un service de gestion des identités et des accès. Ce service peut être basé sur le cloud, par exemple JumpCloud pour Okta, ou sur site, comme Microsoft Active Directory. L'objectif est de faire correspondre automatiquement les rôles d'un utilisateur du fournisseur d'identité aux rôles de votre base de données lorsqu'il se connecte à un client tel que l'éditeur de requête V2, par exemple, ou à

un client JDBC. Pour ce faire, vous devez effectuer quelques tâches de configuration. Cela inclut les éléments suivants :

1. Configurez l'intégration fédérée avec votre fournisseur d'identité (IdP) à l'aide d'une relation de confiance. Il s'agit d'un prérequis. Lorsque vous configurez cette option, le fournisseur d'identité est chargé d'authentifier l'utilisateur au moyen d'une assertion SAML et de fournir des informations d'identification de connexion. Pour plus d'informations, consultez la section Intégration de fournisseurs de solutions SAML tiers avec AWS. Vous trouverez également plus d'informations sur le blog Fédérer l'accès à Amazon Redshift Query Editor V2 avec Active Directory Federation Services (AD FS) ou Fédérer l'accès à authentification unique à Amazon Redshift Query Editor V2 avec Okta.
2. L'utilisateur doit disposer des autorisations suivantes en matière de politique :
   - `GetCredentials` : fournit des informations d'identification pour une autorisation temporaire de connexion à Amazon Redshift sans serveur.
   - `sts:AssumeRoleWithSAML`— Fournit un mécanisme permettant de lier un magasin d'identités ou un répertoire d'entreprise à un accès basé sur les rôles AWS .
   - `sts:TagSession` : autorisation pour l'action balise relative au principal du fournisseur d'identité.

   Dans ce cas, `AssumeRoleWithSAML` renvoie un ensemble d'informations d'identification de sécurité pour les utilisateurs qui ont été authentifiés via une réponse SAML authentifiée. Cette opération fournit un mécanisme permettant de lier une banque d'identités ou un répertoire à un AWS accès basé sur les rôles sans informations d'identification spécifiques à l'utilisateur. Pour les utilisateurs ayant l'autorisation à `AssumeRoleWithSAML`, le fournisseur d'identité est responsable de la gestion de l'assertion SAML utilisée pour transmettre les informations relatives au rôle.

   Il est recommandé d'associer des politiques d'autorisation à un rôle IAM, puis de l'attribuer à des utilisateurs et à des groupes, le cas échéant. Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift.
3. Vous configurez la balise `RedshiftDbRoles` avec les valeurs de rôle séparées par deux points, dans le format role1:role2. Par exemple, `manager:engineer`. Vous pouvez les récupérer à partir d'une mise en œuvre de balisage de session configurée dans votre fournisseur d'identité. La demande d'authentification SAML transmet les rôles par programmation. Pour plus d'informations sur la transmission des balises de session, consultez Transmission des balises de session dans AWS STS.

   Si vous transmettez un nom de rôle qui n'existe pas dans la base de données, il est ignoré.

Dans ce cas d'utilisation, lorsqu'un utilisateur se connecte à l'aide d'une identité fédérée, ses rôles sont transmis dans la demande d'autorisation par le biais de la clé et de la valeur de la balise de session. Ensuite, après autorisation, `GetCredentials` transmet les rôles à la base de données. Lorsque la connexion est établie, les rôles de la base de données sont mappés et l'utilisateur peut effectuer les tâches de la base de données correspondant à son rôle. L'essentiel de l'opération consiste à attribuer à la balise de la session `RedshiftDbRoles` les rôles prévus dans la demande d'autorisation initiale. Pour plus d'informations sur la transmission de balises de session, voir Transmettre des balises de session à l'aide de AssumeRoleWithSAML.

Connexion à l'aide des informations d'identification IAM

Dans le deuxième cas d'utilisation, des rôles peuvent être attribués à un utilisateur et celui-ci peut accéder à une application client de base de données par le biais d'informations d'identification IAM.

1. L'utilisateur qui se connecte dans ce cas doit se voir attribuer des autorisations de politique pour les actions suivantes :
   - `tag:GetResources` : renvoie les ressources balisées associées aux balises spécifiées.
   - `tag:GetTagKeys` : renvoie les balises en cours d'utilisation.

     Il est recommandé d'associer des politiques d'autorisation à un rôle IAM, puis de l'attribuer à des utilisateurs et à des groupes, le cas échéant. Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift.
2. Des autorisations sont également nécessaires pour accéder au service de base de données, comme Amazon Redshift sans serveur.
3. Pour ce cas d'utilisation, configurez les valeurs de balisage pour vos rôles dans Gestion des identités et des accès AWS. Vous pouvez choisir de modifier les balises et de créer une clé de balise appelée RedshiftDbRoles accompagnée d'une chaîne de valeur de balise contenant les rôles. Par exemple, manager:engineer.

Lorsqu'un utilisateur se connecte, son rôle est ajouté à la demande d'autorisation et transmis à la base de données. Il est mappé à un rôle de base de données existant.

Ressources supplémentaires

Comme indiqué dans les cas d'utilisation, vous pouvez configurer la relation de confiance entre votre IdP et AWS. Pour plus d'informations, consultez Configuration de votre IdP SAML 2.0 à l'aide d'une relation d'approbation des parties utilisatrices et ajout de demandes.

Identity and Access Management dans Amazon Redshift Serverless

L'accès à Amazon Redshift nécessite des informations d'identification qui AWS peuvent être utilisées pour authentifier vos demandes. Ces informations d'identification doivent être autorisées à accéder à AWS des ressources, telles qu'Amazon Redshift Serverless.

Les sections suivantes fournissent des informations sur la manière dont vous pouvez utiliser Gestion des identités et des accès AWS (IAM) et Amazon Redshift pour sécuriser vos ressources en contrôlant qui peut y accéder. Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Redshift.

Octroi d'autorisations à Amazon Redshift Serverless

Pour accéder à d'autres AWS services, Amazon Redshift Serverless a besoin d'autorisations. Certaines fonctionnalités d'Amazon Redshift nécessitent qu'Amazon Redshift accède à AWS d'autres services en votre nom. Pour que votre instance Amazon Redshift sans serveur agisse en votre nom, fournissez-lui des informations d'identification de sécurité. La méthode préférée pour fournir des informations d'identification de sécurité consiste à spécifier un rôle Gestion des identités et des accès AWS (IAM). Vous pouvez également créer un rôle IAM via la console Amazon Redshift et le définir comme rôle par défaut. Pour de plus amples informations, veuillez consulter Création d'un rôle IAM par défaut pour Amazon Redshift.

Pour accéder à d'autres AWS services, créez un rôle IAM doté des autorisations appropriées. Vous devez également associer le rôle à Amazon Redshift sans serveur. En outre, spécifiez l'Amazon Resource Name (ARN) du rôle lorsque vous exécutez la commande Amazon Redshift ou spécifiez le mot clé `default`.

Lorsque vous modifiez la relation de confiance pour le rôle IAM dans le https://console.aws.amazon.com/iam/, assurez-vous qu'il contient `redshift-serverless.amazonaws.com` et `redshift.amazonaws.com` comme noms de service principaux. Pour plus d'informations sur la façon de gérer les rôles IAM afin d'accéder à d'autres AWS services en votre nom, consultezAutorisation d'accès à Amazon Redshift AWS services en votre nom.

Création d'un rôle IAM par défaut pour Amazon Redshift

Lorsque vous créez des rôles IAM via la console Amazon Redshift, Amazon Redshift crée les rôles par programme dans votre. Compte AWS Amazon Redshift y associe également automatiquement

les politiques AWS gérées existantes. Cette approche signifie que vous pouvez rester dans la console Amazon Redshift et que vous n'avez pas besoin de passer à la console IAM pour créer des rôles.

Le rôle IAM que vous créez via la console pour votre cluster a la politique gérée par `AmazonRedshiftAllCommandsFullAccess` attachée automatiquement. Ce rôle IAM permet à Amazon Redshift de copier, décharger, interroger et analyser les données relatives AWS aux ressources de votre compte IAM. Les commandes associées incluent COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL TABLE, CREATE EXTERNAL SCHEMA, CREATE MODEL et CREATE LIBRARY. Pour plus d'informations sur le mode de création d'un rôle IAM par défaut pour Amazon Redshift, consultez Création d'un rôle IAM par défaut pour Amazon Redshift.

Pour commencer à créer un rôle IAM par défaut pour Amazon Redshift, ouvrez Console de gestion AWS le, choisissez la console Amazon Redshift, puis choisissez Redshift Serverless dans le menu. Depuis le tableau de bord sans serveur, vous pouvez créer un nouveau groupe de travail. Les étapes de création vous guident dans la sélection d’un rôle IAM ou la configuration d’un nouveau rôle IAM.

Si vous disposez d’un groupe de travail Amazon Redshift sans serveur existant et que vous souhaitez configurer des rôles IAM pour celui-ci, ouvrez la Console de gestion AWS. Choisissez la console Amazon Redshift, puis choisissez Redshift sans serveur). Sur la console Amazon Redshift sans serveur, choisissez Configuration d’espace de noms pour un groupe de travail existant. Sous Sécurité et chiffrement, vous pouvez modifier les autorisations.

Attribution de rôles IAM à un espace de noms

Chaque rôle IAM est une AWS identité dotée de politiques d'autorisation qui déterminent les actions que chaque rôle peut effectuer. AWS Le rôle est destiné à être endossé par toute personne qui en a besoin. En outre, chaque espace de noms représente une collection d'objets, tels que des tables et des schémas, et d'utilisateurs. Lorsque vous utilisez Amazon Redshift sans serveur, vous pouvez associer plusieurs rôles IAM à votre espace de noms. Il est ainsi plus facile de structurer vos autorisations de manière appropriée pour une collection d'objets de base de données, afin que les rôles puissent effectuer des actions sur les données internes et externes. Par exemple, pour que vous puissiez exécuter une commande `COPY` dans une base de données Amazon Redshift pour récupérer des données d'Amazon S3 et remplir une table Redshift.

Vous pouvez associer plusieurs rôles à un espace de noms à l'aide de la console, comme décrit précédemment dans cette section. Vous pouvez également utiliser la commande API `CreateNamespace`, ou la commande CLI `create-namespace`. Avec l'API ou la commande CLI,

vous pouvez attribuer des rôles IAM à l'espace de noms en remplissant `IAMRoles` avec un ou plusieurs rôles. Plus précisément, vous ajoutez des ARN pour des rôles spécifiques à la collection.

Gestion des rôles IAM associés à l'espace de noms

Sur le, Console de gestion AWS vous pouvez gérer les politiques d'autorisation pour les rôles dans Gestion des identités et des accès AWS. Vous pouvez gérer les rôles IAM pour l'espace de noms, en utilisant les paramètres disponibles sous Namespace configuration (Configuration de l'espace de noms). Pour obtenir plus d'informations sur les espaces de noms et leur utilisation dans Amazon Redshift sans serveur, consultez Groupe de travail et espace de noms.

Mise en route avec les informations d'identification IAM pour Amazon Redshift

Lorsque vous vous connectez à la console Amazon Redshift et que vous essayez Amazon Redshift sans serveur pour la première fois, nous vous recommandons de vous connecter en tant qu'utilisateur avec un rôle IAM associé avec les politiques requises. Après avoir commencé à créer une instance Amazon Redshift sans serveur, Amazon Redshift enregistre le nom du rôle IAM que vous avez utilisé pour vous connecter. Vous pouvez utiliser les mêmes informations d'identification pour vous connecter à la console Amazon Redshift et à la console Amazon Redshift sans serveur.

Lors de la création de l'instance Amazon Redshift sans serveur, vous pouvez créer une base de données. Utilisez l'éditeur de requête v2 pour vous connecter à la base de données avec l'option d'informations d'identification temporaires.

Pour ajouter un nouveau nom d'utilisateur et un nouveau mot de passe d'administrateur qui persistent pour la base de données, choisissez Customize admin user credentials (Personnaliser les informations d'identification d'administrateur et entrez un nouveau nom d'administrateur et un nouveau mot de passe d'administrateur.

Pour commencer à utiliser Amazon Redshift sans serveur et créer un groupe de travail et un espace de noms dans la console pour la première fois, utilisez un rôle IAM avec une politique d'autorisations attachée. Assurez-vous que ce rôle dispose de l'autorisation d'administrateur `arn:aws:iam::aws:policy/AdministratorAccess` ou l'autorisation complète Amazon Redshift `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess` attachée à la politique IAM.

Les scénarios suivants décrivent comment vos informations d'identification IAM sont utilisées par Amazon Redshift Serverless lorsque vous démarrez sur la console Amazon Redshift Serverless :

- Si vous choisissez Use default settings (Utiliser les paramètres par défaut)—, Amazon Redshift Serverless traduit votre identité IAM actuelle en super-utilisateur de base de données. Vous pouvez utiliser la même identité IAM avec la console Amazon Redshift sans serveur pour effectuer des actions de super-utilisateur dans votre base de données dans Amazon Redshift sans serveur.
- Si vous choisissez Customize settings (Personnaliser les paramètres) sans spécifier la valeur Admin user name (Nom d'utilisateur administrateur) et le mot de passe de l'administrateur Amazon Redshift sans serveur, vos informations d'identification IAM actuelles sont utilisées comme informations d'identification de l'utilisateur administrateur par défaut.
- Si vous choisissez Customize settings (Personnaliser les paramètres) et spécifiez un nom d'administrateur et un mot de passe Amazon Redshift Serverless, Amazon Redshift Serverless traduit votre identité IAM actuelle en super-utilisateur de base de données. Amazon Redshift Serverless crée également une autre paire de nom d'utilisateur et de mot de passe de connexion à long terme en tant que super-utilisateur. Vous pouvez soit utiliser votre identité IAM actuelle, soit la paire de nom d'utilisateur et de mot de passe créées pour vous connecter à votre base de données en tant que super-utilisateur.

Accès aux objets de base de données Amazon Redshift sans serveur avec des autorisations de rôle de base de données

Cette procédure montre comment accorder une autorisation d'interroger une table via un rôle de base de données Amazon Redshift. Le rôle est attribué au moyen d'une balise attachée à un utilisateur dans IAM et transmise à Amazon Redshift au moment où il se connecte. Il s'agit d'une explication par l'exemple des concepts décrits dans Définition des rôles de base de données à accorder aux utilisateurs fédérés dans Amazon Redshift sans serveur. L'avantage de ces étapes est que vous pouvez associer un utilisateur à un rôle de base de données sans avoir à lui définir des autorisations pour chaque objet de base de données. Il est ainsi plus simple de gérer le pouvoir de l'utilisateur d'interroger, modifier ou ajouter des données à des tables et d'effectuer d'autres actions.

La procédure suppose que vous avez déjà configuré une base de données Amazon Redshift sans serveur et que vous êtes en mesure d'accorder des autorisations dans la base de données. Cela suppose également que vous êtes autorisé à créer un utilisateur IAM dans la AWS console, à créer un rôle IAM et à attribuer des autorisations de politique.

1. Créez un utilisateur IAM à l'aide de la console IAM. Vous vous en servirez par la suite pour vous connecter à la base de données.

2. Créez un rôle de base de données Redshift à l'aide de l'éditeur de requête v2 ou d'un autre client SQL. Pour en savoir plus sur la création de rôles de base de données, consultez CREATE ROLE.

   ```
   CREATE ROLE urban_planning;
   ```

   Interrogez la vue système SVV_ROLES pour vérifier que votre rôle est créé. Elle renvoie également les rôles système.

   ```
   SELECT * from SVV_ROLES;
   ```

3. Accordez au rôle de base de données que vous avez créé l'autorisation d'effectuer une sélection dans une table. (Par la suite, l'utilisateur IAM que vous avez créé se connectera et sélectionnera des enregistrements dans la table au moyen du rôle de base de données.) Le nom de rôle et le nom de table figurant dans l'exemple de code suivant sont des exemples. Ici, autorisation est donnée d'effectuer une sélection dans une table nommée `cities`.

   ```
   GRANT SELECT on TABLE cities to ROLE urban_planning;
   ```

4. Utilisez la Gestion des identités et des accès AWS console pour créer un rôle IAM. Ce rôle accorde l'autorisation d'utiliser l'éditeur de requête v2. Créez un nouveau rôle IAM puis, pour le type d'entité de confiance, choisissez Compte AWS . Choisissez ensuite Ce compte. Accordez au rôle les autorisations de politique suivantes :

   - `AmazonRedshiftReadOnlyAccess`
   - `tag:GetResources`
   - `tag:GetTagKeys`
   - Toutes les actions pour sqlworkbench, dont `sqlworkbench:ListDatabases` et `sqlworkbench:UpdateConnection`.

5. Dans la console IAM, ajoutez une balise avec la Clé `RedshiftDbRoles` à l'utilisateur IAM que vous avez créé précédemment. La valeur de la balise doit correspondre au rôle de base de données que vous avez créé à la première étape. Dans l'exemple, il s'agit de `urban_planning`.

Une fois ces étapes terminées, attribuez le rôle IAM à l'utilisateur que vous avez créé dans la console IAM. Lorsque l'utilisateur se connecte à la base de données avec l'éditeur de requête v2, son nom de rôle de base de données qui figure dans la balise est transmis à Amazon Redshift et lui est associé. Ainsi, il peut interroger les tables appropriées au moyen du rôle de base de données. À titre

d'exemple, l'utilisateur de cet exemple peut interroger la table `cities` via le rôle de base de données `urban_planning`.

Migration à partir d'un cluster provisionné vers Amazon Redshift sans serveur

Vous pouvez migrer vos clusters alloués existants vers Amazon Redshift sans serveur, ce qui permet une mise à l'échelle automatique et à la demande des ressources de calcul. La migration d'un cluster alloué vers Amazon Redshift sans serveur vous permet d'optimiser les coûts en ne payant que pour les ressources que vous utilisez et en mettant automatiquement à l'échelle la capacité en fonction des demandes de charge de travail. Les cas d'utilisation courants de la migration incluent l'exécution de requêtes ad hoc, de tâches de traitement de données périodiques ou la gestion de charges de travail imprévisibles sans surallouer les ressources. Effectuez les tâches suivantes pour migrer votre cluster Amazon Redshift alloué vers l'option de déploiement sans serveur.

Création d'un instantané de votre cluster alloué

> **Note**
>
> Amazon Redshift convertit automatiquement les clés entrelacées en clés composées lorsque vous restaurez un instantané de cluster provisionné dans un espace de noms sans serveur.

Pour transférer des données de votre cluster provisionné vers Amazon Redshift sans serveur, créez un instantané de votre cluster provisionné, puis restaurez l'instantané dans Amazon Redshift sans serveur.

> **Note**
>
> Avant de migrer vos données vers un groupe de travail sans serveur, vérifiez que les besoins de votre cluster provisionné sont compatibles avec la quantité de RPU que vous choisissez dans Amazon Redshift Serverless.

Pour créer un instantané de votre cluster provisionné

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.

2. Dans le menu de navigation, choisissez Clusters, Snapshots (Instantanés), puis choisissez l'onglet Create snapshot (Créer un instantané).
3. Entrez les propriétés de la définition de l'instantané, puis choisissez Create snapshot (Créer un instantané). L'instantané n'est pas toujours disponible immédiatement.

Pour restaurer un instantané de cluster provisionné dans un espace de noms sans serveur :

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Démarrez la console de cluster provisionné Amazon Redshift et accédez à Clusters, sur la page Snapshots (Instantanés).
3. Choisissez un instantané à utiliser.
4. Choisissez Restore snapshot (Restaurer un instantané), Restore to serverless namespace (Restaurer vers un espace de noms sans serveur).
5. Choisissez un espace de noms dans lequel restaurer votre instantané.
6. Confirmez que vous souhaitez effectuer une restauration à partir de votre instantané. Cette action remplace toutes les bases de données de votre point de terminaison sans serveur par les données de votre cluster alloué. Choisissez Restore (Restaurer).

Pour plus d'informations sur les instantanés de cluster provisionnés, consultez Instantanées Amazon Redshift.

Connexion à Amazon Redshift sans serveur à l'aide d'un pilote

Pour vous connecter à Amazon Redshift sans serveur avec votre client SQL préféré, vous pouvez utiliser le pilote JDBC version 2.x fourni par Amazon Redshift. Nous vous recommandons de vous connecter à Amazon Redshift à l'aide de la dernière version du pilote JDBC Amazon Redshift version 2.x. Le numéro de port est facultatif. Si vous ne l'incluez pas, Amazon Redshift sans serveur utilise par défaut le numéro de port 5439. Vous pouvez passer à un autre port dans la plage de ports 5431-5455 ou 8191-8215. Pour modifier le port par défaut d'un point de terminaison sans serveur, utilisez l' AWS CLI API Amazon Redshift.

Pour connaître le point de terminaison exact à utiliser pour le pilote JDBC, ODBC ou Python, consultez Configuration du groupe de travail dans Amazon Redshift sans serveur. Vous pouvez également utiliser l'opération d'API Amazon Redshift Serverless `GetWorkgroup` ou l' AWS CLI

opération `get-workgroups` pour renvoyer des informations sur votre groupe de travail, puis vous connecter.

Connexion à l'aide d'une authentification par mot de passe

Pour établir une connexion à l'aide du pilote JDBC Amazon Redshift version 2.x avec authentification par mot de passe, utilisez la syntaxe suivante :

```
jdbc:redshift://<workgroup-name>.<account-number>.<aws-region>.redshift-
serverless.amazonaws.com:5439/?username=username&password=password
```

Pour établir une connexion à l'aide du connecteur Amazon Redshift Python avec authentification par mot de passe, utilisez la syntaxe suivante :

```
import redshift_connector
with redshift_connector.connect(
    host='<workgroup-name>.<account-number>.<aws-region>.redshift-
serverless.amazonaws.com',
    database='<database-name>',
    user='username',
    password='password'
    # port value of 5439 is specified by default
) as conn:
    pass
```

Pour établir une connexion à l'aide du pilote ODBC Amazon Redshift version 2.x avec authentification par mot de passe, utilisez la syntaxe suivante :

```
Driver={Amazon Redshift ODBC Driver (x64)}; Server=<workgroup-name>.<account-
number>.<aws-region>.redshift-serverless.amazonaws.com; Database=database-name;
 User=username; Password=password
```

Connexion à l'aide d'IAM

Si vous préférez vous connecter avec IAM, utilisez l'opération d'API Amazon Redshift sans serveur `GetCredentials`.

Pour utiliser l'authentification IAM, ajoutez `iam:` à l'URL Amazon Redshift JDBC après `jdbc:redshift:`, comme indiqué dans l'exemple suivant.

```
jdbc:redshift:iam://<workgroup-name>.<account-number>.<aws-region>.redshift-
serverless.amazonaws.com:5439/<database-name>
```

Ce point de terminaison Amazon Redshift sans serveur ne prend pas en charge la personnalisation de dbUser, dbGroup ou la création automatique. Par défaut, le pilote crée automatiquement des utilisateurs de base de données lors de la connexion. Il affecte ensuite les utilisateurs aux rôles de base de données Amazon Redshift en fonction des balises spécifiées dans IAM ou des groupes définis dans votre fournisseur d'identité (IdP).

Assurez-vous que votre AWS identité dispose de la bonne politique IAM pour l'`redshift-serverless:GetCredentials`action. Voici un exemple de politique IAM qui accorde les autorisations appropriées à une AWS identité pour qu'elle se connecte à Amazon Redshift Serverless. Pour plus d'informations sur les autorisations IAM, consultez la rubrique Ajout et suppression d'autorisations basées sur l'identité IAM dans le Guide de l'utilisateur IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Action": "redshift-serverless:GetCredentials",
            "Resource": "*"
        }
    ]
}
```

Pour établir une connexion à l'aide du connecteur Amazon Redshift Python avec une authentification basée sur IAM, utilisez `iam=true` dans votre code, comme indiqué dans la syntaxe suivante :

```
import redshift_connector
with redshift_connector.connect(
    iam=True,
    host='<workgroup-name>.<account-number>.<aws-region>.redshift-
serverless.amazonaws.com',
    database='<database-name>'
    <IAM credentials>
```

```
) as conn:
    pass
```

Pour `IAM credentials`, vous pouvez utiliser toutes les informations d'identification, y compris les suivantes :

- AWS configuration du profil.
- Informations d'identification IAM (ID de clé d'accès, clé d'accès secrète et éventuellement jeton de session).
- Fédération du fournisseur d'identité

Pour établir une connexion à l'aide du pilote ODBC Amazon Redshift version 2.x avec une authentification basée sur IAM et un profil, utilisez la syntaxe suivante :

```
Driver={Amazon Redshift ODBC Driver (x64)}; IAM=true; Server=<workgroup-name>.<account-number>.<aws-region>.redshift-serverless.amazonaws.com; Database=database-name;
 Profile=aws-profile-name;
```

Connexion via IAM avec l'API GetClusterCredentials

> **Note**
>
> Lorsque vous vous connectez à Amazon Redshift sans serveur, nous vous recommandons d'utiliser l'API `GetCredentials`. Cette API offre une fonctionnalité complète de contrôle d'accès basé sur les rôles (RBAC) ainsi que d'autres nouvelles fonctionnalités qui ne sont pas disponibles dans `GetClusterCredentials`. Nous prenons en charge l'API `GetClusterCredentials` afin de simplifier la transition entre les clusters alloués et les groupes de travail sans serveur, mais nous vous recommandons vivement de migrer vers `GetCredentials` dès que possible pour une compatibilité optimale.

Vous pouvez établir une connexion à Amazon Redshift sans serveur à l'aide de l'API `GetClusterCredentials`. Pour implémenter cette méthode d'authentification, modifiez votre client ou votre application en incorporant les paramètres suivants :

- `iam=true`
- `clusterid/cluster_identifier=redshift-serverless-<workgroup-name>`

- `region=<aws-region>`

Les exemples suivants illustrent le plug-in BrowserSAML sur les trois pilotes. Cela représente l'une des nombreuses approches d'authentification disponibles. Les exemples peuvent être modifiés pour utiliser des méthodes d'authentification ou des plug-ins alternatifs en fonction de vos besoins spécifiques.

Autorisations relatives à la politique IAM pour GetClusterCredentials

Voici un exemple de politique IAM avec les autorisations requises pour utiliser `GetClusterCredentials` avec Amazon Redshift sans serveur :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "redshift-serverless:GetWorkgroup",
                "redshift-serverless:GetNamespace",
                "redshift:GetClusterCredentials",
                "redshift:CreateClusterUser",
                "redshift:JoinGroup",
                "redshift:ExecuteQuery",
                "redshift:FetchResults",
                "redshift:DescribeClusters",
                "redshift:DescribeTable"
            ],
            "Resource": [
                "arn:aws:redshift-serverless:us-
east-1:111122223333:workgroup/workgroup-name",
                "arn:aws:redshift-serverless:us-
east-1:111122223333:namespace/namespace-name",
                "arn:aws:redshift:us-east-1:111122223333:cluster:cluster-name",
                "arn:aws:redshift:us-east-1:111122223333:dbuser:database-name/
${redshift:DbUser}"
            ]
        }
```

```
    ]
}
```

Pour établir une connexion à l'aide du pilote JDBC Amazon Redshift version 2.x avec `GetClusterCredentials`, utilisez la syntaxe suivante :

```
jdbc:redshift:iam://redshift-serverless-<workgroup-name>:<aws-region>/<database-name>?
plugin_name=com.amazon.redshift.plugin.BrowserSamlCredentialsProvider&login_url=<single
 sign-on URL from IdP>"
```

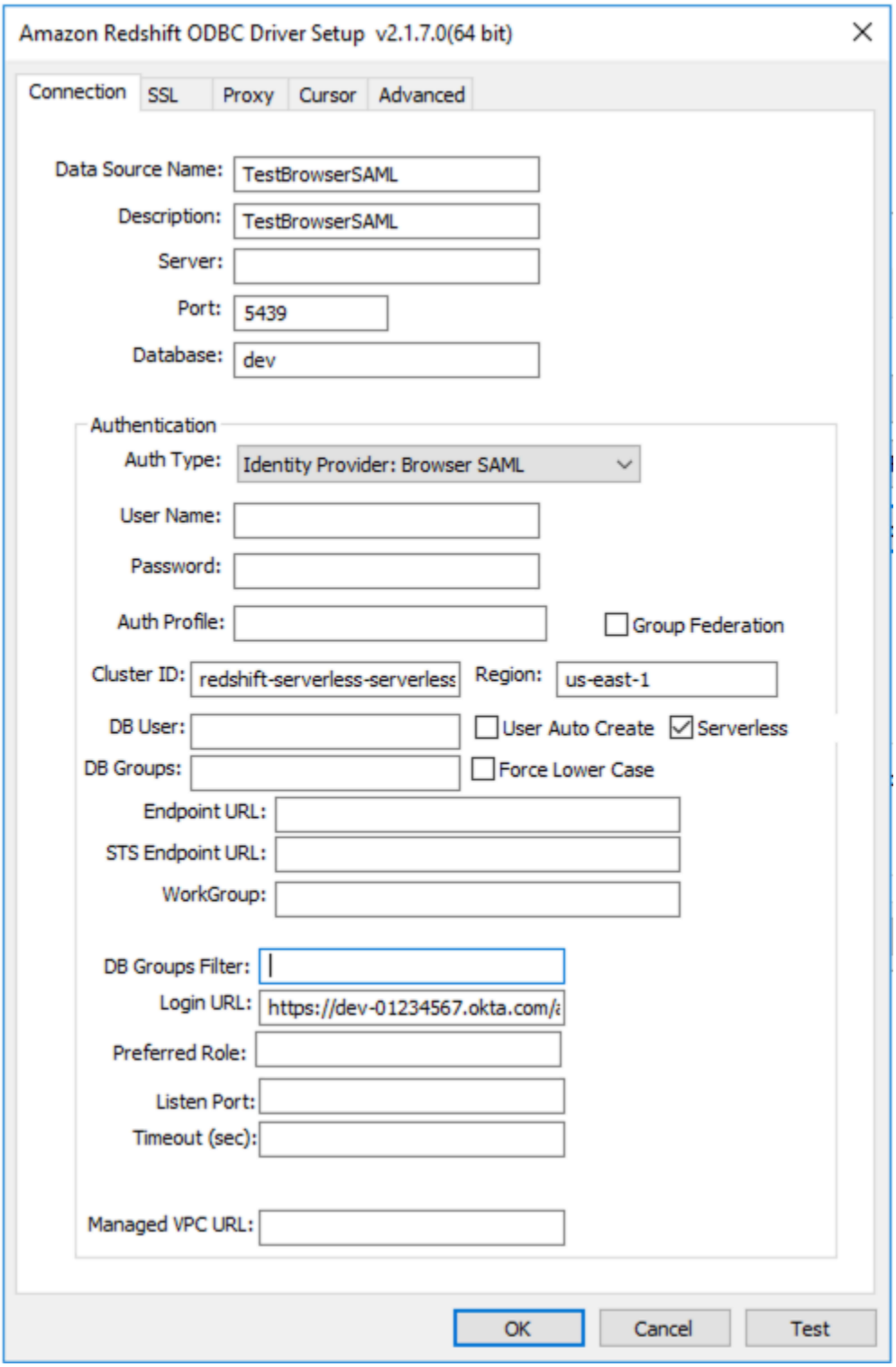
Pour établir une connexion à l'aide du connecteur Amazon Redshift Python avec `GetClusterCredentials`, utilisez la syntaxe suivante :

```
import redshift_connector
with redshift_connector.connect(
    iam=True,
    cluster_identifier='redshift-serverless-<workgroup-name>',
    region='<aws-region>',
    database='<database-name>',
    credentials_provider='BrowserSamlCredentialsProvider'
    login_url='<single sign-on URL from IdP>'
    # port value of 5439 is specified by default
) as conn:
    pass
```

Pour établir une connexion à l'aide du pilote ODBC Amazon Redshift version 2.x avec `GetClusterCredentials`, utilisez la syntaxe suivante :

```
Driver= {Amazon Redshift ODBC Driver (x64)}; IAM=true; isServerless=true;
 ClusterId=redshift-serverless-<workgroup-name>; region=<aws-region>;
 plugin_name=BrowserSAML;login_url=<single sign-on URL from IdP>
```

Voici un exemple de configuration DSN ODBC sous Windows :



Utilisation du kit SDK Amazon Redshift sans serveur

Si vous avez écrit des scripts de gestion à l'aide du kit SDK Amazon Redshift, vous devez utiliser le nouveau kit SDK Amazon Redshift sans serveur pour gérer Amazon Redshift sans serveur et les

ressources associées. Pour plus d'informations sur les opérations d'API disponibles, consultez le guide de référence de l'API de données Amazon Redshift sans serveur.

Groupe de travail et espace de noms

Pour isoler les charges de travail et gérer différentes ressources dans Amazon Redshift sans serveur, vous pouvez créer des espaces de noms et des groupes de travail et gérer séparément les ressources de stockage et de calcul.

Un espace de noms est une collection d'objets de base de données et d'utilisateurs. L'espace de noms lié au stockage regroupe des schémas, des tables, des utilisateurs ou des AWS Key Management Service clés pour chiffrer les données. Les propriétés de stockage comprennent le nom de la base de données et le mot de passe de l'utilisateur administrateur, les autorisations, le chiffrement et la sécurité. D'autres ressources sont regroupées dans les espaces de noms, notamment les unités de partage des données, les points de récupération et les limites d'utilisation. Vous pouvez configurer ces propriétés de stockage à l'aide de la console Amazon Redshift Serverless, des API Amazon Redshift Serverless ou des API Amazon Redshift Serverless pour la ressource spécifique. AWS Command Line Interface

Le groupe de travail est une collection de ressources informatiques. Le groupe de travail lié à l'informatique regroupe les ressources informatiques comme les RPU, les groupes de sous-réseau VPC et les groupes de sécurité. Les propriétés du groupe de travail comprennent les paramètres de réseau et de sécurité. Les limites d'accès et d'utilisation sont d'autres ressources qui sont regroupées dans les groupes de travail. Vous pouvez configurer ces propriétés de calcul à l'aide de la console Amazon Redshift Serverless, des API Amazon Redshift Serverless ou des API Amazon Redshift Serverless. AWS Command Line Interface

Vous pouvez créer un ou plusieurs espaces de noms et groupes de travail. Chaque espace de noms ne peut être associé qu'à un seul groupe de travail. À l'inverse, chaque groupe de travail ne peut être associé qu'à un seul espace de noms.

Groupes de travail et espaces de noms à l'aide de la console

La mise en place d'Amazon Redshift sans serveur implique de passer par plusieurs étapes de configuration. Lorsque vous suivez les étapes de configuration d'Amazon Redshift sans serveur, vous créez un espace de noms et un groupe de travail, et vous les associez les uns aux autres. Pour commencer à définir la configuration d'Amazon Redshift sans serveur à l'aide de la console Amazon Redshift sans serveur, vous pouvez choisir Get started with Amazon Redshift sans serveur (Démarrer avec Amazon Redshift sans serveur) pour configurer Amazon Redshift sans serveur et commencer

à interagir avec. Vous pouvez choisir un environnement avec des paramètres par défaut pour une installation plus rapide, ou configurer explicitement les paramètres en fonction des besoins de votre organisation. Au cours de ce processus, vous spécifiez les paramètres de votre groupe de travail et votre espace de noms.

Après avoir configuré l'environnement, Propriétés d'un groupe de travail et Propriétés de l'espace de noms vous aident à vous familiariser avec les paramètres.

Groupes de travail et espaces de noms utilisant le AWS Command Line Interface et API sans serveur Amazon Redshift

Outre l'utilisation de la AWS console, vous pouvez également utiliser l' AWS CLI API Amazon Redshift Serverless pour interagir avec les groupes de travail et les espaces de noms. Le tableau ci-dessous répertorie les opérations d'API et CLI que vous pouvez utiliser pour gérer les instantanés et les points de récupération.

Opération API	Commande de la CLI	Description
CreateNamespace	create-namespace	Crée un espace de noms. Par défaut, Amazon Redshift Serverless crée des espaces de noms avec une AWS Key Management Service clé par défaut, mais vous pouvez spécifier une autre clé pour chiffrer vos données. Vous pouvez également créer un espace de noms en restauran t un instantané. Pour plus d'informations, consultez Utilisation des instantanés et des points de récupération.
UpdateNamespace	update-namespace	Met à jour un espace de noms.
GetNamespace	get-namespace	Extrait des informations sur un espace de noms.

Opération API	Commande de la CLI	Description
ListNamepaces	list-namespaces	Extrait des informations sur une liste d'espaces de noms.
DeleteNamespace	delete-namespace	Supprime un espace de noms.
CreateWorkgroup	create-workgroup	Crée un groupe de travail. Lorsque vous créez un groupe de travail, assurez-vous de disposer d'un espace de noms existant que vous pouvez associer au groupe de travail. Lorsque vous créez le groupe de travail, vous pouvez spécifier des ressources de calcul, comme des sous-rése aux, des groupes de sécurité et des RPU.
UpdateWorkgroup	update-workgroup	Met à jour un groupe de travail.
GetWorkgroup	get-workgroup	Extrait des informations sur un groupe de travail.
ListWorkgroups	list-workgroups	Extrait des informations sur une liste de groupes de travail.
DeleteWorkgroup	delete-workgroup	Supprime un groupe de travail.

Groupes de travail

Avec Amazon Redshift sans serveur, vous pouvez créer et gérer des groupes de travail pour isoler et contrôler les ressources de calcul pour différentes charges de travail ou différents utilisateurs. Les groupes de travail vous permettent de définir des options de configuration telles que les limites de mise à l'échelle de la mémoire et de la simultanéité, et de prioriser l'exécution des requêtes

pour toutes les charges de travail. Le groupe de travail lié à l'informatique regroupe des ressources informatiques comme les RPU et les groupes de sous-réseau VPC.

Création d'un groupe de travail avec un espace de noms

Suivez ces étapes pour créer un groupe de travail. Pour plus d'informations sur la configuration réseau, consultez Propriétés d'un groupe de travail.

1. Choisissez Serverless dashboard (Tableau de bord sans serveur). Choisissez ensuite Create workgroup (Créer un groupe de travail).
2. Saisissez le nom du groupe de travail.
3. Choisissez un type d'adresse IP pour le groupe de travail. Voici les choix possibles :
   - IPv4 : avec cette option, vos ressources AWS communiquent uniquement via le protocole d'adressage IPv4.
   - Dual-stack mode : avec cette option, vos AWS ressources peuvent communiquer via le protocole d'adressage IPv4, IPv6 ou les deux. Vous devez également associer un bloc CIDR IPv6 au VPC et aux sous-réseaux utilisés pour votre groupe de travail dans le VPC Amazon. Vous pouvez utiliser la console Amazon VPC pour créer un VPC Amazon ou mettre à jour un VPC Amazon existant pour utiliser l'adressage IPv6. Pour plus d'informations, consultez la section Prise en charge de IPv6 pour votre VPC dans le Guide de l'utilisateur Amazon VPC.
4. Choisissez un Virtual private cloud (VPC) [Cloud privé virtuel (VPC)] pour Amazon Redshift sans serveur. Cela affecte le groupe de travail à un réseau virtuel spécifique de votre AWS environnement. Lorsque vous utilisez le mode double pile, le VPC Amazon que vous choisissez doit prendre en charge l'adressage IPV6. Pour plus d'informations sur les VPC Amazon, consultez Vue d'ensemble des VPC et des sous-réseaux.
5. Choisissez un ou plusieurs VPC security groups (Groupes de sécurité VPC). Pour plus d'informations, consultez Contrôler le trafic vers les ressources à l'aide des groupes de sécurité.
6. Choisissez si vous souhaitez activer des ressources de calcul supplémentaires pour les optimisations automatiques. Pour plus d'informations, consultez la section Allocation de ressources de calcul supplémentaires pour l'optimisation automatique des bases de données dans le manuel Amazon Redshift Database Developer Guide.
7. Sous Subnet (Sous-réseau), spécifiez un ou plusieurs sous-réseaux à associer à votre base de données. Ces sous-réseaux font partie du VPC Amazon que vous avez choisi précédemment et doivent se trouver dans trois zones de disponibilité distinctes. Pour en savoir plus, consultez Considérations relatives à l'utilisation d'Amazon Redshift sans serveur.

8. Sélectionnez la capacité RPU de base qui correspond à vos besoins.

Choisir un espace de noms

1. Choisissez soit Create a new namespace (Créer un espace de noms) et entrez le nom de l'espace de noms, soit Add to an existing namespace (Ajouter à un espace de noms existant) et sélectionnez l'espace de noms dans la liste déroulante.
2. Pour le champ Database name and password (Nom et mot de passe de la base de données), indiquez le nom de la première base de données. Vous pouvez également spécifier un administrateur autre que celui de la console par défaut, en modifiant le champ Admin user credentials (Informations d'identification de l'utilisateur Admin).
3. Pour Permissions (Autorisations), vous choisissez Associate IAM role (Associer un rôle IAM) pour associer des rôles IAM spécifiques à votre espace de noms et à votre groupe de travail. Pour plus d'informations sur l'association des rôles IAM avec Amazon Redshift, consultez Identity and access management in Amazon Redshift (Gestion des identités et des accès dans Amazon Redshift).
4. Vous pouvez personnaliser vos paramètres de chiffrement en créant une nouvelle clé ou en choisissant une clé autre que celle par défaut. Pour Audit logging (Journalisation de l'audit), choisissez les journaux à exporter. Chaque type de journal spécifie des métadonnées différentes. Choisissez Continue (Continue)r pour passer en revue vos choix.

Examiner les sélections des groupes de travail

1. Examinez vos paramètres sous la rubrique Review and create (Examiner et créer). Elle affiche les paramètres que vous avez choisis dans les étapes précédentes.
2. Choisissez Enregistrer.

Une fois que vous avez créé le groupe de travail, il est ajouté à la liste Workgroups (Groupes de travail).

Affichage des propriétés d'un groupe de travail

Dans Amazon Redshift sans serveur, un groupe de travail est une collection de ressources de calcul prêtes à être utilisées. Lorsque vous choisissez Amazon Redshift Serverless, dans la AWS console, vous pouvez choisir Configuration du groupe de travail dans le menu de navigation pour afficher une liste. Vous pouvez utiliser la zone Search (Recherche) pour trouver des groupes de travail qui

répondent à vos critères de recherche. Quelques propriétés sont affichées pour chaque entrée de groupe de travail :

- WorkGroup (Groupe de travail) : le nom du groupe de travail. Vous pouvez le sélectionner pour afficher et modifier les propriétés du groupe de travail.
- Status (État) : indique si le groupe de travail est disponible.
- Namespace (Espace de noms) : l'espace de noms associé au groupe de travail. Chaque groupe de travail est associé à un espace de noms.
- Date de création : la date à laquelle le groupe de travail a été créé.
- Balises : balises associées au groupe de travail.

En outre, la configuration des groupes de travail comporte une autre liste pour les groupes de travail gérés, qui sont des groupes de travail Amazon Redshift Serverless gérés par. AWS Glue Pour plus d'informations sur les groupes de travail gérés, consultez Groupes de travail gérés dans le Guide du développeur de base de données Amazon Redshift.

Propriétés d'un groupe de travail

Vous pouvez répertorier les groupes de travail en choisissant Workgroup configuration (Configuration des groupes de travail) dans le menu de gauche. Vous pouvez ensuite choisir un groupe de travail dans la liste. Plusieurs panneaux affichent les propriétés du groupe de travail. Vous pouvez également effectuer des actions. La section General information (Informations générales) affiche les éléments suivants :

- WorkGroup (Groupe de travail) : le nom du groupe de travail.
- Namespace (Espace de noms) : l'espace de noms associé au groupe de travail. Vous pouvez le sélectionner pour afficher ses propriétés. Un groupe de travail est associé à un seul espace de noms.
- Date created (Date de création) : date à laquelle le groupe de travail a été créé.
- Status (État) : indique si les ressources du groupe de travail sont disponibles. Si elles sont disponibles, vous pouvez vous connecter avec un client à l'instance Amazon Redshift sans serveur, afin d'interroger des données ou de créer des ressources de base de données, ou vous pouvez vous connecter avec l'éditeur de requêtes v2.
- Endpoint (Point de terminaison) : l'URL.

- JDBC URL (URL JDBC) : l'URL pour établir des connexions client JDBC. Vous pouvez utiliser cette URL pour vous connecter avec un pilote JDBC pour Amazon Redshift. Pour plus d'informations, consultez Configuration d'une connexion pour le pilote JDBC version 2.x pour Amazon Redshift.
- ODBC URL (URL ODBC) : l'URL permettant d'établir des connexions client ODBC. Elle contient des propriétés, comme la base de données et l'ID utilisateur, ainsi que leurs valeurs.
- Version du groupe de travail et version du correctif : Amazon Redshift sans serveur publie régulièrement de nouvelles versions et de nouveaux correctifs. Vous pouvez utiliser les numéros de version de groupe de travail et de version de correctif pour suivre les mises à jour logicielles de votre groupe de travail Amazon Redshift sans serveur. Pour plus d'informations sur les modifications et les fonctionnalités incluses dans des correctifs spécifiques, consultez Versions de cluster pour Amazon Redshift.
- ARN du groupe de travail - Le nom de la ressource Amazon pour le groupe de travail.
- Ressources de calcul supplémentaires pour les optimisations automatiques - Si Amazon Redshift alloue des ressources de calcul supplémentaires pour effectuer des optimisations automatiques, même pendant les périodes d'utilisation intensive. Pour plus d'informations, consultez la section Allocation de ressources de calcul supplémentaires pour l'optimisation automatique des bases de données dans le manuel Amazon Redshift Database Developer Guide.

L'onglet Data access (Accès aux données) contient plusieurs panneaux :

- Réseau et sécurité : vous pouvez voir les propriétés du réseau, telles que l'identifiant Cloud privé virtuel (VPC), la liste Groupes de sécurité VPC, le routage VPC amélioré, le type d'adresse IP et le paramètre Publiquement accessible. Si vous choisissez Edit (Modifier), vous pouvez modifier ces paramètres. En outre, vous pouvez sélectionner l'option Turn on enhanced VPC routing (Activer le routage VPC amélioré), qui achemine le trafic réseau entre votre base de données sans serveur et vos référentiels de données via un VPC, pour une confidentialité et une sécurité accrues. Vous pouvez également sélectionner l'option Turn on Public Accessible (Activer l'accès public), qui rend la base de données publiquement accessible depuis l'extérieur du VPC, permettant ainsi aux instances et aux appareils de se connecter.

  Le type d'adresse IP peut être défini sur le mode double pile pour permettre l'accès aux groupes de travail à la fois sur IPv4 et IPv6. Pour plus d'informations sur les protocoles Internet (IP) de communication au niveau de la couche réseau, voir Protocole Internet sur Wikipédia.
- Redshift managed VPC endpoints (Points de terminaison VPC gérés par Redshift) : vous pouvez créer des points de terminaison VPC gérés pour accéder à Amazon Redshift sans serveur depuis un autre VPC.

L'onglet Limits (Limites) comporte des paramètres permettant de contrôler les limites de capacité et d'utilisation d'Amazon Redshift sans serveur. Il contient les panneaux suivants :

- Base capacity in Redshift processing units (RPUs) [Capacité de base en unités de traitement Redshift (RPU)] : vous pouvez définir la capacité de base des ressources de calcul utilisées pour traiter votre charge de travail. Pour plus d'informations, consultez Capacité de calcul pour Amazon Redshift sans serveur.
- Limites d'utilisation : vous pouvez définir jusqu'à quatre limites pour les ressources de calcul maximales que votre instance Amazon Redshift sans serveur peut utiliser au cours d'une période donnée, et sélectionner les actions qu'Amazon Redshift sans serveur doit exécuter quand ces limites sont atteintes. Par exemple, vous pouvez définir deux limites pour votre groupe de travail, l'une de 500 heures de RPU et l'autre de 900 heures de RPU. Vous pouvez demander à Amazon Redshift sans serveur de vous envoyer une alerte lorsqu'il atteint la première limite de 500 heures de RPU, puis de désactiver les requêtes des utilisateurs lorsqu'il atteint la deuxième limite de 900 heures. Ces limites permettent de contrôler les coûts et de les rendre plus prévisibles.
- Query limits (Limites des requêtes) : vous pouvez fixer des limites aux requêtes, comme le paramètre de délai d'expiration. Ces limites vous aident à optimiser les coûts et les performances.

L'onglet Onglets comporte le panneau Balises, qui affiche toutes les balises que vous avez créées pour votre groupe de travail. Pour plus d'informations sur le balisage des ressources, consultez Étiquetage des ressources Amazon Redshift sans serveur.

Propriétés d'un groupe de travail géré

Vous pouvez également choisir des groupes de travail gérés par le AWS Glue Data Catalog dans la liste Groupes de travail gérés.

Les groupes de travail gérés ont des propriétés différentes de celles des groupes de travail classiques. Pour plus d'informations sur les groupes de travail gérés, consultez Groupes de travail gérés dans le Guide du développeur de base de données Amazon Redshift.

La section General information (Informations générales) affiche les éléments suivants :

- Groupe de travail : le nom du groupe de travail géré.
- Date de création : date (UTC) à laquelle le groupe de travail géré a été créé.
- ARN du catalogue : Amazon Resource Name (ARN) du groupe de travail géré dans le AWS Glue Data Catalog.

- État : indique si les ressources de calcul du groupe de travail géré sont disponibles. Si les ressources sont disponibles, vous pouvez vous connecter au catalogue qui utilise le groupe de travail géré avec un client Apache Iceberg-compatible SQL afin d'interroger des données ou de créer des ressources de base de données. Vous pouvez également vous connecter au catalogue à l'aide d'Amazon Redshift Query Editor V2.

Surveillance des requêtes et des bases de données contient le graphe Performances du groupe de travail géré, qui indique le temps moyen écoulé par toutes les requêtes du groupe de travail au fil du temps.

L'onglet Historique des requêtes est une liste de toutes les requêtes du groupe de travail géré. Ses détails incluent des informations telles que l'utilisateur qui a exécuté la requête, le moteur client d'où provient la requête, ainsi que l'ID et le statut de la requête. L'onglet Utilisateurs est une liste de tous les utilisateurs du groupe de travail. L'onglet Métriques de performance affiche diverses métriques telles que le temps moyen des requêtes, le nombre de requêtes terminées et le pourcentage de capacité de stockage utilisée.

Suppression d'un groupe de travail

Vous pouvez supprimer un groupe de travail à l'aide de la console. Avant de faire cela, assurez-vous que vos données sont sauvegardées et que des instantanés sont en place. Dans de nombreux cas, les ressources supprimées dans le cadre du groupe de travail ne peuvent pas être récupérées.

Procédez comme suit :

1. Sélectionnez Amazon Redshift sans serveur (Amazon Redshift sans serveur), choisissez Workgroup configuration (Configuration du groupe de travail) et sélectionnez Delete Amazon Redshift sans serveur instance (Supprimer l'instance Amazon Redshift sans serveur).

2. Une boîte de dialogue s'ouvre. Lorsque vous choisissez de supprimer le groupe de travail, toutes les limites d'utilisation sont supprimées, tous les points de terminaison VPC sont supprimés et l'accès aux points de terminaison VPC est également supprimé.

   Entrez delete (supprimer) et sélectionnez Delete (Supprimer) pour confirmer la suppression.

Une fois les étapes terminées, l'état du groupe de travail est Deleting (Suppression) et une bannière indique que le groupe de travail est en cours de suppression. Pendant que le processus de suppression est en cours, certaines fonctionnalités du Serverless dashboard (Tableau de bord sans

serveur) sont désactivées. Mais vous pouvez configurer des clusters provisionnés sur le Provisioned clusters dashboard (Tableau de bord des clusters provisionnés).

Après avoir supprimé le groupe de travail, il n'apparaît plus dans l'espace de noms. Vous pouvez cliquer sur le bouton Create workgroup (Créer un groupe de travail) pour en créer un autre.

Vous pouvez supprimer un groupe de travail existant et associer un nouveau groupe de travail avec une configuration différente au même espace de noms. Lors de la création du nouveau groupe de travail, choisissez la capacité de base qui correspond à la taille des données associées à l'espace de noms.

Vous pouvez associer un groupe de travail à un espace de noms qui a été créé avec une clé gérée par le client (CMK). Pour plus d'informations sur AWS KMS, consultez la section AWS KMS Concepts.

Espaces de noms

Dans Amazon Redshift sans serveur, un espace de noms définit un conteneur logique pour les objets de la base de données. Il peut contenir des tables, des groupes de travail et d'autres ressources de base de données. Si vous n'avez pas créé de groupe de travail ni d'espace de noms et que vous recherchez des instructions expliquant comment démarrer avec Amazon Redshift sans serveur, consultez Configurer Amazon Redshift sans serveur pour la première fois.

Propriétés de l'espace de noms

Dans Amazon Redshift sans serveur, un espace de noms définit un conteneur pour les objets de la base de données. Vous pouvez choisir Namespace configuration (Configuration des espaces de noms) dans la liste de navigation, sélectionner un espace de noms dans la liste et modifier ses paramètres.

Les informations générales relatives à l'espace de noms sont les suivantes :

- Namespace (Espace de noms) : le nom.
- Namespace ID (ID de l'espace de noms) : l'identifiant unique.
- ARN : identifiant unique utilisé pour spécifier la ressource à travers AWS. Il contient des propriétés comme la région et le service.
- Status (État) : l'état, tel que Available (Disponible).
- Date de création : la date (UTC) de création de l'espace de noms.

- Storage used (Stockage utilisé) : l'espace de stockage utilisé par l'espace de noms et tous ses objets.
- Admin user name (Nom d'utilisateur de l'administrateur) : le compte de l'administrateur. Il s'agit généralement du compte utilisé pour créer l'espace de noms.
- Database name (Nom de la base de données) : le nom de la base de données contenue dans l'espace de noms.
- Total table count (Nombre total de tables) : le nombre de tables dans tous les schémas.

Les paramètres et propriétés supplémentaires de l'espace de noms figurent sur plusieurs onglets. Cela inclut les éléments suivants :

- Workgroup (Groupe de travail) : indique le groupe de travail associé à l'espace de noms.
- Data back up (Sauvegarde des données) : dans ce panneau, vous pouvez configurer et créer des instantanés, ainsi que configurer des points de récupération.
- Security and encryption (Sécurité et chiffrement) : vous pouvez gérer les autorisations des rôles IAM et afficher ou modifier vos paramètres de sécurité et de chiffrement. Il s'agit notamment de l'état de votre clé de chiffrement et du paramètre permettant d'activer la journalisation des audits. Pour plus d'informations sur la journalisation d'audit pour Amazon Redshift sans serveur, consultez Journalisation d'audit pour Amazon Redshift sans serveur.
- Unités de partage des données : affiche les unités de partage des données. Grâce au partage des données, vous pouvez donner accès aux données sans avoir à les copier ou à les déplacer. Pour plus d'informations sur le partage de données, consultez Partage de données dans Amazon Redshift sans serveur.

Recherche d'un espace de noms

Dans le menu Amazon Redshift, vous pouvez sélectionner un élément dans la liste Namespaces (Espaces de noms) afin d'afficher ou de modifier les propriétés d'un espace de noms. Les informations sur la console comprennent le nom de l'espace de noms, le nom de l'administrateur et d'autres propriétés.

Les paramètres et propriétés d'un espace de noms se trouvent sur plusieurs onglets. Cela inclut les éléments suivants :

- Workgroup (Groupe de travail) : affiche les groupes de travail associés à l'espace de noms.

- Data back up (Sauvegarde des données) : vous pouvez configurer et créer des instantanés, ainsi que configurer des points de récupération.
- Security and encryption (Sécurité et chiffrement) : vous pouvez gérer les autorisations des rôles IAM et afficher ou modifier vos paramètres de sécurité et de chiffrement. Il s'agit notamment de l'état de votre clé de chiffrement et de vos paramètres de journalisation des audits.
- Unités de partage des données : affiche les unités de partage des données.

Modification de la sécurité et du chiffrement

Amazon Redshift sans serveur est sécurisé au moyen du chiffrement KMS. Vous pouvez mettre à jour les paramètres de chiffrement via la console :

1. Choisissez Namespace configuration (Configuration d'espace de noms) dans le menu principal de la console, choisissez l'espace de noms à modifier, puis sélectionnez Edit (Modifier) dans l'onglet Security and encryption (Sécurité et chiffrement). Une boîte de dialogue s'affiche.
2. Vous pouvez sélectionner Personnaliser les paramètres de chiffrement, puis Choisir une clé gérée par le AWS client pour modifier la clé utilisée pour chiffrer vos ressources.
3. Pour Audit logging (Journalisation de l'audit), choisissez les journaux à exporter. Chaque type de journal spécifie des métadonnées différentes.
4. Pour terminer la mise à jour de la configuration, choisissez Save changes (Enregistrer les modifications).

Modifier le AWS KMS clé pour un espace de noms

Dans Amazon Redshift, le chiffrement protège les données au repos. Amazon Redshift Serverless utilise automatiquement le chiffrement par AWS KMS clé pour chiffrer à la fois vos ressources Amazon Redshift Serverless et vos instantanés. En tant que bonne pratique, la plupart des organisations passent en revue le type de données qu'elles stockent et prévoient un plan de rotation des clés de chiffrement selon un calendrier. La fréquence de rotation des clés peut varier, en fonction de vos politiques de sécurité des données. Amazon Redshift Serverless prend en charge la modification de la AWS KMS clé de l'espace de noms afin que vous puissiez respecter les politiques de sécurité de votre organisation.

Lorsque vous modifiez la AWS KMS clé, les données restent inchangées.

Modifier un AWS KMS touche à l'aide de la console

Dans Amazon Redshift, le chiffrement protège les données au repos. Amazon Redshift sans serveur utilise le chiffrement automatique des clés AWS KMS pour chiffrer à la fois Amazon Redshift sans serveur et les instantanés. En tant que bonne pratique, la plupart des organisations passent en revue le type de données qu'elles stockent et prévoient un plan de rotation des clés de chiffrement selon un calendrier. La fréquence de rotation des clés peut varier, en fonction de vos politiques de sécurité des données. Amazon Redshift Serverless prend en charge la modification de la AWS KMS clé de l'espace de noms afin que vous puissiez respecter les politiques de sécurité de votre organisation.

Lorsque vous modifiez la AWS KMS clé, les données restent inchangées.

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Namespace configuration (Configuration de l'espace de noms). Choisissez votre espace de noms dans la liste.
3. Dans l'onglet Security and encryption (Sécurité et chiffrement), sélectionnez Edit (Modifier).
4. Choisissez Customize encryption settings (Personnaliser les paramètres de chiffrement), puis sélectionnez une clé pour l'espace de noms. Vous pouvez éventuellement créer une clé.

En évolution AWS KMS clés de chiffrement à l'aide du AWS CLI

Permet `update-namespace` de modifier la AWS KMS clé de l'espace de noms. L'exemple suivant montre la syntaxe de la commande :

```
aws redshift-serverless update-namespace
--namespace-name
[--kms-key-id <id-of-kms-key>]
// other parameters omitted here
```

Vous devez avoir créé un espace de noms, sinon la commande CLI donne lieu à une erreur.

Le temps nécessaire pour changer la clé dépend de la quantité de données dans Amazon Redshift sans serveur. Cette opération prend généralement quinze minutes par tranche de 8 To de données stockées.

Limitations

Vous ne pouvez pas passer d'une clé KMS gérée par le client à une AWS KMS clé. Dans ce cas, vous devez créer un nouvel espace de noms.

Vous ne pouvez pas effectuer d’autres actions pendant la modification de la clé.

Suppression d’un espace de noms

Si vous souhaitez supprimer un espace de noms auquel est associé un groupe de travail, vous devez d’abord supprimer le groupe de travail.

Sur la console Amazon Redshift sans serveur, effectuez les étapes suivantes :

1. Choisissez Namespace configuration (Configuration des espaces de noms) dans le menu de gauche, puis choisissez dans la liste l’espace de noms que vous souhaitez supprimer.
2. Choisissez Actions et sélectionnez Delete namespace (Supprimer l’espace de noms).
3. Une boîte de dialogue s’affiche. Vous pouvez conserver vos données en créant un instantané manuel avant d’effectuer l’opération de suppression.

   Entrez delete (supprimer) et sélectionnez Delete (Supprimer) pour confirmer la suppression.

Surveillance des requêtes et des charges de travail avec Amazon Redshift sans serveur

Vous pouvez surveiller vos requêtes Amazon Redshift sans serveur et votre charge de travail à l’aide des vues système fournies.

Les vues de surveillance sont des vues système dans Amazon Redshift sans serveur utilisées pour contrôler l’utilisation des requêtes et des charges de travail. Ces vues se trouvent dans le schéma `pg_catalog`. Les vues système disponibles ont été conçues pour vous fournir les informations nécessaires pour surveiller Amazon Redshift sans serveur, ce qui s’avère beaucoup plus simple que nécessaire pour les clusters mis en service. Les vues système SYS ont été conçues pour fonctionner avec Amazon Redshift sans serveur. Pour afficher les informations fournies par ces vues, exécutez les instructions SQL SELECT.

Les vues système sont définies pour prendre en charge les objectifs de surveillance suivants.

Surveillance de la charge de travail

Vous pouvez contrôler vos activités de requête au fil du temps pour les tâches suivantes :

- Comprendre les modèles de charge de travail, afin de savoir ce qui est normal (référence) et ce que contiennent les contrat de niveau de service (SLA).
- Identifier rapidement l'écart par rapport à la normale, qui peut être un problème transitoire ou quelque chose qui justifie une action supplémentaire.

Surveillance du chargement et du déchargement de données

Le mouvement des données vers et depuis Amazon Redshift sans serveur constitue une fonction essentielle. Vous utilisez COPY et UNLOAD pour charger ou décharger des données, et vous devez suivre de près les progrès en termes de bytes/rows transfert et de fichiers complétés afin de suivre le respect des SLA commerciaux. Cela se fait normalement en exécutant fréquemment des requêtes dans les tables système (c'est-à-dire toutes les minutes) pour suivre les progrès et émettre des alertes pour investigation/corrective intervenir si des écarts importants sont détectés.

Diagnostic d'échecs et des problèmes

Dans certains cas, vous devez prendre des mesures en cas d'échec de requête ou d'exécution. Les développeurs s'appuient sur des tables système pour auto-diagnostiquer les problèmes et déterminer les solutions correctes.

Personnalisation de performances

Vous devrez peut-être régler les requêtes qui ne répondent pas aux exigences de SLA depuis le début ou qui se sont dégradées au fil du temps. Pour effectuer un réglage, vous devez disposer de détails sur l'exécution, notamment le plan d'exécution, les statistiques, la durée et la consommation de ressources. Il vous faut des données de référence pour les requêtes incriminées afin de déterminer la cause de l'écart et de vous indiquer comment améliorer les performances.

Surveillance des événements des objets utilisateur

Vous devez contrôler les actions et les activités sur les objets utilisateur, comme l'actualisation des vues matérialisées, le vide et l'analyse. Cela inclut les événements gérés par le système, tels que l'actualisation automatique des vues matérialisées. Vous souhaitez contrôler la moment où un événement se termine s'il est initié par l'utilisateur, ou la dernière exécution réussie si le système est initié.

Suivi de l’utilisation pour la facturation

Vous pouvez contrôler vos tendances d’utilisation au fil du temps pour effectuer les actions suivantes :

- Informer la planification budgétaire et les estimations de l’expansion opérationnelle.
- Identifier les opportunités potentielles d’économies telles que la suppression des données froides.

Utilisez les vues système SYS pour surveiller Amazon Redshift sans serveur. Pour plus d’informations sur les vues de surveillance SYS, consultez Vues de surveillance SYS dans le Guide du développeur de base de données Amazon Redshift.

Ajout d’une politique de surveillance des requêtes

Un super-utilisateur peut fournir un accès à des utilisateurs qui ne sont pas des super-utilisateurs afin de pouvoir effectuer une surveillance des requêtes pour tous les utilisateurs. Tout d’abord, vous ajoutez une politique pour un utilisateur ou un rôle afin de fournir un accès à la surveillance des requêtes. Vous accordez ensuite une autorisation de surveillance des requêtes à l’utilisateur ou au rôle.

Pour ajouter la politique de surveillance des requêtes

1. Sélectionnez https://console.aws.amazon.com/iam/.
2. Sous Access Management (Gestion des accès), choisissez Policies (politiques).
3. Choisissez Create Policy (Créer une politique).
4. Choisissez JSON, puis collez la définition de politique suivante.

   JSON

```
{
"Version":"2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
    "redshift-data:ExecuteStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:GetStatementResult",
```

```
    "redshift-data:ListDatabases"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": "redshift-serverless:GetCredentials",
"Resource": "*"
}
]
}
```

5. Choisissez Examiner une politique.
6. Dans le champ Nom, saisissez le nom de la politique, par exemple `query-monitoring`.
7. Choisissez Create Policy (Créer une politique).

Après avoir créé la politique, vous pouvez accorder les autorisations appropriées.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM dans le Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Octroi d’autorisations de surveillance des requêtes à un utilisateur

Les utilisateurs avec une autorisation `sys:monitor` peuvent afficher toutes les requêtes. En outre, les utilisateurs avec une autorisation `sys:operator` peuvent annuler des requêtes, analyser l’historique des requêtes et effectuer des opérations de vide.

Pour accorder une autorisation de surveillance des requêtes à un utilisateur

1. Saisissez la commande suivante pour fournir un accès au moniteur système, où user-name correspond au nom de l’utilisateur auquel vous souhaitez fournir un accès.

```
grant role sys:monitor to "IAM:user-name";
```

2. (Facultatif) Saisissez la commande suivante pour fournir un accès à l’opérateur système, où user-name correspond au nom de l’utilisateur auquel vous souhaitez fournir un accès.

```
grant role sys:operator to "IAM:user-name";
```

Octroi d’autorisations de surveillance des requêtes à un rôle

Les utilisateurs ayant un rôle avec une autorisation `sys:monitor` peuvent afficher toutes les requêtes. En outre, les utilisateurs ayant un rôle qui a une autorisation `sys:operator` peuvent annuler des requêtes, analyser l’historique des requêtes et effectuer des opérations de vide.

Pour accorder une autorisation de surveillance des requêtes à un rôle

1. Saisissez la commande suivante pour fournir un accès au moniteur système, où role-name correspond au nom du rôle auquel vous souhaitez fournir un accès.

```
grant role sys:monitor to "IAMR:role-name";
```

2. (Facultatif) Saisissez la commande suivante pour fournir un accès à l’opérateur système, où role-name correspond au nom du rôle auquel vous souhaitez fournir un accès.

```
grant role sys:operator to "IAMR:role-name";
```

Définition des limites d’utilisation, y compris la définition des limites des RPU

Sous l’onglet Limits (Limites) d’un groupe de travail, vous pouvez ajouter une ou plusieurs limites d’utilisation pour contrôler le nombre maximal de RPU que vous utilisez au cours d’une période donnée, ou pour définir une limite d’utilisation du partage des données.

1. Choisissez Manage usage limits (Gérer les limites d’utilisation). La section des limites apparaît au bas du panneau Utilisation du calcul par période.
2. Définissez une limite d’utilisation sous la forme d’un nombre d’heures de RPU.
3. Choisissez une Fréquence, qui peut être Quotidienne, Hebdomadaire ou Mensuelle. Ce paramètre définit la période de temps pour la limite d’utilisation. Choisir Daily (Quotidienne) dans ce cas vous donne un contrôle plus détaillé.
4. Définissez une limite d’utilisation, en nombre d’heures.
5. Définissez l’action. Les actions sont les suivantes :

   - Journaliser dans la table système : ajoute un enregistrement à la vue système SYS_QUERY_HISTORY. Vous pouvez interroger la colonne `usage_limit` dans cette vue pour déterminer si une requête a dépassé la limite.
   - Alert (Alerte) : utilise Amazon SNS pour configurer les abonnements aux notifications et envoyer des notifications si une limite est dépassée. Vous pouvez choisir une rubrique Amazon SNS existante ou en créer une autre.
   - Turn off user queries (Désactiver les requêtes de l’utilisateur) : désactive les requêtes pour arrêter l’utilisation d’Amazon Redshift sans serveur. L’action envoie également une notification.

   Les deux premières actions ont une visée informative, mais la dernière désactive le traitement des requêtes.
6. Vous pouvez éventuellement définir une limite d'utilisation du partage de Cross-Region données, qui limite la quantité de données transférées de la région productrice vers la région consommatrice que les consommateurs peuvent interroger. Pour ce faire, choisissez Add limit (Ajouter une limite) et suivez les étapes.
7. En bas de la page, choisissez Enregistrer les modifications pour enregistrer cette limite.
8. Définissez jusqu’à 3 limites supplémentaires si nécessaire.

Pour plus d'informations conceptuelles sur les RPU et la facturation, consultez Facturation pour Amazon Redshift sans serveur.

Définition des limites des requêtes

Sous l'onglet Limits (Limites) d'un groupe de travail, vous pouvez ajouter une limite pour surveiller les performances et les limites. Pour plus d'informations sur les limites de surveillance de requête, consultez Règles de surveillance de requête WLM.

1. Choisissez Manage query limits (Gérer les limites des requêtes). Choisissez Add new limit (Ajouter une nouvelle limite) dans la boîte de dialogue Manage query limits (Gérer les limites des requêtes).
2. Choisissez le type de limite que vous souhaitez définir et saisissez une valeur pour la limite correspondante.
3. Choisissez Save changes (Enregistrer les modifications) pour enregistrer la limite.

Lorsque vous modifiez votre limite de requête et vos paramètres de configuration, votre base de données redémarre.

Configuration des files d'attente de requêtes

Amazon Redshift Serverless prend en charge la gestion des ressources de requêtes basée sur les files d'attente. Vous pouvez créer des files d'attente de requêtes dédiées avec des règles de surveillance personnalisées pour différentes charges de travail. Cette fonctionnalité permet un contrôle granulaire de l'utilisation des ressources.

Les règles de surveillance des requêtes (QMR) s'appliquent uniquement au niveau du groupe de travail Redshift Serverless, affectant toutes les requêtes exécutées dans ce groupe de travail de manière uniforme. Queue-based Cette approche vous permet de créer des files d'attente avec des règles de surveillance distinctes. Vous pouvez attribuer ces files d'attente à des rôles d'utilisateur et à des groupes de requêtes spécifiques. Chaque file d'attente fonctionne indépendamment, les règles n'affectant que les requêtes de cette file d'attente.

Les files d'attente vous permettent de définir des prédicats basés sur des métriques et des réponses automatisées. Par exemple, vous pouvez configurer des règles pour abandonner automatiquement les requêtes qui dépassent les limites de temps ou consomment trop de ressources.

Considérations

Lorsque vous utilisez des files d'attente sans serveur, tenez compte des points suivants :

- Les clés de configuration de gestion de la charge de travail (WLM) suivantes utilisées dans les clusters provisionnés par Amazon Redshift ne sont pas prises en charge dans les files d'attente Redshift Serverless :`max_execution_time`,,,`short_query_queue`,`auto_wlm`,,`concurrency_scaling`,`prio` `query_concurrency` `memory_percent_to_use` `user_group` `user_group_wild_card`

  De plus, les actions hop, change_query_priority ne sont pas prises en charge dans Serverless.
- L'action de saut (déplacement des requêtes entre les files d'attente) n'est pas prise en charge dans Amazon Redshift Serverless.
- Les priorités de file d'attente sont prises en charge uniquement pour les clusters provisionnés par Amazon Redshift.
- Amazon Redshift Serverless gère automatiquement la mise à l'échelle et l'allocation des ressources pour des performances optimales. Vous n'avez donc pas besoin de configurer manuellement les priorités des files d'attente.

Configuration de files d'attente de requêtes

Vous pouvez créer des files d'attente sous l'onglet Limites pour un groupe de travail sans serveur à l'aide de l' Console de gestion AWS API AWS CLI Redshift Serverless.

Console

Suivez ces étapes pour créer une file d'attente pour votre groupe de travail sans serveur.

1. Accédez à votre groupe de travail Redshift Serverless.
2. Sélectionnez l'onglet Limites.
3. Dans Query Queues, choisissez Activer les files d'attente.

> **Important**
>
> L'activation des files d'attente de requêtes est une modification permanente. Vous ne pouvez pas revenir à la surveillance sans file d'attente une fois activée.

4. Configurez vos files d'attente à l'aide des paramètres suivants :

Paramètres de niveau de file d'attente

- `name`- Identifiant de file d'attente (obligatoire, unique, non vide)
- `user_role`- Tableau de rôles utilisateur (facultatif)
- `query_group`- Tableau de groupes de requêtes (facultatif)
- `query_group_wild_card`- 0 ou 1 pour activer la correspondance des caractères génériques (facultatif)
- `user_group_wild_card`- 0 ou 1 pour activer la correspondance des caractères génériques (facultatif)
- `rules`- Tableau de règles de surveillance (facultatif)

Paramètres au niveau des règles

- `rule_name`- Identifiant unique, 32 caractères maximum (obligatoire)
- `predicate`- Tableau de conditions, 1 à 3 prédicats (obligatoire)
- `action`- « abandonner » ou « enregistrer » (obligatoire)

Paramètres au niveau du prédicat

- `metric_name`- Métrique à surveiller (obligatoire)
- `operator`- « = », « < », or « > » (obligatoire)
- `value`- Seuil numérique (obligatoire)

Restrictions

- 8 files d'attente maximum
- 25 règles maximum dans toutes les files d'attente
- 3 prédicats maximum par règle
- Les noms de règles doivent être uniques au monde

Exemple de configuration

Exemple de trois files d'attente : une pour les requêtes de tableau de bord avec un délai d'attente court, une pour les requêtes ETL avec un délai d'attente long et une file d'administration :

```
[
  {
    "name": "dashboard",
    "user_role": ["analyst", "viewer"],
    "query_group": ["reporting"],
    "query_group_wild_card": 1,
    "rules": [
      {
        "rule_name": "short_timeout",
        "predicate": [
          {
            "metric_name": "query_execution_time",
            "operator": ">",
            "value": 60
          }
        ],
        "action": "abort"
      }
    ]
  },
  {
    "name": "ETL",
    "user_role": ["data_scientist"],
    "query_group": ["analytics", "ml"],
    "rules": [
      {
        "rule_name": "long_timeout",
        "predicate": [
          {
            "metric_name": "query_execution_time",
            "operator": ">",
            "value": 3600
          }
        ],
        "action": "log"
      },
      {
        "rule_name": "memory_limit",
        "predicate": [
          {
            "metric_name": "query_temp_blocks_to_disk",
            "operator": ">",
            "value": 100000
```

```
          }
        ],
        "action": "abort"
      }
    ]
  },
  {
    "name": "admin_queue",
    "user_role": ["admin"],
    "query_group": ["admin"]
  }
]
```

Dans cet exemple :

- Les requêtes du tableau de bord sont abandonnées si elles durent plus de 60 secondes
- Les requêtes ETL sont enregistrées si elles s'exécutent pendant plus d'une heure
- La file d'attente des administrateurs n'a aucune limite de ressources

CLI

Vous pouvez gérer les files d'attente à l'aide UpdateWorkgroup des API CreateWorkgroup or avec le paramètre `wlm_json_configuration` config pour spécifier les files d'attente au format JSON.

```
aws redshift-serverless create-workgroup \
  --workgroup-name test-workgroup \
  --namespace-name test-namespace \
  --config-parameters '[{"parameterKey": "wlm_json_configuration", "parameterValue":
 "[{\"name\":\"dashboard\",\"user_role\":[\"analyst\",\"viewer\"],\"query_group
\":[\"reporting\"],\"query_group_wild_card\":1,\"rules\":[{\"rule_name\":
\"short_timeout\",\"predicate\":[{\"metric_name\":\"query_execution_time\",
\"operator\":\">\",\"value\":60}],\"action\":\"abort\"}]},{\"name\":\"ETL
\",\"user_role\":[\"data_scientist\"],\"query_group\":[\"analytics\",\"ml
\"],\"rules\":[{\"rule_name\":\"long_timeout\",\"predicate\":[{\"metric_name
\":\"query_execution_time\",\"operator\":\">\",\"value\":3600}],\"action\":
\"log\"},{\"rule_name\":\"memory_limit\",\"predicate\":[{\"metric_name\":
\"query_temp_blocks_to_disk\",\"operator\":\">\",\"value\":100000}],\"action\":
\"abort\"}]},{\"name\":\"admin_queue\",\"user_role\":[\"admin\"],\"query_group\":
[\"admin\"]}]"}]'
```

Bonnes pratiques

Gardez les bonnes pratiques suivantes à l'esprit lorsque vous utilisez des files d'attente sans serveur.

- Utilisez des files d'attente distinctes pour les charges de travail ayant des exigences de limites distinctes (par exemple, ETL, rapports ou analyses ad hoc).
- Commencez par des seuils simples et ajustez-les en fonction du comportement des requêtes et des modèles d'utilisation. Vous pouvez surveiller les modèles d'utilisation des requêtes à l'aide des tableaux et des vues décrits dans Tables et vues système pour les règles de surveillance des requêtes.

Vérification des données récapitulatives d’Amazon Redshift sans serveur à l’aide du tableau de bord

Le tableau de bord d’Amazon Redshift sans serveur contient une série de volets qui affichent en un coup d’œil des métriques et d’autres informations sur votre groupe de travail et votre espace de nom. Ces volets sont les suivants :

- Resources summary (Récapitulatif des ressources) : affiche des informations de haut niveau à propos d’Amazon Redshift sans serveur, telles que le stockage utilisé et d’autres métriques.
- Query summary (Résumé des requêtes) : affiche des informations sur les requêtes, notamment les requêtes terminées et les requêtes en cours d’exécution. Choisissez View details (Afficher les détails) pour accéder à un écran offrant des filtres supplémentaires.
- RPU capacity used (Capacité de RPU utilisée) : affiche la capacité globale utilisée sur une période donnée, comme les dix heures précédentes, par exemple.
- Partage de données : affiche le nombre de partages de données, qui sont utilisés pour partager des données entre des comptes, par exemple. AWS Les métriques indiquent les unités de partage de données nécessitant une autorisation et d’autres informations.
- Utilisation totale du calcul : indique le nombre total d’heures de RPU consommées pour le groupe de travail sélectionné sur une plage de temps sélectionnée, jusqu’aux 7 derniers jours.

À partir du tableau de bord, vous pouvez vous plonger rapidement dans ces métriques disponibles pour vérifier un détail concernant Amazon Redshift sans serveur, ou analyser des requêtes, ou encore suivre des éléments de travail.

Journalisation d’audit pour Amazon Redshift sans serveur

Vous pouvez configurer Amazon Redshift Serverless pour exporter les données des journaux de connexion, d'utilisateur et d'activité des utilisateurs vers un groupe de journaux dans Amazon Logs. CloudWatch Avec Amazon CloudWatch Logs, vous pouvez effectuer une analyse en temps réel des données du journal et les utiliser CloudWatch pour créer des alarmes et afficher des statistiques. Vous pouvez utiliser CloudWatch Logs pour stocker vos enregistrements de journaux dans un espace de stockage durable.

Vous pouvez créer des CloudWatch alarmes pour suivre vos statistiques à l'aide de la console Amazon Redshift. Pour plus d’informations sur la création d’alarmes, consultez Gérer les alarmes.

Pour exporter les données de journal générées vers Amazon CloudWatch Logs, les journaux correspondants doivent être sélectionnés pour exportation dans vos paramètres de configuration Amazon Redshift Serverless, sur la console. Vous pouvez le faire en sélectionnant les paramètres Configuration de l’espace de noms, sous Sécurité et chiffrement.

Enregistrez les événements CloudWatch

Après avoir sélectionné les journaux Redshift à exporter, vous pouvez surveiller les événements dans Amazon CloudWatch Logs. Un nouveau groupe de journaux est automatiquement créé pour Amazon Redshift sans serveur, dans lequel `log_type` représente le type de journal.

```
/aws/redshift/<namespace>/<log_type>
```

Lorsque vous créez votre premier groupe de travail et votre premier espace de noms, Par défaut est le nom de l’espace de noms. Le nom du groupe de journaux varie en fonction du nom que vous donnez à l’espace de noms.

Par exemple, si vous exportez le journal des connexions, les données du journal sont stockées dans le groupe de journaux suivant.

```
/aws/redshift/default/connectionlog
```

Les événements du journal sont exportés vers un groupe de journaux à l’aide du flux de journaux sans serveur. Le comportement dépend des conditions suivante qui sont vraies :

- Un groupe de journaux avec le nom spécifié existe. Redshift exporte les données des journaux en utilisant le groupe de journaux existant. Pour créer des groupes de journaux avec des périodes de

conservation des journaux prédéfinies, des filtres de mesures et un accès client prédéfinis, vous pouvez utiliser une configuration automatique, telle que celle fournie par. AWS CloudFormation

- Aucun groupe de journaux avec le nom spécifié n'existe. Lorsqu'une entrée de journal correspondante est détectée dans le journal de l'instance, Amazon Redshift Serverless crée automatiquement un nouveau groupe de CloudWatch journaux dans Amazon Logs. Le groupe de journaux utilise la période de rétention de journaux par défaut Never Expire (N'expire jamais). Pour modifier la période de conservation des journaux, utilisez la console Amazon CloudWatch Logs, l'API Amazon Logs ou l' AWS CLI API Amazon CloudWatch Logs. Pour plus d'informations sur la modification des périodes de conservation des CloudWatch journaux dans les journaux, voir Modifier la conservation des données des journaux dans Utilisation des groupes de journaux et des flux de journaux.

Pour rechercher des informations dans les événements du journal, utilisez la console Amazon CloudWatch Logs AWS CLI, l'API Amazon Logs ou l'API Amazon CloudWatch Logs. Pour plus d'informations sur la recherche et le filtrage des données de journaux, consultez Recherche et filtrage des données de journaux.

CloudWatch métriques

Les métriques Amazon Redshift sans serveur sont divisées en métriques de calcul et métriques de données et de stockage, relevant respectivement des ensembles de dimensions de groupe de travail et d'espace de noms. Pour plus d'informations sur les groupes de travail et les espaces de noms, consultez Groupes de travail et espaces de noms.

CloudWatch les métriques de calcul sont les suivantes :

Nom de la métrique	Uunités	Description	Jeux de dimensions
`QueriesCompletedPerSecond`	Nombre de requêtes	Nombre de requêtes terminées par seconde.	{Base de données LatencyRange, Groupe de travail}, {LatencyRange, Groupe de travail}
`QueryDuration`	Microsecondes	Durée moyenne pour exécuter une requête.	{Base de données LatencyRange, Groupe de travail},

Nom de la métrique	Uunités	Description	Jeux de dimensions
			{LatencyRange, Groupe de travail}
QueriesRunning	Nombre de requêtes	Nombre de requêtes en cours d'exécution à un moment spécifique.	{Base de données QueryType, Groupe de travail}, {QueryType, Groupe de travail}
QueriesQueued	Nombre de requêtes	Nombre de requêtes dans la file d'attente à un moment spécifique.	{Base de données QueryType, Groupe de travail}, {QueryType, Groupe de travail}
DatabaseConnections	Nombre de connexions	Nombre de connexions à une base de données à un moment spécifique.	{Database, Workgroup}, {Workgroup}
QueryRuntimeBreakdown	Millisecondes	Durée totale d'exécution des requêtes, par étape de la requête.	{Database, Stage, Workgroup}, {Stage, Workgroup}
ComputeCapacity	RPU	Nombre moyen d'unités de calcul allouées au cours des 30 dernières minutes, arrondi à l'entier le plus proche.	{Workgroup}

Nom de la métrique	Uunités	Description	Jeux de dimensions
ComputeSeconds	RPU-seconds	Secondes cumulées d'unité de calcul utilisées au cours des 30 dernières minutes.	{Workgroup}
QueriesSucceeded	Nombre de requêtes	Nombre de requêtes qui ont réussi au cours des 5 dernières minutes.	{Base de données QueryType, Groupe de travail}, {QueryType, Groupe de travail}
QueriesFailed	Nombre de requêtes	Nombre de requêtes qui ont échoué au cours des 5 dernières minutes.	{Base de données QueryType, Groupe de travail}, {QueryType, Groupe de travail}

Nom de la métrique	Uunités	Description	Jeux de dimensions
`UsageLimitAvailable`	RPU-hours ou TbS	En fonction de UsageType , UsageLimitAvailable renvoie les informations suivantes : • Si la valeur UsageType est SERVERLESS_COMPUTE , UsageLimitAvailable renvoie le nombre restant RPU-hours que le groupe de travail peut interroger dans la limite donnée. • Si la valeur UsageType est CROSS_REGION_DATASHARING, UsageLimitAvailable renvoie le nombre de To restants	{UsageLimitId, UsageType, Groupe de travail}

Nom de la métrique	Uunités	Description	Jeux de dimensions
		que le client peut scanner dans la limite spécifiée.	

Nom de la métrique	Uunités	Description	Jeux de dimensions
`UsageLimitConsumed`	RPU-hours ou TbS	En fonction de UsageType , UsageLimitConsumed renvoie les informations suivantes : • Si la valeur UsageType est SERVERLESS_COMPUTE , UsageLimitConsumed renvoie le numéro RPU-hours que le groupe de travail a déjà demandé dans la limite donnée. • Si la valeur UsageType est CROSS_REGION_DATASHARING, UsageLimitConsumed renvoie le nombre de To que le client a déjà utilisés	{UsageLimitId, UsageType, Groupe de travail}

Nom de la métrique	Uunités	Description	Jeux de dimensions
		pour scanner dans la limite spécifiée.	
`ExtraComputeForAutomaticOptimizationChargedSeconds`	RPU-seconds	Nombre de secondes d'unité de calcul facturées pour les opérations d'optimisation automatique au cours des 30 dernières minutes.	{Workgroup}

CloudWatch les mesures relatives aux données et au stockage sont les suivantes :

Nom de la métrique	Uunités	Description	Jeux de dimensions
`TotalTableCount`	Nombre de tables	Le nombre total de tables à un moment donné. Ce total inclut les tables permanentes, les tables temporaires, les tables de partage de données, les tables externes et les vues matérialisées. Les vues et les tables système	{Database, Namespace}

Nom de la métrique	Uunités	Description	Jeux de dimensions
		ne sont pas incluses dans ce décompte.	
`DataStorage`	Mégaoctets	Le nombre de mégaoctets utilisés, en disque ou en espace de stockage, pour les données Redshift.	{Espace de noms}

La `ServerlessUniqueSnapshotStorage` métrique est indépendante des espaces de noms et des groupes de travail. CloudWatchLa `ServerlessUniqueSnapshotStorage` métrique est la suivante :

Nom de la métrique	Uunités	Description	Jeux de dimensions
`ServerlessUniqueSnapshotStorage`	Mégaoctets	Nombre de mégaoctets de blocs de données uniques stockés dans tous les instantanés manuels actifs.	{}

Les jeux de dimensions sont les dimensions de regroupement appliquées à vos métriques. Vous pouvez utiliser ces groupes de dimensions pour spécifier comment vos statistiques sont extraites.

Le tableau suivant détaille les dimensions et les valeurs de dimension pour des métriques spécifiques :

Dimension	Description et valeurs
`DatabaseName`	Nom de la base de données. Une valeur personnalisée.
`Latency`	Les valeurs possibles sont les suivantes : • Court : moins de 10 secondes • Moyen : entre 10 secondes et 10 minutes • Long : plus de 10 minutes
`QueryType`	Les valeurs possibles sont : `INSERT`, `DELETE`, `UPDATE`, `UNLOAD`, `LOAD`, `SELECT`, `CTAS` et `OTHER`.
`stage`	Étapes de l'exécution d'une requête. Les valeurs possibles sont les suivantes : • QueryPlanning : Temps passé à analyser et à optimiser les instructions SQL. • QueryWaiting: temps passé à attendre dans la file d'attente du WLM. • QueryExecutingRead: temps passé à exécuter des requêtes de lecture. • QueryExecutingInsert: temps passé à exécuter des requêtes d'insertion. • QueryExecutingDelete: temps passé à exécuter des requêtes de suppression. • QueryExecutingUpdate: temps passé à exécuter des requêtes de mise à jour. • QueryExecutingCtas: temps passé à exécuter la création d'une table sous forme de requêtes. • QueryExecutingUnload: temps passé à exécuter des requêtes de déchargement.

Dimension	Description et valeurs
	• QueryExecutingCopy: temps passé à exécuter des requêtes de copie. • QueryCommit: Temps passé à s'engager.
`Namespace`	Nom de l’espace de noms. Une valeur personnalisée.
`Workgroup`	Le nom du groupe de travail. Une valeur personnalisée.
`UsageLimitId`	L’identifiant de la limite d’utilisation.
`UsageType`	La fonctionnalité Amazon Redshift sans serveur est limitée. Les valeurs possibles sont les suivantes : • SERVERLESS_COMPUTE • CROSS_REGION_DATASHARING

Instantanés et points de récupération

Une sauvegarde dans Amazon Redshift sans serveur est une représentation à un instant donné des objets et des données figurant dans votre espace de noms. Il existe deux types de sauvegardes : les instantanés créés manuellement et les points de récupération qu’Amazon Redshift sans serveur crée automatiquement pour vous.

Amazon Redshift sans serveur crée automatiquement des points de restauration toutes les 30 minutes ou tous les 5 Go de modifications de données par nœud, selon ce qui arrive en premier. Pour les jeux de données plus importants (plus de 5 Go × nombre de nœuds), l’intervalle minimal entre les points de restauration est de 15 minutes. tous les points de récupération sont conservés 24 heures.

> **Note**
>
> Vous ne pouvez pas créer votre propre planification des instantanés pour contrôler le moment où les points de restauration sont créés.

Amazon Redshift sans serveur crée des instantanés dans Redshift Managed Storage (RMS). Pour de plus amples informations, veuillez consulter Capacité de calcul pour Amazon Redshift sans serveur.

> **Note**
>
> No-backup les tables ne sont pas prises en charge pour les clusters provisionnés RG ou RA3 et les groupes de travail Amazon Redshift Serverless. Une table marquée comme sans sauvegarde dans un cluster RG ou RA3 ou un groupe de travail sans serveur est traitée comme une table permanente qui sera toujours sauvegardée lors de la prise d'un instantané, et toujours restaurée lors de la restauration à partir d'un instantané. Pour éviter les coûts liés aux instantanés pour les tables sans sauvegarde, tronquez-les avant de prendre un instantané.

Si vous souhaitez récupérer les données dans un instantané ou un point de récupération, vous pouvez restaurer un instantané dans un espace de noms sans serveur ou dans un cluster provisionné. Il existe trois scénarios dans lesquels vous pouvez restaurer des instantanés :

- Restauration d'un instantané sans serveur dans un espace de noms sans serveur.
- Restauration d'un instantané sans serveur sur un cluster mis en service.
- Restauration d'un instantané de cluster mis en service dans un espace de noms sans serveur.

Lorsque vous restaurez un instantané sans serveur sur un cluster provisionné, vous devez choisir le type de nœud à utiliser, tel que RG ou RA3, et le nombre de nœuds, ce qui vous permet de contrôler les paramètres au niveau du cluster ou du nœud.

Pour restaurer un instantané de cluster mis en service vers un espace de noms sans serveur, accédez à la console mise en service de Redshift, choisissez l'instantané à restaurer, puis sélectionnez Restore from snapshot (Restaurer à partir de l'instantané), Restore to serverless namespace (Restaurer vers l'espace de noms sans serveur). Amazon Redshift convertit les tables avec des clés entrelacées en clés de tri composées lorsque vous restaurez un instantané de cluster

provisionné dans un espace de noms sans serveur. Pour plus d'informations sur les clés de tri, consultez Utilisation des clés de tri.

Si vous souhaitez ajouter un contexte supplémentaire, vous pouvez baliser les instantanés et les points de restauration à l'aide de paires clé-valeur qui fournissent des métadonnées et des informations aux instantanés et aux points de restauration. Pour plus d'informations sur le balisage des ressources, consultez Aperçu des ressources de balisage.

Enfin, vous pouvez également partager des instantanés avec d'autres AWS comptes, ce qui leur permet d'accéder aux données contenues dans l'instantané et d'exécuter des requêtes.

AWS Backup intégration

Vous pouvez également créer et restaurer des instantanés à l'aide AWS Backup d'un service entièrement géré qui vous permet de centraliser et d'automatiser la protection des données entre les AWS services, dans le cloud et sur site. Pour de plus amples informations, veuillez consulter AWS Backup intégration avec Amazon Redshift. Pour plus d'informations AWS Backup, voir Qu'est-ce que c'est AWS Backup ? dans le Guide AWS Backup du développeur.

Création d'un instantané

> **Note**
>
> No-backup les tables ne sont pas prises en charge pour les clusters provisionnés RG ou RA3 et les groupes de travail Amazon Redshift Serverless. Une table marquée comme sans sauvegarde dans un cluster RG ou RA3 ou un groupe de travail sans serveur est traitée comme une table permanente qui sera toujours sauvegardée lors de la prise d'un instantané, et toujours restaurée lors de la restauration à partir d'un instantané. Pour éviter les coûts liés aux instantanés pour les tables sans sauvegarde, tronquez-les avant de prendre un instantané.

Pour créer un instantané, suivez les étapes de la procédure suivante.

Pour créer un instantané

1. Sur la console Amazon Redshift sans serveur, choisissez Data backup (Sauvegarde de données).
2. Choisissez Créer un instantané.

3. Choisissez un espace de noms pour créer un instantané.
4. Entrez un identifiant d’instantané.
5. (Facultatif) Choisissez une période de rétention. Si vous choisissez Custom value (Valeur personnalisée), choisissez le nombre de jours. Le nombre que vous choisissez doit être compris entre 1 et 3 653 jours, inclus. La valeur par défaut permet de conserver indéfiniment les données.
6. Choisissez Créer.

Pour créer un instantané à partir de la configuration de l’espace de noms

1. Sur la console Amazon Redshift sans serveur, choisissez Namespace configuration (Configuration de l’espace de noms).
2. Choisissez l’espace de noms à partir duquel vous souhaitez créer un instantané. Vous pouvez uniquement créer des instantanés d’espaces de noms associés à un groupe de travail et dont l’état est Available (Disponible).
3. Cliquez sur l’onglet Data backup (Sauvegarde des données).
4. Choisissez Créer un instantané.
5. Entrez un identifiant d’instantané.
6. (Facultatif) Choisissez une période de rétention. Si vous choisissez Custom value (Valeur personnalisée), choisissez le nombre de jours. Le nombre que vous choisissez doit être compris entre 1 et 3 653 jours, inclus.
7. Choisissez Créer.

Création d’un instantané final

Pour créer un instantané final de toutes les données dans un espace de noms avant de supprimer l’espace de noms, suivez les étapes de la procédure suivante.

Pour créer un instantané final.

1. Sur la console Amazon Redshift sans serveur, choisissez Namespace configuration (Configuration de l’espace de noms).
2. Choisissez l’espace de noms à supprimer.
3. Sélectionnez Actions, Supprimer.

4. Sélectionnez Create final snapshot (Créer un instantané final).
5. Entrez un nom pour l'instantané.
6. Saisissez « delete » (supprimer).
7. Sélectionnez Delete (Supprimer).

Partage d'un instantané ou suppression des autorisations relatives aux instantanés

Pour partager un instantané avec un autre AWS compte ou supprimer l'accès d'un compte à un instantané, effectuez la procédure suivante.

Pour partager un instantané ou supprimer l'accès à celui-ci

1. Sur la console Amazon Redshift sans serveur, choisissez Data backup (Sauvegarde de données).
2. Choisissez un instantané à partager.
3. Choisissez Action, Manage access (Gérer l'accès).
4. Pour partager un instantané avec un autre compte, saisissez un ID de Compte AWS . Pour retirer l'accès d'un compte, choisissez Retirer.
5. Sélectionnez Enregistrer les modifications.

Planification d'un instantané

Pour contrôler avec précision à quel moment prendre un instantané, vous pouvez créer une planification d'instantané pour des espaces de noms spécifiques. Lorsque vous planifiez la création d'un instantané, vous pouvez créer un événement ponctuel ou utiliser des expressions cron Unix pour créer un calendrier récurrent. Les expressions cron prennent en charge trois champs séparés par un espace.

```
cron(Minutes Hours Day-of-month Month Day-of-week Year)
```

Champs	Valeurs	Caractères génériques
Minutes	0–59	, - * /

Champs	Valeurs	Caractères génériques
Heures	0 – 23	, - * /
Day-of-month	1–31	, - * ? / L W
Mois	1 à 12 ou JAN-DEC	, - * /
Day-of-week	1 à 7 ou SUN-SAT	, - * ? L #
Année	1970-2199	, - * /

Caractères génériques

- Le caractère générique , (virgule) inclut des valeurs supplémentaires. Dans le champ `Day-of-week`, `MON,WED,FRI` correspond à lundi, mercredi et vendredi. Le nombre total de valeurs est limité à 24 par champ.
- Le caractère générique - (tiret) spécifie des plages. Dans le champ `Hour`, 1–15 correspond aux heures 1 à 15 du jour spécifié.
- Le caractère générique * (astérisque) inclut toutes les valeurs du champ. Dans le champ `Hours`, * inclut chaque heure.
- Le caractère générique / (barre oblique) spécifie les incréments. Dans le champ `Hours`, vous pouvez saisir **`1/10`** pour spécifier toutes les 10 heures à partir de la première heure de la journée (par exemple, 01 h 00, 11 h 00 et 21 h 00).
- Le caractère générique ? (point d'interrogation) indique l'un ou l'autre. Dans le `Day-of-month` champ, vous pouviez entrer 7, et si vous ne vous souciiez pas de savoir quel jour de la semaine se situait le 7, vous pouviez entrer ? sur le Day-of-week terrain.
- Le caractère générique L dans les champs ou spécifie le dernier jour du mois ou de la semaine.`Day-of-monthDay-of-week`
- Le caractère générique W dans le champ spécifie un jour de la semaine. `Day-of-month` Dans le champ `Day-of-month`, `3W` spécifie le jour le plus proche du troisième jour de semaine du mois.
- Le caractère générique # dans le Day-of-week champ spécifie une certaine instance du jour de la semaine spécifié au cours d'un mois. Par exemple, 3#2 correspond au deuxième mardi du mois : le 3 fait référence à mardi, car c'est le troisième jour de chaque semaine, et le 2 fait référence à la deuxième journée de ce type dans le mois.

> **Note**
>
> Si vous utilisez un caractère « # », vous ne pouvez définir qu'une seule expression dans le champ « day-of-week » (jour de la semaine). Par exemple, « 3#1,6#3 » n'est pas valide, car il est interprété comme deux expressions.

Restrictions

- Vous ne pouvez pas spécifier les champs `Day-of-month` et `Day-of-week` de la même expression cron. Si vous spécifiez une valeur dans l'un de ces champs, vous devez utiliser un signe ? (point d'interrogation) dans l'autre.
- Les programmes d'instantanés ne prennent pas en charge les fréquences suivantes :
  - Instantanés programmés à une fréquence supérieure à 1 par heure.
  - Instantanés programmés à une fréquence inférieure à 1 par jour (24 heures).

  Si des planifications se chevauchent et entraînent la planification de plusieurs instantanés dans une fenêtre d'une heure, une erreur de validation se produit.

Le tableau suivant contient quelques exemples de chaînes cron.

Minutes	Heures	Jour de la semaine	Signification
0	14- 20/1	TUE	Mardi, toutes les heures entre 14 h 00 et 20 h 00.
0	21	MON-FRI	Tous les soirs à 21 h 00 du lundi au vendredi.
30	0/6	SAT-SUN	Le samedi et le dimanche, toutes les 6 heures, 30 minutes

Minutes	Heures	Jour de la semaine	Signification			
			après minuit (00 h 30). Le résultat est un instantané chaque jour à 00 h 30, 06 h 30, 12 h 30 et 18 h 30.			
30	12/4	*	Tous les jours, toutes les 4 heures à partir de 12 h 30. Cela équivaut à 12 h 30, 16 h 30, 20 h 30.			

L'exemple suivant montre comment créer une planification qui se déroule par tranches de 2 heures à partir de 15 h 15 chaque jour.

```
cron(15 15/2 *)
```

Vous pouvez utiliser la console Amazon Redshift Serverless, l'API ou créer un calendrier AWS CLI de capture d'écran.

Pour planifier un instantané

1. Sur la console Amazon Redshift sans serveur, choisissez Data backup (Sauvegarde de données).
2. Choisissez Planification des instantanés.
3. Choisissez Créer une planification.
4. Entrez un nom pour la planification des instantanés.
5. Sélectionnez l'espace de noms pour lequel vous souhaitez créer des instantanés.
6. Entrez une expression cron pour la planification ou utilisez le générateur de planification pour en créer une.

7. (Facultatif) Choisissez une période de rétention. Si vous choisissez Valeur personnalisée, spécifiez le nombre de jours.
8. Choisissez Créer une planification.

Mise à jour d’une période de conservation des instantanés

Pour mettre à jour la période de conservation des instantanés, procédez comme suit.

Pour mettre à jour la période de conservation des instantanés

1. Sur la console Amazon Redshift sans serveur, choisissez Data backup (Sauvegarde de données).
2. Choisissez un instantané à mettre à jour.
3. Choisissez Actions, Set manual snapshot settings (Définir les paramètres manuels des instantanés).
4. Choisissez une période de conservation. Si vous choisissez Custom value (Valeur personnalisée), choisissez le nombre de jours.
5. Sélectionnez Enregistrer les modifications.

Suppression d'un instantané

Pour supprimer un instantané, utilisez la procédure suivante.

Pour supprimer un instantané

> **Note**
>
> Vous ne pouvez pas supprimer un instantané qui a été partagé avec un autre compte. Vous devez d’abord retirer l’accès de ce compte à l’instantané avant de supprimer l’instantané.

1. Sur la console Amazon Redshift sans serveur, choisissez Data backup (Sauvegarde de données).
2. Choisissez un instantané à supprimer.
3. Sélectionnez Actions, Supprimer.

4. Sélectionnez Supprimer.

Restauration d’un instantané

> **Note**
>
> No-backup les tables ne sont pas prises en charge pour les clusters provisionnés RG ou RA3 et les groupes de travail Amazon Redshift Serverless. Une table marquée comme sans sauvegarde dans un cluster RG ou RA3 ou un groupe de travail sans serveur est traitée comme une table permanente qui sera toujours sauvegardée lors de la prise d'un instantané, et toujours restaurée lors de la restauration à partir d'un instantané. Pour éviter les coûts liés aux instantanés pour les tables sans sauvegarde, tronquez-les avant de prendre un instantané.

La restauration d’un instantané dans un espace de noms sans serveur remplace la base de données actuelle par la base de données de l’instantané.

La restauration d’un instantané dans un espace de noms sans serveur se fait en deux phases. La première phase se termine en quelques minutes, restaure les données dans votre espace de noms et les rend disponibles pour les requêtes. La deuxième phase de la restauration permet le réglage de votre base de données, ce qui peut entraîner des problèmes de performance mineurs. Cette deuxième phase peut durer de quelques heures à plusieurs jours, voire quelques semaines dans certains cas. Le temps nécessaire dépend de la taille des données, mais les performances s’améliorent progressivement au fur et à mesure que la base de données est optimisée. À la fin de cette phase, votre espace de noms sans serveur est entièrement réglé et vous pouvez soumettre des requêtes sans subir de problèmes de performances.

Pour restaurer un instantané dans un espace de noms sans serveur

1. Sur la console Amazon Redshift sans serveur, choisissez Data backup (Sauvegarde de données).
2. Choisissez l’instantané à restaurer. Vous ne pouvez restaurer qu’un seul instantané à la fois.
3. Choisissez Actions, Restore to serverless namespace (Restaurer l’espace de noms sans serveur).
4. Choisissez un espace de noms disponible pour la restauration. Vous ne pouvez restaurer que les espaces de noms dont l’état est Available (Disponible).

5. Choisissez Restore (Restaurer).

Pour restaurer un instantané sur un cluster approvisionné

1. Sur la console Amazon Redshift sans serveur, choisissez Data backup (Sauvegarde de données).
2. Choisissez un instantané à restaurer.
3. Choisissez Action, Restore to provisioned cluster (Restaurer le cluster mis en service).
4. Entrez un identifiant de cluster.
5. Choisissez un Node type (Type de nœud). Le nombre de nœuds dépend du type de nœud.
6. Suivez les instructions de la page de la console pour entrer les propriétés du champ Cluster configuration (Configuration du cluster). Pour plus d'informations, consultez Création d'un cluster.

Pour plus d'informations sur les instantanés dans des clusters provisionnés, consultez Instantanés et sauvegardes Amazon Redshift.

Conversion d'un point de récupération

Les points de récupération d'Amazon Redshift sans serveur sont créés toutes les 30 minutes environ et enregistrés pendant 24 heures. Pour convertir un point de récupération en instantané, suivez les étapes de la procédure suivante.

Pour convertir un point de récupération en instantané

1. Sur la console Amazon Redshift sans serveur, choisissez Data backup (Sauvegarde de données).
2. Sous Recovery points (Points de récupération), choisissez l'heure de création du point de récupération que vous souhaitez convertir en instantané.
3. Choisissez Create snapshot from recovery point (Créer un instantané à partir d'un point de récupération).
4. Entrez un identifiant d'instantané.
5. Choisissez Créer.

Restauration d’un point de récupération

Les points de récupération d’Amazon Redshift sans serveur sont créés toutes les 30 minutes environ et enregistrés pendant 24 heures. Pour restaurer un point de récupération dans un espace de noms sans serveur, suivez les étapes dans la procédure suivante

Pour restaurer un point de récupération dans un espace de noms sans serveur

1. Sur la console Amazon Redshift sans serveur, choisissez Data backup (Sauvegarde de données).
2. Sous Recovery points (Points de récupération), choisissez l’heure de création du point de récupération que vous souhaitez restaurer.
3. Choisissez Restore (Restaurer). Vous ne pouvez restaurer que les espaces de noms dont l’état est Available (Disponible).
4. Entrez restore dans le champ de saisie de texte et choisissez Restore (Restaurer).

Copier des sauvegardes vers un autre Région AWS

Vous pouvez configurer Amazon Redshift Serverless pour copier automatiquement les instantanés et les points de restauration vers un autre. Région AWS Lorsque vous créez un instantané dans la Région AWSsource, il est copié dans une région de destination. Vous pouvez configurer votre espace de noms de manière à ce qu'il copie uniquement les instantanés et les points de restauration vers une seule destination Région AWS à la fois. Pour obtenir la liste des sites Régions AWS où Amazon Redshift Serverless est disponible, consultez les points de terminaison répertoriés pour l'API Redshift Serverless dans le. Référence générale d'Amazon Web Services

Lorsque vous configurez la copie des sauvegardes, vous pouvez également spécifier une période de conservation pendant laquelle Amazon Redshift sans serveur doit conserver l’instantané copié. Vous ne pouvez pas modifier la période de conservation des points de récupération, qui doit être d’un jour. La période de conservation des instantanés dans la région de destination est distincte de celle des instantanés dans la région source. Par défaut, la période de conservation stipule de conserver l’instantané indéfiniment. Si vous choisissez Valeur personnalisée, choisissez le nombre de jours. Le nombre que vous choisissez doit être compris entre 1 et 3 653 jours, limites incluses.

Pour modifier la région de destination dans laquelle copier les instantanés, commencez par désactiver la copie des sauvegardes, puis spécifiez la nouvelle région de destination lorsque vous réactivez la copie.

Une fois qu'un instantané ou un point de récupération est copié dans une région de destination, vous pouvez l'utiliser pour restaurer les données dans cette région.

Par défaut, vos données sont cryptées à l'aide d'une clé qui les AWS gère pour vous. Pour utiliser une autre clé, choisissez celle que vous souhaitez utiliser lors de la configuration de la copie de sauvegarde dans la source Région AWS, et Amazon Redshift Serverless créera automatiquement une autorisation qui active le chiffrement des instantanés dans la destination. Région AWS

Pour copier des sauvegardes dans une autre région, assurez-vous de disposer des autorisations IAM suivantes :

```
redshift-serverless:CreateSnapshotCopyConfiguration
redshift-serverless:UpdateSnapshotCopyConfiguration
redshift-serverless:ListSnapshotCopyConfigurations
redshift-serverless:DeleteSnapshotCopyConfiguration
```

Si vous utilisez votre propre clé KMS pour chiffrer vos sauvegardes, vous devez également disposer des autorisations suivantes :

```
kms:CreateGrant
kms:DescribeKey
```

Pour configurer la copie de vos instantanés ou de vos points de récupération dans une autre Région AWS

1. Dans la console Amazon Redshift sans serveur, choisissez l'espace de noms pour lequel vous souhaitez configurer la copie des instantanés et des points de récupération.
2. Choisissez Actions, puis Configuration de la sauvegarde entre régions.
3. Choisissez la destination Région AWS vers laquelle copier le cliché.
4. (Facultatif) Choisissez la durée de conservation de l'instantané. Si vous choisissez Valeur personnalisée, choisissez le nombre de jours. Le nombre que vous choisissez doit être compris entre 1 et 3 653 jours, limites incluses. La valeur par défaut stipule de conserver indéfiniment les données.
5. (Facultatif) Choisissez une autre AWS KMS clé à utiliser pour chiffrer dans la région de destination.
6. Choisissez Save configuration.

Restauration d’une table

Vous pouvez également restaurer une table spécifique à partir d’un instantané ou d’un point de récupération. Dans ce cas, vous spécifiez l’instantané ou le point de récupération source, la base de données, le schéma, la table, la base de données cible, le schéma et le nom de la nouvelle table. Cette nouvelle table ne peut pas porter le même nom qu’une table existante. Si vous souhaitez remplacer une table existante en restaurant une table, vous devez d’abord renommer ou supprimer la table avant de restaurer la table.

> **Note**
>
> No-backup les tables ne sont pas prises en charge pour les clusters provisionnés RG ou RA3 et les groupes de travail Amazon Redshift Serverless. Une table marquée comme sans sauvegarde dans un cluster RG ou RA3 ou un groupe de travail sans serveur est traitée comme une table permanente qui sera toujours sauvegardée lors de la prise d'un instantané, et toujours restaurée lors de la restauration à partir d'un instantané. Cependant, la restauration sélective de tables sans sauvegarde n’est pas prise en charge.

La table cible est créée à l’aide des définitions de colonne de la table source, des attributs de table et des attributs de colonne à l’exception des clés étrangères. Pour éviter les conflits liés aux dépendances, la table cible n’hérite pas les clés étrangères de la table source. Toutes les dépendances, telles que les vues ou les autorisations accordées sur la table source, ne sont pas appliquées à la table cible.

Si le propriétaire de la table source existe, l’utilisateur est le propriétaire de la table restaurée, à condition que l’utilisateur dispose des autorisations suffisantes pour devenir le propriétaire d’une relation du schéma et de la base de données spécifiés. Sinon, la table restaurée appartient à l’administrateur qui a été créé lorsque le cluster a été lancé.

La table restaurée retourne à l’état où elle était au moment de la sauvegarde. Cela inclut les règles de visibilité des transactions, définies par l’adhésion d’Amazon Redshift au principe d’isolement sérialisable, qui signifie que les données sont immédiatement visibles des transactions en cours démarrées après la sauvegarde.

Vous pouvez utiliser la console Amazon Redshift sans serveur pour restaurer des tables à partir d’un instantané.

La restauration d’une table à partir d’une sauvegarde de données présente les limitations suivantes :

- Vous ne pouvez restaurer qu'une seule table à la fois.
- Toutes les dépendances, telles que les vues ou les autorisations accordées sur la table source, ne sont pas appliquées à la table cible.
- Si la sécurité au niveau des lignes est activée pour une table en cours de restauration, Amazon Redshift sans serveur restaure la table dans les mêmes conditions, avec la sécurité au niveau des lignes activée.

Pour restaurer une table à l'aide de la console Amazon Redshift sans serveur

1. Sur la console Amazon Redshift sans serveur, choisissez Data backup (Sauvegarde de données).
2. Choisissez l'instantané ou le point de récupération contenant la table à restaurer.
3. Choisissez Actions, Restaurer la table à partir d'un instantané ou Restaurer la table à partir d'un point de récupération.
4. Saisissez les informations sur l'instantané ou le point de récupération source et la table cible, puis choisissez Restaurer la table.

Partage de données dans Amazon Redshift sans serveur

Grâce au partage des données, vous disposez d'un accès direct aux données afin que vos utilisateurs puissent consulter les informations les plus récentes et les plus cohérentes au fur et à mesure qu'elles sont mises à jour dans Amazon Redshift sans serveur..

Vous pouvez partager des données à des fins de lecture entre différentes instances Amazon Redshift sans serveur dans ou entre des Comptes AWS.

Vous pouvez commencer à partager des données à l'aide de l'interface SQL ou de la console Amazon Redshift. Pour plus d'informations, consultez Partage de données dans Amazon Redshift dans le Guide du développeur de base de données Amazon Redshift.

Grâce au partage de données, les espaces de noms Amazon Redshift Serverless et les clusters provisionnés peuvent partager des données en direct entre eux, qu'elles se trouvent au sein d'un cluster ou d'un cluster à Compte AWS l' Comptes AWS autre. Régions AWS Pour plus d'informations, consultez Régions où le partage de données est disponible.

Pour commencer à partager des données au sein d'un Compte AWS, ouvrez le Console de gestion AWS, puis choisissez la console Amazon Redshift. Choisissez Configuration de l’espace de noms, puis Unités de partage des données.

Pour commencer à interroger les données dans une unité de partage des données, créez une base de données dans un espace de noms auquel est associé un groupe de travail. À partir d’une unité de partage des données spécifiée, choisissez un espace de noms auquel est associé un groupe de travail et créez une base de données pour interroger les données.

Considérations

Voici des considérations relatives à l’utilisation du partage de données dans Amazon Redshift sans serveur :

- Amazon Redshift prend en charge le partage de données en tant que producteurs ou consommateurs sur des clusters RG et RA3 provisionnés et des groupes de travail de terminaux sans serveur.
- Amazon Redshift sans serveur est chiffré par défaut.

Pour obtenir la liste des limites de l’unité de partage des données, notamment les objets de base de données pris en charge, les exigences en matière de chiffrement et les exigences en matière de clés de tri, consultez Éléments à prendre en compte lors de l’utilisation du partage de données dans Amazon Redshift. dans le Guide du développeur de base de données Amazon Redshift.

Octroi d’un accès pour afficher des unités de partage des données

Un super-utilisateur peut fournir un accès à des utilisateurs qui ne sont pas des super-utilisateurs afin qu’ils puissent afficher les unités de partage des données créées par tous les utilisateurs.

Pour fournir un accès à une unité de partage des données à un utilisateur, utilisez la commande suivante pour fournir un accès à l’unité de partage des données à un utilisateur, où datashare_name correspond au nom de l’unité de partage des données et user-name correspond au nom de l’utilisateur auquel vous souhaitez fournir un accès.

```
grant share on datashare datashare_name to "IAM:test_user";
```

Pour accorder l’accès à une unité de partage des données pour un groupe d’utilisateurs, créez d’abord un groupe d’utilisateurs avec des utilisateurs. Pour plus d’informations sur la création de groupes d’utilisateurs, consultez CREATE GROUP. Accordez ensuite l’accès à l’unité de partage des

données à un utilisateur à l'aide de la commande suivante, où datashare_name correspond au nom de l'unité de partage des données et user-group correspond au nom du groupe d'utilisateurs auquel vous souhaitez accorder l'accès.

```
grant share on datashare datashare_name to group user_group;
```

Pour plus d'informations sur l'utilisation de l'instruction GRANT, consultez GRANT.

Enregistrement d'espaces de noms dans le AWS Glue Data Catalog

Vous pouvez enregistrer des espaces de noms complets dans AWS Glue Data Catalog et créer des catalogues gérés par. AWS Glue Vous pouvez accéder à ces catalogues avec n'importe quel moteur SQL prenant en charge l'API REST d'Apache Iceberg. Pour plus d'informations sur la création de Iceberg-compatible catalogues Apache à partir d'Amazon Redshift, consultez la section Compatibilité d'Apache Iceberg avec Amazon Redshift dans le Amazon Redshift Database Developer Guide.

Pour enregistrer un espace de noms sans serveur dans le AWS Glue Data Catalog

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Redshift sans serveur. Le tableau de bord sans serveur s'affiche. Cette Namespaces/Workgroups section contient la liste des espaces de noms et des groupes de travail actuels pour votre compte. Région AWS Si vous n'avez aucun espace de noms, choisissez Créer un groupe de travail pour créer un groupe de travail et l'espace de noms correspondant.
3. Choisissez le nom de l'espace de noms que vous voulez enregistrer.
4. Dans Actions, choisissez S'inscrire pour AWS Glue Data Catalog. La fenêtre contextuelle Enregistrer auprès du AWS Glue Data Catalog s'affiche.
5. Entrez l'ID de AWS compte sur lequel vous souhaitez enregistrer l'espace de noms sous ID de compte de destination. Il s'agit de l'identifiant de compte qui contiendra le catalogue dans le AWS Glue Data Catalog.
6. Entrez un nom sous Enregistrer l'espace de noms en tant que. Il s'agira du nom de l'espace de noms dans le Catalogue de données.
7. Choisissez S'inscrire. Vous serez redirigé vers la AWS Lake Formation console.
8. Suivez le processus de création du catalogue dans AWS Lake Formation. Pour plus d'informations sur la création d'un catalogue, consultez Intégration des données Amazon Redshift dans le AWS Glue Data Catalog dans le Guide du développeur AWS Lake Formation .

Étiquetage des ressources Amazon Redshift sans serveur

Dans AWS, les balises sont des étiquettes définies par l'utilisateur qui se composent de paires clé-valeur. Amazon Redshift Serverless prend en charge le balisage pour fournir des métadonnées sur les ressources en un coup d'œil.

Les balises ne sont pas nécessaires pour les ressources, mais elles permettent de fournir un contexte. Vous pourriez souhaiter baliser des ressources avec des métadonnées contenant des informations relatives à la ressource. Par exemple, supposons que vous souhaitiez suivre quelles ressources appartiennent à un environnement de test et quelles ressources appartiennent à un environnement de production. Vous pourriez créer une clé nommée « environnement » et fournir la valeur test ou production pour identifier les ressources utilisées dans chaque environnement. Si vous utilisez le balisage dans d'autres AWS services ou si vous avez des catégories standard pour votre entreprise, nous vous recommandons de créer les mêmes paires clé-valeur pour les ressources, par souci de cohérence.

Si vous supprimez une ressource, les balises associées sont supprimées. Vous pouvez utiliser à la fois la console Serverless AWS CLI et Amazon Redshift pour baliser les ressources sans serveur. Les opérations disponibles sont `TagResource`, `UntagResource` et `ListTagsForResource`.

Chaque ressource possède un ensemble de balises, lequel constitue un ensemble d’une ou de plusieurs balises affectées à la ressource. Chaque ressource peut avoir jusqu’à 50 balises par ensemble de balises. Vous pouvez ajouter des balises lorsque vous créez une ressource et après qu'une ressource a été créée. Vous pouvez ajouter des balises aux types de ressources sans serveur suivants :

- Groupes de travail
- Espaces de noms
- Instantanés
- Points de récupération

Les balises possèdent les exigences suivantes :

- Les clés ne peuvent pas être préfixées par `aws:`.
- Les clés doivent être uniques par ensemble de balises.
- Une clé doit comporter entre 1 et 128 caractères autorisés.
- Une valeur doit comprendre entre 0 et 256 caractères autorisés.

- Les valeurs ne doivent pas être uniques par ensemble de balises.
- Les caractères autorisés pour les clés et les valeurs sont les lettres Unicode, les chiffres, les espaces et les symboles suivants : _ . : / = + - @.
- Les clés et les valeurs sont sensibles à la casse.

Pour gérer les étiquettes de vos ressources Amazon Redshift

1. Sur la console Amazon Redshift Serverless, choisissez Data backup (Sauvegarde de données).
2. Entrez le type de ressource à rechercher et choisissez Rechercher des ressources. Choisissez la ressource pour laquelle vous souhaitez gérer les balises, puis Manage tags (Gérer les balises).
3. Spécifiez les clés et les valeurs facultatives que vous souhaitez ajouter à la ressource. Lorsque vous modifiez une balise, vous pouvez modifier la valeur de la balise, mais pas la clé.
4. Une fois que vous avez terminé d'ajouter, de supprimer ou de modifier des balises, choisissez Enregistrer les modifications, puis choisissez Appliquer pour enregistrer vos modifications.

Clusters Amazon Redshift provisionnés

Un entrepôt des données Amazon Redshift est un ensemble de ressources informatiques appelées nœuds, qui sont organisées en un groupe appelé cluster. Chaque cluster exécute un moteur Amazon Redshift et contient une ou plusieurs bases de données.

> **Note**
>
> À ce jour, le moteur Amazon Redshift version 1.0 est disponible. Toutefois, à mesure que le moteur est mis à jour, plusieurs versions du moteur Amazon Redshift peuvent être disponibles pour la sélection.

Clusters et nœuds dans Amazon Redshift

Un cluster Amazon Redshift est constitué de nœuds. Chaque cluster possède un nœud principal et un ou plusieurs nœuds de calcul. Le nœud principal reçoit les requêtes d'applications clientes, analyse les requêtes et développe les plans d'exécution de requête. Le nœud principal coordonne ensuite l'exécution parallèle de ces plans avec les nœuds de calcul et regroupe les résultats intermédiaires de ces nœuds. Enfin, il renvoie ensuite les résultats aux applications clientes.

Les nœuds de calcul exécutent les plans d'exécution de requête et communiquent les données entre eux afin de traiter ces requêtes. Les résultats intermédiaires sont renvoyés au nœud « leader » afin d'être compilés, puis transmis aux applications clientes. Pour plus d'informations sur les nœuds principaux et les nœuds de calcul, consultez Architecture du système d'entrepôt des données dans le Guide du développeur de la base de données Amazon Redshift.

> **Note**
>
> Lorsque vous créez un cluster sur la console Amazon Redshift (https://console.aws.amazon.com/redshiftv2/), vous pouvez obtenir une recommandation concernant la configuration de votre cluster en fonction de la taille de vos données et des caractéristiques de vos requêtes. Pour utiliser ce calculateur de dimensionnement, recherchez Aidez-moi à choisir sur la console dans AWS Régions prenant en charge les types de nœuds RG ou RA3. Pour de plus amples informations, veuillez consulter Création d'un cluster.

Lorsque vous lancez un cluster, vous spécifiez notamment l'option correspondant au type de nœud. Le type de nœud détermine l'UC, la RAM, la capacité de stockage et le type de disque de stockage de chaque nœud.

Amazon Redshift propose différents types de nœuds pour s'adapter à vos charges de travail, et nous vous recommandons de choisir RG ou RA3 en fonction des performances requises, de la taille des données et de la croissance attendue des données.

Les nœuds RG et RA3 dotés d'un stockage géré vous permettent d'optimiser votre entrepôt de données en adaptant et en payant indépendamment le calcul et le stockage géré. Avec RG ou RA3, vous choisissez le nombre de nœuds en fonction de vos exigences de performances et vous ne payez que pour le stockage géré que vous utilisez. Dimensionnez votre cluster RG ou RA3 en fonction de la quantité de données que vous traitez quotidiennement. Vous lancez des clusters qui utilisent les types de nœuds RG ou RA3 dans un cloud privé virtuel (VPC). Pour de plus amples informations, veuillez consulter Création d'un cluster alloué Amazon Redshift ou d'un groupe de travail Amazon Redshift sans serveur dans un VPC.

Le stockage géré Amazon Redshift utilise de grands SSD hautes performances dans chaque nœud RG et RA3 pour un stockage local rapide et Amazon S3 pour un stockage durable à long terme. Si les données d'un nœud dépassent la taille des grands SSD locaux, le stockage géré d'Amazon Redshift décharge automatiquement ces données sur Amazon S3. Vous payez le même tarif avantageux pour le stockage géré par Amazon Redshift, que les données se trouvent dans des disques SSD haute performance ou dans Amazon S3. Pour les charges de travail qui nécessitent un stockage grandissant, le stockage géré vous permet de faire mettre à l'échelle automatiquement la capacité de stockage de votre entrepôt des données séparément des nœuds de calcul.

Les nœuds RG fournissent les fonctionnalités suivantes par rapport aux types de nœuds RA3 :

- Graviton-based types d'instances : offrez des performances tarifaires supérieures pour les charges de travail analytiques
- Moteur de requêtes de lac de données intégré : les clusters RG incluent un moteur de requête de lac de données intégré qui s'exécute directement sur les ressources de calcul du cluster. Les clusters RA3 utilisent Amazon Redshift Spectrum pour les requêtes sur les lacs de données.

Les nœuds DC2 vous permettent de posséder des entrepôts des données gourmands en calcul avec stockage SSD local inclus. Vous choisissez le nombre de nœuds dont vous avez besoin en fonction de la taille des données et des exigences en matière de performance. Les nœuds DC2 stockent vos données localement pour des performances élevées et, alors que la taille des données grandit, vous

pouvez ajouter plus de nœuds de calcul afin d'augmenter la capacité de stockage du cluster. Pour les ensembles de données de 1 To (compressé), nous vous recommandons les types de nœuds DC2 qui vous permettent de bénéficier des meilleures performances au prix le plus bas. Si vous souhaitez voir vos données grandir, nous vous recommandons d'utiliser les nœuds RA3. De cette manière, vous pouvez dimensionner le calcul et le stockage indépendamment afin de bénéficier de tarifs et de performances amélioré(s). Les clusters utilisant les types de nœuds DC2 sont lancés dans un cloud privé virtuel (VPC). Pour plus d'informations, consultez Création d'un cluster alloué Amazon Redshift ou d'un groupe de travail Amazon Redshift sans serveur dans un VPC.

Les types de nœuds sont disponibles en différentes tailles. La taille de nœud et le nombre de nœuds de déterminent le stockage total d'un cluster. Pour plus d'informations, consultez Détails de type de nœud.

Certains types de nœud autorisent un nœud (type à nœud unique) ou deux ou plusieurs nœuds (type à plusieurs nœuds). Le nombre minimum de nœuds pour les clusters de certains types de nœuds est de deux nœuds. Sur un cluster à nœud unique, le nœud est partagé pour les fonctionnalités de leader et de calcul. Single-node les clusters ne sont pas recommandés pour exécuter des charges de travail de production. Sur un cluster à plusieurs nœuds, le nœud principal est distinct des nœuds de calcul. Le nœud de ligne est le même type de nœud que les nœuds de calcul. Vous ne payez que pour les nœuds de calcul.

Amazon Redshift applique des quotas de ressources pour chaque AWS compte dans chaque AWS région. Un quota limite le nombre de ressources que votre compte peut créer pour un type de ressource donné, tel que des nœuds ou des instantanés, au sein d'une AWS région. Pour plus d'informations sur les quotas par défaut qui s'appliquent aux ressources Amazon Redshift, consultez Quotas et limites d'Amazon Redshift.

Le coût de votre cluster dépend de la AWS région, du type de nœud, du nombre de nœuds et de la réservation préalable des nœuds. Pour plus d'informations sur le coût des nœuds, consultez la page de Tarification d'Amazon Redshift.

Détails de type de nœud

Les tableaux suivants résument les spécifications de nœud de chaque type de nœud et taille. Les en-têtes dans les tableaux ont les significations suivantes :

- vCPU correspond au nombre de processeurs virtuels de chaque nœud.
- RAM correspond à la quantité de mémoire en gibioctets (Gio) de chaque nœud.

- Tranches par nœud est le nombre de tranches dans lesquelles un nœud de calcul est partitionné lorsqu'un cluster est créé ou redimensionné avec un redimensionnement classique.

  Le nombre de sections par nœud peut changer si le cluster est redimensionné à l'aide du redimensionnement Elastic. Cependant, le nombre total de tranches sur tous les nœuds de calcul dans le cluster reste le même après le redimensionnement élastique.

  Lorsque vous créez un cluster avec l'opération de restauration à partir d'un instantané, le nombre de tranches du cluster résultant peut changer par rapport au cluster d'origine si vous modifiez le type de nœud.
- Stockage correspond à la capacité et au type de stockage de chaque nœud.
- La plage de nœuds est le nombre minimum et maximum de nœuds qu'Amazon Redshift prend en charge pour le type et la taille de nœud.

  > **Note**
  >
  > Il se peut que vous soyez limité à un nombre réduit de nœuds en fonction du quota appliqué à votre AWS compte dans la AWS région sélectionnée. Pour plus d'informations sur les quotas par défaut qui s'appliquent aux ressources Amazon Redshift, consultez Quotas et limites d'Amazon Redshift.
- Capacité totale correspond à la capacité de stockage totale du cluster si vous déployez le nombre maximal de nœuds spécifié dans la plage de nœuds.

Le tableau suivant décrit les spécifications des nœuds RG.

Type de nœud	vCPU	RAM (Gio)	Tranche par défaut par nœud	Limite de stockage géré par nœud [1]	Plage de nœuds avec la création d'un cluster	Capacité de stockage géré totale [2]	
rg.large (nœud unique)	2	16	2	1 To	1	1 To	

Type de nœud	vCPU	RAM (Gio)	Tranche par défaut par nœud	Limite de stockage géré par nœud [1]	Plage de nœuds avec la création d'un cluster	Capacité de stockage géré totale [2]
rg.large (multi-nœuds)	2	16	2	8 TO	2 à 16	128 To
rg.xlarge (multi-nœuds)	4	32	2	32 To	2 à 16 3	1024 To [3]
environ 4 x large	16	128	8	128 To	2 à 32 4	8192 ET 4
environ 12 x large	48	384	16	128 To	2–128	16 384 To

[1] La limite de stockage pour le stockage géré Amazon Redshift. Il s'agit d'une limite stricte.

[2] La limite de stockage géré totale correspond au nombre maximal de nœuds multiplié par la limite de stockage géré par nœud.

[3] Vous pouvez créer un cluster avec le type de nœud rg.xlarge (multi-nœuds) comportant jusqu'à 16 nœuds. Pour les clusters à plusieurs nœuds, vous pouvez redimensionner avec le redimensionnement Elastic jusqu'à 32 nœuds maximum.

[4] Vous pouvez créer un cluster avec le type de nœud rg.4xlarge (multi-nœuds) avec un maximum de 32 nœuds. Vous pouvez le redimensionner avec un redimensionnement Elastic jusqu'à un maximum de 64 nœuds.

La table suivante décrit les spécifications des nœuds RA3.

Type de nœud	vCPU	RAM (Gio)	Tranche par défaut par nœud	Limite de stockage géré par nœud [1]	Plage de nœuds avec la création d'un cluster	Capacité de stockage géré totale [2]
ra3.large (single-node)	2	16	2	1 To	1	1 À [3]
ra3.large (multi-node)	2	16	2	8 TO	2-16	128 To
ra3.xlplus (nœud unique)	4	32	2	4 To	1	4 To[3]
ra3.xlplus (multi-nœuds)	4	32	2	32 To	2–16[4]	1 024 To[4]
ra3.4xlarge	12	96	4	128 To	2–32[5]	8 192 To[5]
ra3.16xlarge	48	384	16	128 To	2–128	16 384 To

[1] La limite de stockage pour le stockage géré Amazon Redshift. Il s'agit d'une limite stricte.

[2] La limite de stockage géré totale correspond au nombre maximal de nœuds multiplié par la limite de stockage géré par nœud.

[3] Pour redimensionner un cluster à nœud unique en cluster à plusieurs nœuds, seul le redimensionnement classique est pris en charge.

[4] Vous pouvez créer un cluster avec le type de nœud ra3.xlplus (multi-nœuds) qui a jusqu'à 16 nœuds. Pour les clusters à plusieurs nœuds, vous pouvez redimensionner avec le redimensionnement Elastic jusqu'à 32 nœuds maximum.

[5] Vous pouvez créer un cluster avec le type de nœud ra3.4xlarge qui a jusqu'à 32 nœuds. Vous pouvez le redimensionner avec un redimensionnement Elastic jusqu'à un maximum de 64 nœuds.

La table suivante décrit les spécifications relatives aux nœuds de calcul dense.

Type de nœud	vCPU	RAM (Gio)	Tranche par défaut par nœud	Stockage par nœud	Plage de nœuds	Capacité totale
dc2.large	2	15	2	160 Go NVMe-SSD	1–32	5.12 To
dc2.8xlarge	32	244	16	2,56 To NVMe-SSD	2–128	326 To

> **Note**
>
> Les types de nœuds de stockage dense (DS2) ne sont plus disponibles.

Noms précédents des types de nœud

Dans les versions précédentes d'Amazon Redshift, certains types de nœuds avaient des noms différents. Vous pouvez utiliser les noms précédents dans l'API Amazon Redshift et AWS CLI. Néanmoins, nous vous recommandons de mettre à jour tous les scripts qui font référence à ces noms afin d'utiliser les noms actuels à la place. Les noms anciens et actuels sont les suivants.

Nom actuel	Noms précédents
ds2.xlarge	ds1.xlarge, dw.hs1.xlarge, dw1.xlarge
ds2.8xlarge	ds1.8xlarge, dw.hs1.8xlarge, dw1.8xlarge
dc1.large	dw2.large

Nom actuel	Noms précédents
dc1.8xlarge	dw2.8xlarge

Détermination du nombre de nœuds

Étant donné qu'Amazon Redshift distribue et exécute les requêtes en parallèle sur l'ensemble des nœuds de calcul d'un cluster, vous pouvez augmenter les performances des requêtes en ajoutant des nœuds à votre cluster. Lorsque vous exécutez un cluster équipé d'au moins deux nœuds de calcul, les données présentes sur chaque nœud sont toujours mises en miroir sur les disques de l'autre nœud, réduisant ainsi le risque de perte de données.

Vous pouvez surveiller les performances des requêtes dans la console Amazon Redshift et à l'aide des CloudWatch métriques Amazon. Vous pouvez également ajouter ou supprimer des nœuds si nécessaire pour atteindre l'équilibre entre le prix et les performances de votre cluster. Lorsque vous demandez un nœud supplémentaire, Amazon Redshift prend en charge tous les détails du déploiement, de l'équilibrage de charge et de la maintenance des données. Pour plus d'informations sur les performances des clusters, consultez Surveiller les performances de cluster Amazon Redshift.

Les nœuds réservés conviennent aux charges de travail régulières en production et vous permettent de réaliser d'importantes économies par rapport aux nœuds à la demande. Vous pouvez acheter des nœuds réservés après avoir exécuté des expériences et des preuves de concepts pour valider votre configuration de production. Pour plus d'informations, consultez Nœuds réservés.

Lorsque vous mettez en pause un cluster, vous suspendez la facturation à la demande pendant la période de mise en pause du cluster. Pendant cette période de pause, vous ne payez que pour le stockage de sauvegarde. Vous n'avez donc pas à vous soucier de la planification et de l'achat de capacités pour l'entrepôt des données en amont, ce qui vous permet de gérer de manière rentable vos environnements à des fins de test ou de développement.

Pour plus d'informations sur la tarification des nœuds à la demande et réservés, consultez la Tarification Amazon Redshift.

Utiliser EC2 pour créer votre cluster

Les clusters Amazon Redshift s'exécutent dans des instances Amazon EC2 configurées pour le type et la taille de nœud Amazon Redshift que vous sélectionnez. Pour plus d'informations sur

ces plateformes réseau, consultez Plateformes prises en charge dans le Guide de l'utilisateur Amazon EC2.

> **Note**
>
> Afin d'éviter les problèmes de connexion entre les outils clients SQL et la base de données Amazon Redshift, nous vous conseillons d'opter pour l'une des deux approches suivantes. Vous pouvez configurer une règle de trafic entrant qui permet aux hôtes de négocier la taille des paquets. Vous pouvez également désactiver les trames TCP/IP jumbo en réglant l'unité de transmission maximale (MTU) sur 1500 sur l'interface réseau (NIC) de vos instances Amazon EC2. Pour plus d'informations sur ces approches, consultez Des requêtes semblent se bloquer et parfois échouent à atteindre le cluster.

Amazon Virtual Private Cloud (Amazon VPC)

Lorsque vous utilisez Amazon VPC, votre cluster s'exécute dans un cloud privé virtuel (VPC) isolé logiquement de votre compte. AWS Si vous provisionnez votre cluster avec Amazon VPC, vous contrôlez l'accès à votre cluster en associant un ou plusieurs groupes de sécurité VPC au cluster. Pour plus d'informations, consultez Groupes de sécurité pour votre VPC dans le manuel Amazon VPC Guide de l'utilisateur.

Pour créer un cluster dans un VPC, vous devez d'abord créer un groupe de sous-réseau de cluster Amazon Redshift en fournissant les informations de sous-réseau de votre VPC, puis renseigner le groupe de sous-réseau lors du lancement du cluster. Pour plus d'informations, consultez Sous-réseaux pour les ressources Redshift.

Pour plus d'informations sur Amazon Virtual Private Cloud (Amazon VPC), consultez la Page détaillée du produit Amazon VPC.

Alarme d'espace disque par défaut

Lorsque vous créez un cluster Amazon Redshift, vous pouvez éventuellement configurer une CloudWatch alarme Amazon pour surveiller le pourcentage moyen d'espace disque utilisé sur tous les nœuds de votre cluster. Nous nous référons à cette alarme comme alarme d'espace disque par défaut.

Le but d'une alarme d'espace disque par défaut consiste à vous aider à surveiller la capacité de stockage de votre cluster. Vous pouvez configurer cette alarme selon les besoins de votre entrepôt

des données. Par exemple, vous pouvez utiliser l'avertissement comme indicateur vous signalant que vous devez redimensionner le cluster. Vous pouvez redimensionner votre cluster soit en un type de nœud différent, soit pour ajouter des nœuds, ou encore pour acheter des nœuds réservés en vue d'une expansion future.

L'alarme d'espace disque par défaut se déclenche lorsque l'utilisation du disque atteint ou dépasse un pourcentage spécifié un certain nombre de fois et sur une durée spécifiée. Par défaut, l'alarme se déclenche lorsque le pourcentage que vous spécifiez est atteint, puis demeure à cette valeur ou à une valeur supérieure pendant cinq minutes ou plus. Vous pouvez modifier les valeurs par défaut après que vous avez lancé le cluster.

Lorsque l' CloudWatch alarme se déclenche, Amazon Simple Notification Service (Amazon SNS) envoie une notification aux destinataires spécifiés pour les avertir que le seuil de pourcentage est atteint. Amazon SNS utilise une rubrique pour spécifier les destinataires et le message transmis dans une notification. Vous pouvez utiliser une rubrique Amazon SNS existant ; sinon, une rubrique est créée en fonction des paramètres que vous spécifiez lorsque vous lancez le cluster. Vous pouvez modifier la rubrique de cette alarme après avoir lancé le cluster. Pour plus d'informations sur la création de sujets Amazon SNS, consultez Démarrage avec Amazon Simple Notification Service.

Après avoir lancé le cluster, vous pouvez afficher et modifier l'alarme dans la fenêtre État du cluster, sous CloudWatch Alarmes. Le nom est ***string*** percentage-disk-space-used-default-< >. Vous pouvez ouvrir l'alarme pour afficher la rubrique Amazon SNS à laquelle elle est associée et modifier les paramètres de l'alarme. Si vous n'avez pas sélectionné de rubrique Amazon SNS existante à utiliser, celle créée pour vous est nommée < ***clustername*** >-default-alarm (< ***recipient*** >) ; par exemple, examplecluster-default-alarm (notify@example.com).

Pour plus d'informations sur la configuration et la modification de l'alarme d'espace disque par défaut, consultez Création d'un cluster et Création d'une alarme d'espace disque.

> **Note**
>
> Si vous supprimez votre cluster, l'alarme associée au cluster n'est pas supprimée, mais elle ne se déclenchera pas. Vous pouvez supprimer l'alarme de la CloudWatch console si vous n'en avez plus besoin.

Statut du cluster

L'état actuel du cluster s'affiche. Le tableau suivant fournit une description de chaque état du cluster.

Statut	Description
`available`	Le cluster est en cours d'exécution et disponible.
`available, prep-for-resize`	Le cluster est préparé pour le redimensionnement Elastic. Le cluster est exécuté et disponible pour les requêtes d'écriture et de lecture, mais les opérations du cluster, comme la création d'un instantané, ne sont pas disponibles.
`available, resize-cleanup`	L'opération de redimensionnement Elastic finalise le transfert des données vers les nouveaux nœuds du cluster. Le cluster est exécuté et disponible pour les requêtes d'écriture et de lecture, mais les opérations du cluster, comme la création d'un instantané, ne sont pas disponibles.
`cancelling-resize`	L'opération de redimensionnement est en cours d'annulation.
`creating`	Amazon Redshift crée le cluster. Pour plus d'informations, consultez Création d'un cluster.
`deleting`	Amazon Redshift supprime le cluster. Pour plus d'informations, consultez Arrêt et suppression d'un cluster.
`final-snapshot`	Amazon Redshift prend un instantané final du cluster avant de le supprimer. Pour plus d'informations, consultez Arrêt et suppression d'un cluster.
`hardware-failure`	Le cluster subit une défaillance matérielle. Si vous avez un cluster à nœud unique, le nœud ne peut pas être remplacé. Pour récupérer votre cluster, restaurez un instantané. Pour plus d'informations, consultez Instantanés et sauvegardes Amazon Redshift.
`incompatible-hsm`	Amazon Redshift ne peut pas se connecter au module de sécurité matérielle (HSM). Vérifiez la configuration du HSM entre le cluster et le module de sécurité matérielle. Pour plus d'informations, consultez Chiffrement à l'aide de modules de sécurité matérielle.

Statut	Description
`incompatible-network`	Il y a un problème avec la configuration du réseau sous-jacent. Assurez-vous que le VPC dans lequel vous avez lancé le cluster existe et que ses paramètres sont corrects. Pour plus d'informations, consultez Ressources Redshift dans un VPC.
`incompatible-parameters`	Problème avec une ou plusieurs valeurs du groupe de paramètres associé, et la ou les valeurs de paramètre ne peuvent pas s'appliquer. Modifiez le groupe de paramètres et mettez à jour les valeurs non valides. Pour plus d'informations, consultez Groupes de paramètres Amazon Redshift.
`incompatible-restore`	Problème de restauration du cluster à partir de l'instantané. Essayez de restaurer le cluster à nouveau avec un autre instantané. Pour plus d'informations, consultez Instantanés et sauvegardes Amazon Redshift.
`modifying`	Amazon Redshift applique les modifications au cluster. Pour plus d'informations, consultez Modification d'un cluster.
`paused`	Le cluster est mis en pause. Pour plus d'informations, consultez Suspension et reprise d'un cluster.
`rebooting`	Amazon Redshift redémarre le cluster. Pour plus d'informations, consultez Redémarrage d'un cluster.
`renaming`	Amazon Redshift applique un nouveau nom au cluster. Pour plus d'informations, consultez Renommer un cluster.
`resizing`	Amazon Redshift redimensionne le cluster. Pour plus d'informations, consultez Redimensionnement d'un cluster.
`rotating-keys`	Amazon Redshift effectue une rotation des clés de chiffrement pour le cluster. Pour plus d'informations, consultez Rotation des clés de chiffrement.
`storage-full`	Le cluster a atteint sa capacité de stockage. Redimensionnez le cluster pour ajouter des nœuds ou choisir une autre taille de nœud. Pour plus d'informations, consultez Redimensionnement d'un cluster.

Statut	Description
`updating-hsm`	Amazon Redshift met à jour la configuration HSM.

Considérations relatives à l'utilisation des clusters alloués Amazon Redshift

Une fois votre cluster créé, vous trouverez dans cette section des informations sur les régions où les fonctionnalités sont disponibles, les tâches de maintenance, les types de nœuds et les limites d'utilisation.

Considérations sur les régions et les zones de disponibilité

Amazon Redshift est disponible dans plusieurs AWS régions. Par défaut, Amazon Redshift approvisionne votre cluster dans une zone de disponibilité (AZ) sélectionnée au hasard au sein de la AWS région que vous avez choisie. Tous les nœuds de cluster sont alloués dans la même zone de disponibilité.

Vous pouvez éventuellement demander une zone de disponibilité spécifique si Amazon Redshift est disponible dans cette zone. Par exemple, si vous avez déjà une instance Amazon EC2 en exécution dans une zone de disponibilité, vous pouvez créer votre cluster Amazon Redshift dans la même zone pour réduire la latence. D'autre part, vous pouvez choisir une autre zone de disponibilité pour une plus grande disponibilité. Amazon Redshift n'est peut-être pas disponible dans toutes les zones de disponibilité d'une AWS région.

Pour obtenir la liste des AWS régions prises en charge dans lesquelles vous pouvez provisionner un cluster Amazon Redshift, consultez la section Points de terminaison Amazon Redshift dans le. Référence générale d'Amazon Web Services

Maintenance du cluster

Amazon Redshift effectue régulièrement une maintenance pour appliquer les mises à niveau à votre cluster. Au cours de ces mises à jour, votre cluster Amazon Redshift n'est pas disponible pour les opérations normales. Il existe plusieurs manières de contrôler la gestion de votre cluster. Par exemple, vous pouvez contrôler le déploiement des mises à jour sur vos clusters. Vous pouvez également choisir si votre cluster est exécuté sur la version la plus récente ou sur la version

publiée juste avant celle-ci. Enfin, vous avez également la possibilité de reporter les mises à jour de maintenance non obligatoires pendant une certaine période.

Fenêtres de maintenance

Amazon Redshift attribue une fenêtre de maintenance de 30 minutes au hasard sur une période de 8 heures par AWS région, survenant un jour aléatoire de la semaine (du lundi au dimanche inclus).

Fenêtres de maintenance par défaut

La liste suivante indique les plages horaires pour chaque AWS région à partir de laquelle les fenêtres de maintenance par défaut sont attribuées :

- Région USA Est (Virginie du Nord) : 03:00 – 11:00 UTC
- Région USA Est (Ohio) : 03:00 – 11:00 UTC
- Région USA Ouest (Californie du Nord) : 06:00 – 14:00 UTC
- Région USA Ouest (Oregon) : 06:00 – 14:00 UTC
- Région Afrique (Le Cap) : 20:00 – 04:00 UTC
- Région Asie-Pacifique (Hong Kong) : 13:00 – 21:00 UTC
- Région Asie-Pacifique (Hyderabad) : 16:30 – 00:30 UTC
- Région Asie-Pacifique (Jakarta) : 15:00 – 23:00 UTC
- Région Asie-Pacifique (Malaisie) : 14:00 – 22:00 UTC
- Région Asie-Pacifique (Melbourne) : 12:00 – 20:00 UTC
- Région Asie-Pacifique (Mumbai) : 16:30 – 03:00 UTC
- Région Asie-Pacifique (Nouvelle Zélande) : 10:00 – 18:00 UTC
- Région Asie-Pacifique (Osaka) : 13:00 – 21:00 UTC
- Région Asie-Pacifique (Seoul) : 13:00 – 21:00 UTC
- Région Asie-Pacifique (Singapour) : 14:00 – 22:00 UTC
- Région Asie-Pacifique (Sydney) : 12:00 – 20:00 UTC
- Région Asie-Pacifique (Taipei) : 14:00 – 22:00 UTC
- Région Asie-Pacifique (Thaïlande) : 15:00 – 23:00 UTC
- Région Asie-Pacifique (Tokyo) : 13:00 – 021:00 UTC
- Région Canada (Centre) : 03:00 – 11:00 UTC

- Région Canada Ouest (Calgary) : 4 h 00–12 h 00 UTC
- Région Chine (Beijing) : 13:00 – 21:00 UTC
- Région Chine (Ningxia) : 13:00 – 21:00 UTC
- Région Europe (Francfort) : 06:00 – 14:00 UTC
- Région Europe (Irlande) : 22:00 – 06:00 UTC
- Région Europe (Londres) : 22:00 – 06:00 UTC
- Région Europe (Milan) : 21:00 – 05:00 UTC
- Région Europe (Paris) : 23:00 – 07:00 UTC
- Région Europe (Stockholm) : 23:00 – 07:00 UTC
- Région Europe (Zurich) : 20:00 – 04:00 UTC
- Région Israël (Tel Aviv) : 20:00 – 04:00 UTC
- Région Mexique (Centre) : 04:00 – 12:00 UTC
- Région Europe (Espagne) : 21:00 – 05:00 UTC
- Région Moyen-Orient (Bahreïn) : 13:00 – 21:00 UTC
- Région Moyen-Orient (EAU) : 18:00 – 02:00 UTC
- Région Amérique du Sud (São Paulo) : 19:00 – 03:00 UTC

Si un événement de maintenance est planifié pour une semaine donnée, il démarre pendant la fenêtre de maintenance de 30 minutes attribuée. Pendant qu'Amazon Redshift effectue la maintenance, il met fin à toutes les requêtes ou autres opérations en cours. Les interruptions de service survenues lors de la maintenance planifiée ne sont pas considérées comme des interruptions mensuelles ou des indisponibilités dans le cadre du contrat de niveau de service Amazon Redshift. La plus grande partie de la maintenance s'effectue pendant la fenêtre de maintenance de 30 minutes, mais certaines tâches de maintenance peuvent continuer à s'exécuter après la fermeture de la fenêtre. S'il n'y a aucune tâche de maintenance à effectuer pendant la fenêtre de maintenance planifiée, votre cluster continue à fonctionner normalement jusqu'à la prochaine fenêtre de maintenance.

Vous pouvez modifier la fenêtre de maintenance planifiée en modifiant le cluster, soit de manière programmatique, soit en utilisant la console Amazon Redshift. Vous pouvez trouver la fenêtre de maintenance et définir le jour et l'heure auxquels elle se produit pour le cluster sous l'onglet Maintenance.

Il est possible qu'un cluster redémarre en dehors d'une fenêtre de maintenance. Cela peut se produire pour plusieurs raisons. Une des raisons les plus courantes est qu'un problème a été détecté avec le cluster et que des opérations de maintenance sont en cours pour le ramener à un état sain. Pour plus d'informations, consultez l'article Pourquoi mon cluster Amazon Redshift a-t-il redémarré en dehors de la fenêtre de maintenance ?, qui fournit des détails sur les raisons pour lesquelles cela peut se produire.

Report de la maintenance

Pour replanifier la fenêtre de maintenance de votre cluster, vous pouvez reporter la maintenance jusqu'à 60 jours. Par exemple, si la fenêtre de maintenance de votre cluster est définie sur mercredi 8 h 30 – 9 h UTC, mais que vous devez accéder à votre cluster à ce moment précis, vous pouvez reporter la maintenance.

Si vous reportez la maintenance, Amazon Redshift appliquera toujours les mises à jour matérielles ou autres mises à jour de sécurité obligatoires à votre cluster. Votre cluster n'est pas disponible au cours de ces mises à jour.

Si une mise à jour matérielle ou une autre mise à jour de sécurité obligatoire est planifiée pendant la prochaine fenêtre de maintenance, Amazon Redshift vous envoie des notifications anticipées dans la catégorie En attente. Pour en savoir plus sur les notifications d'événements En attente, consultez Notifications d'événement d'un cluster alloué Amazon Redshift.

Vous pouvez également choisir de recevoir des notifications d'événements d'Amazon Simple Notification Service (Amazon SNS). Pour plus d'informations sur l'abonnement à la notification d'événements Amazon RDS, consultez Abonnements aux notifications d'événements de cluster Amazon Redshift.

Si vous reportez la maintenance de votre cluster, la fenêtre de maintenance suivant la période de report ne peut pas être reportée.

> **Note**
>
> Vous ne pouvez pas reporter une opération de maintenance une fois celle-ci entamée.

Pour plus d'informations sur la maintenance du cluster, consultez la documentation suivante :

- Fenêtres de maintenance
- Opérations de cluster

- Modification d’un cluster

Sélection du suivi de maintenance des clusters

Lorsque Amazon Redshift publie une nouvelle version du cluster, votre cluster est mis à jour pendant sa fenêtre de maintenance. Vous pouvez vérifier si votre cluster est mis à jour par rapport à la dernière version ou à la précédente.

Le suivi contrôle la version du cluster qui est appliquée au cours d’une fenêtre de maintenance. Lorsqu’Amazon Redshift publie une nouvelle version du cluster, cette version est assignée au suivi Current (Actuellle) et la version précédente est assignée au suivi Trailing (Précédente).

Pour plus d’informations sur le suivi du cluster, consultez Suivi des clusters alloués Amazon Redshift et des groupes de travail sans serveur.

Comprendre comment les nœuds RG et RA3 séparent le calcul du stockage

Ces sections détaillent les tâches disponibles pour les types de nœuds RG et RA3, en montrant leur applicabilité à un ensemble de cas d'utilisation et en détaillant leurs avantages par rapport aux types de nœuds précédemment disponibles.

Avantages et disponibilité des nœuds RG et RA3

Les nœuds RG et RA3 présentent les avantages suivants :

- Ils sont flexibles pour augmenter votre capacité de calcul sans augmenter vos coûts de stockage. De plus, ils adaptent votre stockage sans surprovisionner la capacité de calcul.
- Ils utilisent des disques SSD haute performance pour vos données sensibles (hot data) et Amazon S3 pour les données non sensibles (cold data). Ils offrent ainsi une facilité d’utilisation, un stockage économique et des performances de requête élevées.
- Ils utilisent un réseau à haut débit basé sur le système AWS Nitro afin de réduire davantage le temps nécessaire au déchargement et à la récupération des données vers Amazon S3.

Pensez à choisir les types de nœuds RG et RA3 dans les cas suivants :

- Si vous avez besoin de la flexibilité nécessaire pour dimensionner et payer le calcul indépendamment du stockage.
- Vous interrogez une fraction de vos données totales.
- Votre volume de données augmente rapidement ou devrait croître rapidement.

- Vous souhaitez avoir la flexibilité nécessaire pour dimensionner le cluster uniquement en fonction de vos besoins en performances.

Considérations relatives au calcul des requêtes de lac de données — Sur les clusters provisionnés en DC2 et RA3, les requêtes de lac de données sont exécutées sur Redshift Spectrum, qui utilise des serveurs Amazon Redshift dédiés indépendants de votre cluster. Sur les clusters provisionnés par RG, les requêtes du lac de données s'exécutent sur les propres ressources de calcul du cluster et partagent ces ressources avec d'autres charges de travail. Pour les charges de travail impliquant une utilisation intensive des requêtes de lac de données, considérez cela lors du dimensionnement de votre cluster RG.

Pour utiliser les types de nœuds RG, votre AWS région doit prendre en charge le RG. Pour plus d'informations, consultez Disponibilité du type de nœud RG dans AWS Régions.

Pour utiliser les types de nœuds RA3, votre AWS région doit prendre en charge le RA3. Pour plus d'informations, consultez Disponibilité du type de nœud RA3 dans AWS Régions.

> **Important**
>
> Vous pouvez utiliser les types de nœuds ra3.xlplus uniquement avec la version de cluster 1.0.21262 ou ultérieure. Vous pouvez consulter la version d'un cluster existant avec la console Amazon Redshift. Pour plus d'informations, consultez Déterminer la version du groupe de travail ou du cluster.
> Assurez-vous d'utiliser la nouvelle console Amazon Redshift lorsque vous travaillez avec des nœuds de type RG ou RA3.
> En outre, pour utiliser des types de nœuds RG ou RA3 avec des opérations Amazon Redshift qui utilisent le suivi, la valeur du suivi de maintenance doit être définie sur une version de cluster prenant en charge le RG ou le RA3. Pour plus d'informations sur le suivi, consultez Sélection du suivi de maintenance des clusters.

Prenez en compte les points suivants lorsque vous utilisez des types de nœuds RA3 à nœud unique.

- Les producteurs et consommateurs d'unités de partage des données sont pris en charge.
- Pour modifier les types de nœuds, seul le redimensionnement classique est pris en charge. La modification du type de nœud avec le redimensionnement élastique ou la restauration d'instantané n'est pas prise en charge. Les scénarios suivants sont pris en charge :
  - Redimensionnement classique de dc2.xlarge à 1 nœud vers ra3.xlplus à 1 nœud, et vice versa.

- Redimensionnement classique de dc2.xlarge à 1 nœud vers ra3.xlplus à nœuds multiples, et vice versa.
- Redimensionnement classique de dc2.xlarge à nœuds multiples vers ra3.xlplus à 1 nœud, et vice versa.

Utilisation du stockage géré Amazon Redshift

Avec le stockage géré d'Amazon Redshift, vous pouvez stocker et traiter toutes vos données dans Amazon Redshift tout en bénéficiant d'une plus grande flexibilité pour faire évoluer séparément la capacité de calcul et de stockage. Vous continuez à ingérer des données avec la commande COPY ou INSERT. Pour optimiser les performances et gérer le placement automatique des données sur les différents niveaux de stockage, Amazon Redshift tire parti d'optimisations telles que la température des blocs de données, leur âge et les modèles de charge de travail. Lorsque cela est nécessaire, Amazon Redshift met automatiquement à niveau le stockage vers Amazon S3 sans nécessiter d'action manuelle.

Pour plus d'informations sur les coûts de stockage, consultez Tarification Amazon Redshift.

Gestion des types de nœuds RG ou RA3

Pour tirer parti de la séparation entre le calcul et le stockage, vous pouvez créer ou mettre à niveau votre cluster avec le type de nœud RG ou RA3. Pour utiliser les types de nœuds RG ou RA3, créez vos clusters dans un cloud privé virtuel ()EC2-VPC.

Pour modifier le nombre de nœuds du cluster Amazon Redshift avec un type de nœud RG ou RA3, effectuez l'une des opérations suivantes :

- Ajoutez ou supprimez des nœuds avec l'opération de redimensionnement élastique. Dans certains cas, la suppression de nœuds d'un cluster RG ou RA3 n'est pas autorisée avec le redimensionnement élastique. Par exemple, lorsqu'une mise à niveau du nombre de nœuds 2:1 place le nombre de tranches par nœud à 32. Pour plus d'informations, consultez Redimensionnement d'un cluster. Si le redimensionnement élastique n'est pas disponible, utilisez le redimensionnement classique.
- Ajoutez ou supprimez des nœuds avec l'opération de redimensionnement classique. Choisissez cette option lorsque vous effectuez un redimensionnement sur une configuration qui ne permet pas le redimensionnement Elastic Le redimensionnement élastique est plus rapide que le redimensionnement classique. Pour plus d'informations, consultez Redimensionnement d'un cluster.

Disponibilité du type de nœud RG dans AWS Régions

Les types de nœuds RG ne sont disponibles que dans les AWS régions suivantes :

- Région USA Est (Virginie du Nord) (us-east-1)
- Région USA Est (Ohio) (us-east-2)
- Région US Ouest (Californie du Nord) (us-west-1)
- Région USA Ouest (Oregon) (us-west-2)
- Région Afrique (Le Cap) (af-south-1)
- Région Asie-Pacifique (Hong Kong) (ap-east-1)
- Région Asie-Pacifique (Taipei) (ap-east-2)
- Région Asie-Pacifique (Tokyo) (ap-northeast-1)
- Région Asie-Pacifique (Séoul) (ap-northeast-2)
- Région Asie-Pacifique (Osaka) (ap-northeast-3)
- Région Asie-Pacifique (Mumbai) (ap-south-1)
- Région Asie-Pacifique (Hyderabad) (ap-south-2)
- Région Asie-Pacifique (Singapour) (ap-southeast-1)
- Région Asie-Pacifique (Sydney) (ap-southeast-2)
- Région Asie-Pacifique (Jakarta) (ap-southeast-3)
- Région Asie-Pacifique (Melbourne) (ap-southeast-4)
- Région Asie-Pacifique (Malaisie) (ap-southeast-5)
- Région Asie-Pacifique (Thaïlande) (ap-southeast-7)
- Région Canada (Centre) (ca-central-1)
- Région Europe (Francfort) (eu-central-1)
- Région Europe (Zurich) (eu-central-2)
- Région Europe (Stockholm) (eu-north-1)
- Région Europe (Milan) (eu-south-1) (rg.xlarge et rg.4xlarge uniquement)
- Région Europe (Espagne) (eu-south-2)
- Région Europe (Irlande) (eu-west-1)
- Région Europe (Londres) (eu-west-2)
- Région Europe (Paris) (eu-west-3)

- Région Mexique (Centre) (mx-central-1)
- Région Amérique du Sud (Sao Paulo) (sa-east-1)
- AWS GovCloud (US-East) (us-gov-east-1)
- AWS GovCloud (US-West) (US-GOV-West-1)

Disponibilité du type de nœud RA3 dans AWS Régions

Les types de nœuds RA3 ne sont disponibles que dans les AWS régions suivantes :

- Région USA Est (Virginie du Nord) (us-east-1)
- Région USA Est (Ohio) (us-east-2)
- Région US Ouest (Californie du Nord) (us-west-1)
- Région USA Ouest (Oregon) (us-west-2)
- Région Afrique (Le Cap) (af-south-1)
- Région Asie-Pacifique (Hong Kong) (ap-east-1)
- Région Asie-Pacifique (Hyderabad) (ap-south-2)
- Région Asie-Pacifique (Jakarta) (ap-southeast-3)
- Région Asie-Pacifique (Malaisie) (ap-southeast-5)
- Région Asie-Pacifique (Melbourne) (ap-southeast-4)
- Région Asie-Pacifique (Mumbai) (ap-south-1)
- Région Asie-Pacifique (Nouvelle Zélande) (ap-southeast-6)
- Région Asie-Pacifique (Osaka) (ap-northeast-3)
- Région Asie-Pacifique (Séoul) (ap-northeast-2)
- Région Asie-Pacifique (Singapour) (ap-southeast-1)
- Région Asie-Pacifique (Sydney) (ap-southeast-2)
- Région Asie-Pacifique (Taipei) (ap-east-2)
- Région Asie-Pacifique (Thaïlande) (ap-southeast-7)
- Région Asie-Pacifique (Tokyo) (ap-northeast-1)
- Région Canada (Centre) (ca-central-1)
- Région Canada Ouest (Calgary) (ca-west-1)
- Région Chine (Beijing) (cn-north-1)

- Région Chine (Ningxia) (cn-northwest-1)
- Région Europe (Francfort) (eu-central-1)
- Région Europe (Zurich) (eu-central-2)
- Région Europe (Irlande) (eu-west-1)
- Région Europe (Londres) (eu-west-2)
- Région Europe (Milan) (eu-south-1)
- Région Europe (Espagne) (eu-south-2)
- Région Europe (Paris) (eu-west-3)
- Région Europe (Stockholm) (eu-north-1)
- Région Israël (Tel Aviv) (il-central-1)
- Région Mexique (Centre) (mx-central-1)
- Région Moyen-Orient (Bahreïn) (me-south-1)
- Région Moyen-Orient (Émirats arabes unis) (me-central-1)
- Région Amérique du Sud (Sao Paulo) (sa-east-1)
- AWS GovCloud (US-East) (us-gov-east-1)
- AWS GovCloud (US-West) (US-GOV-West-1)

Mise à niveau vers des types de nœuds RG ou RA3

Pour mettre à niveau votre type de nœud existant vers RG ou RA3, vous disposez des options suivantes pour modifier le type de nœud :

- Restauration à partir d'un instantané : Amazon Redshift utilise l'instantané le plus récent de votre cluster et le restaure pour créer un nouveau cluster RG ou RA3. Dès que la création du cluster est terminée (généralement en quelques minutes), les nœuds RG ou RA3 sont prêts à exécuter votre charge de travail de production complète. Comme le calcul est séparé du stockage, les données chaudes sont introduites dans le cache local à des vitesses rapides grâce à une large bande passante réseau. Si vous effectuez une restauration à partir du dernier instantané DC2, RG et RA3 préservent les informations relatives aux hot blocks de la charge de travail DC2 et remplissent son cache local avec les blocs les plus chauds. Pour plus d’informations, consultez Restauration d’un cluster à partir d’un instantané.

  Pour conserver le même point de terminaison pour vos applications et vos utilisateurs, vous pouvez renommer le nouveau cluster RG ou RA3 avec le même nom que le cluster DC2 d'origine. Pour

renommer le cluster, modifiez le cluster dans la console Amazon Redshift ou via l'opération API `ModifyCluster`. Pour plus d'informations, consultez Renommer un cluster ou Opérations de l'API de `ModifyCluster` dans la Référence API Amazon Redshift.

- Redimensionnement élastique – Redimensionner le cluster à l'aide du redimensionnement Elastic. Lorsque vous utilisez le redimensionnement Elastic pour changer de type de nœud, Amazon Redshift crée automatiquement un instantané, puis un nouveau cluster, supprime l'ancien cluster et renomme le nouveau cluster. L'opération de redimensionnement Elastic peut être exécutée à la demande ou programmée pour être exécutée plus tard. Vous pouvez rapidement mettre à niveau vos clusters de type nœud DC2 existants vers RG ou RA3 grâce au redimensionnement élastique. Pour plus d'informations, consultez Elastic resize (Redimensionnement élastique).

> **Note**
>
> Pour migrer des clusters RA3 existants vers rg.xlarge ou rg.4xlarge, votre cluster source doit exécuter le correctif P201 ou une version ultérieure. Pour migrer vers rg.large ou rg.12xlarge, votre cluster source doit exécuter P202 ou une version ultérieure. Pour créer ou migrer vers un cluster rg.large à nœud unique, votre cluster doit exécuter P204 ou une version ultérieure. Les clusters DC2 peuvent migrer vers RG quelle que soit la version du correctif.

Le tableau suivant présente les recommandations relatives à la mise à niveau vers les types de nœuds RG.

Les recommandations de cette table concernent les types et tailles de nœuds de cluster de départ, mais dépendent des exigences informatiques de votre charge de travail. Le RG possède des caractéristiques de performance différentes. Le mappage recommandé est donc un point de départ. Comparez vos charges de travail critiques et ajustez le nombre de nœuds à la hausse ou à la baisse en fonction des performances observées. Le prix par vCPU des instances RG est inférieur à celui des instances RA3. L'ajout de nœuds pour optimiser les performances peut donc tout de même se traduire par une baisse du coût global. Pour plus d'informations sur la tarification par type de nœud, consultez la tarification d'Amazon Redshift.

Pour mieux estimer vos besoins, envisagez de réaliser une preuve de concept (POC) qui utilise Test Drive pour exécuter des configurations potentielles. Allouez un cluster pour votre entrepôt de données POC au lieu de Redshift sans serveur. Pour plus d'informations sur la réalisation d'une preuve de concept, consultez Réaliser une preuve de concept (POC) pour Amazon Redshift dans le Guide du développeur de base de données Amazon Redshift.

Type de nœud existant	Nombre de nœuds existants	Nouveau type de nœud recommandé	Action de mise à niveau
ra3.16xlarge	2–128	rg.12 x large	Commencez avec 1 nœud de rg.12xlarge pour chaque nœud de ra3.16xlarge 1.
ra3.4xlarge	2 à 64	rg.4 x large	Commencez avec 3 nœuds de rg.4xlarge pour 4 nœuds de ra3.4xlarge 1.
ra3.xlplus	1	rg.large	Commencez avec 2 nœuds de rg.large pour un cluster ra3.xlplus à nœud unique 1 ,2.
ra3.xlplus	2—32	rg.xlarge	Commencez avec 1 nœud de rg.xlarge pour chaque nœud de ra3.xlplus 1.
ra3.large	1 à 16 ans	rg.large	Commencez avec 1 nœud de rg.large pour chaque nœud de ra3.large 1,2.
dc2.8xlarge	2–15	rg.4 x large	Commencez avec 3 nœuds de rg.4xlarge pour 2 nœuds de dc2.8xlarge 1.
dc2.8xlarge	16–128	rg.12 x large	Commencez avec 1 nœud de rg.12xlarge pour 2 nœuds de dc2.8xlarge 1.
dc2.large	1 à 3	rg.large	Commencez avec 1 nœud de rg.large pour chaque nœud de dc2.large 1,2.
dc2.large	4	rg.large	Commencez avec 3 nœuds de rg.large 1.
dc2.large	5–15	rg.xlarge	Commencez avec 3 nœuds de rg.xlarge pour 8 nœuds de dc2.large 1.

Type de nœud existant	Nombre de nœuds existants	Nouveau type de nœud recommandé	Action de mise à niveau
dc2.large	16–32	rg.4 x large	Commencez avec 1 nœud de rg.4xlarge pour 10 nœuds de dc2.large 1.

[1]Des nœuds supplémentaires peuvent être nécessaires en fonction des exigences de charge de travail. Ajoutez ou supprimez des nœuds en fonction des besoins de calcul de vos performances de requête requises. Le prix par vCPU des instances RG est inférieur à celui des instances RA3. L'ajout de nœuds peut donc tout de même entraîner une baisse du coût global par rapport à votre configuration précédente. Pour plus d'informations, consultez Tarification d'Amazon Redshift.

[2] Pour les clusters à nœud unique, voir Single-node clusters sousÉléments à prendre en compte lors de la mise à niveau vers les nœuds RG.

Le tableau suivant présente des recommandations lors de la mise à niveau vers des types de nœuds RA3.

Les recommandations de cette table concernent les types et tailles de nœuds de cluster de départ, mais dépendent des exigences informatiques de votre charge de travail. Pour mieux estimer vos besoins, envisagez de réaliser une preuve de concept (POC) qui utilise Test Drive pour exécuter des configurations potentielles. Allouez un cluster pour votre entrepôt de données POC au lieu de Redshift sans serveur. Pour plus d'informations sur la réalisation d'une preuve de concept, consultez Réaliser une preuve de concept (POC) pour Amazon Redshift dans le Guide du développeur de base de données Amazon Redshift.

Type de nœud existant	Nombre de nœuds existants	Nouveau type de nœud recommandé	Action de mise à niveau
dc2.8xlarge	2–15	ra3.4xlarge	Commencez par 2 nœuds de ra3.4xlarge pour chaque nœud de dc2.8xlarge[1].
dc2.8xlarge	16–128	ra3.16xlarge	Commencez par 1 nœud de ra3.16xlarge

Type de nœud existant	Nombre de nœuds existants	Nouveau type de nœud recommandé	Action de mise à niveau
			pour tous les 2 nœuds de dc2.8xlarge[1].
dc2.large	1 – 4	ra3.large	Commencez par 1 nœud de ra3.large pour chaque nœud de dc2.large[1]. Commencez par 2 nœuds de ra3.large tous les 2 nœuds de dc2.large[1]. Commencez par 3 nœuds de ra3.large tous les 3 nœuds de dc2.large[1]. Commencez par 3 nœuds de ra3.large tous les 4 nœuds de dc2.large[1].
dc2.large	5–15	ra3.xlplus	Commencez par 3 nœuds de ra3.xlplus tous les 8 nœuds de dc2.large[1].
dc2.large	16–32	ra3.4xlarge	Commencez par 1 nœud de ra3.4xlarge tous les 8 nœuds de dc2.large[1,2].

[1]Des nœuds supplémentaires peuvent être nécessaires en fonction des exigences de charge de travail. Ajoutez ou supprimez des nœuds en fonction des besoins de calcul de vos performances de requête requises.

[2]Les clusters avec le type de nœud dc2.large sont limités à 32 nœuds.

Le nombre minimum de nœuds pour certains types de nœud RA3 est de deux nœuds. Prenez cela en compte lors de la création d'un cluster RA3.

Fonctionnalités réseau prises en charge par les nœuds RG et RA3

Les nœuds RG et RA3 prennent en charge un ensemble de fonctionnalités réseau non disponibles pour les autres types de nœuds. Cette section fournit une brève description de chaque fonctionnalité et des liens vers de la documentation supplémentaire :

- Provisioned-cluster Point de terminaison VPC : lorsque vous créez ou restaurez un cluster RG ou RA3, Amazon Redshift utilise un port compris entre 5431 et 5455 ou 8191-8215. Lorsque le cluster est défini sur un port de l'une de ces plages, Amazon Redshift crée automatiquement un point de terminaison VPC dans votre AWS compte pour le cluster et y attache une adresse IP privée. Si vous configurez le cluster pour qu'il soit accessible au public, Redshift crée une adresse IP Elastic dans votre compte AWS et l'attache au point de terminaison d'un VPC. Pour plus d'informations, consultez Configuration des paramètres de communication des groupes de sécurité pour un cluster Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur
- Single-subnet Clusters RG ou RA3 : vous pouvez créer un cluster RG ou RA3 avec un seul sous-réseau, mais il ne peut pas utiliser les fonctionnalités de reprise après sinistre. Une exception se produit si vous activez la relocalisation de cluster alors que le sous-réseau ne dispose pas de plusieurs zones de disponibilité (AZ).
- Multi-subnet Clusters et groupes de sous-réseaux RG ou RA3 : vous pouvez créer un cluster RG ou RA3 avec plusieurs sous-réseaux en créant un groupe de sous-réseaux lorsque vous provisionnez le cluster dans votre cloud privé virtuel (VPC). Un groupe de sous-réseaux de cluster vous permet de spécifier un ensemble de sous-réseaux dans votre VPC et Amazon Redshift crée le cluster dans l'un d'entre eux. Après avoir créé un groupe de sous-réseaux, vous pouvez supprimer les sous-réseaux ajoutés précédemment ou en ajouter plus. Pour de plus amples informations, consultez Groupes de sous-réseaux de cluster Amazon Redshift.
- Cross-account ou accès aux points de terminaison entre VPC : vous pouvez accéder à un cluster provisionné ou à un groupe de travail Amazon Redshift Serverless en configurant un point de terminaison VPC. Redshift-managed Vous pouvez le configurer en tant que connexion privée entre un VPC qui contient un cluster ou un groupe de travail et un VPC dans lequel vous exécutez

un outil client, par exemple. Ainsi, vous pouvez accéder à l'entrepôt des données sans utiliser d'adresse IP publique ni acheminer le trafic sur Internet. Pour plus d'informations, consultez la section Utilisation des points de Redshift-managed terminaison VPC.

- Relocalisation de cluster : vous pouvez déplacer un cluster vers une autre zone de disponibilité (AZ) sans subir la moindre de perte de données en cas d'interruption de service. Vous devez l'activer dans la console. Pour plus d'informations, consultez Relocalisation d'un cluster.
- Nom de domaine personnalisé – Vous pouvez créer un nom de domaine personnalisé, également appelé URL personnalisée, pour votre cluster Amazon Redshift. Il s'agit d'un enregistrement DNS facile à lire qui achemine les SQL-client connexions vers le point de terminaison de votre cluster. Pour plus d'informations, consultez Noms de domaine personnalisé pour les connexions client.

Éléments à prendre en compte lors de la mise à niveau vers les nœuds RG

Version du correctif

Pour migrer de RA3 vers RG, votre cluster source doit respecter la version de correctif minimale requise : P201 pour rg.xlarge et rg.4xlarge, P202 pour rg.large et rg.12xlarge à nœuds multiples et P204 pour rg.large à nœud unique. Les clusters DC2 peuvent migrer vers RG quelle que soit la version du correctif. Avant de migrer, testez vos charges de travail en restaurant un instantané sur un cluster RG avant de déplacer le trafic de production. Pour plus de détailsCorrectif 201 d'Amazon Redshift, reportez-vous Correctif 202 d'Amazon Redshift aux sections etCorrectif 204 d'Amazon Redshift.

Single-node clusters

- Single-node Les clusters RG sont pris en charge sur rg.large uniquement.
- Un cluster rg.large à nœud unique prend en charge jusqu'à 1 To de stockage géré, contre 4 To pour un cluster ra3.xlplus à nœud unique. Utilisez un cluster rg.large à nœuds multiples si la taille de vos données dépasse 1 To ou si l'on s'attend à ce qu'elles dépassent ce chiffre.
- Single-node les clusters sont destinés aux charges de travail de développement et de test. Pour les charges de travail de production, utilisez au moins deux nœuds. Pour plus d'informations, consultez Clusters et nœuds dans Amazon Redshift et Détails de type de nœud.

Charges de travail liées au spectre

Les clusters dont les charges de travail utilisent fortement Spectrum peuvent observer un ralentissement des performances de requête après la migration vers RG. Contrairement à RA3 et

DC2, RG exécute le moteur de requête de lac de données intégré directement sur les nœuds de calcul du cluster plutôt que sur un parc Spectrum distinct. Si vous constatez une dégradation des performances de Spectrum, augmentez le nombre de nœuds de votre cluster RG ou migrez vers un type de nœud RG plus important.

Les clusters RG prennent également en charge l'interrogation de données dans des compartiments Amazon S3 situés dans une AWS région différente, supprimant ainsi la limitation de même région qui s'applique aux clusters RA3 et DC2 utilisant Spectrum. Cross-region les requêtes entraînent des frais de transfert de données supplémentaires. Pour plus d'informations, consultez la section Interrogation de votre lac de données.

Cursor-based charges de travail

Les nœuds RG ont une taille de curseur prise en charge différente de celle des nœuds RA3 et DC2. Reportez-vous à la section Contraintes du curseur pour connaître les limites de taille du curseur. Si votre charge de travail dépend fortement des curseurs et que la taille des curseurs est limitée, migrez vers un type de nœud RG plus important. Vous pouvez réduire le nombre de nœuds proportionnellement pour maintenir une taille et un coût de cluster totaux similaires.

Éligibilité au dimensionnement de la simultanéité

Si votre cluster utilise Concurrency Scaling et compte plus de 32 nœuds, et que vous souhaitez migrer vers rg.12xlarge, utilisez Elastic Resize ou Snapshot Restore pour maintenir la prise en charge de la mise à l'échelle de la concurrence. Si votre cluster compte plus de 32 nœuds et que vous effectuez un redimensionnement classique au format rg.12xlarge, le cluster perd la prise en charge de la mise à l'échelle de la concurrence. Les clusters rg.12xlarge récemment créés avec plus de 32 nœuds ne prennent pas en charge le dimensionnement de la concurrence. Pour plus d'informations, consultez la section Mise à l'échelle des candidats à la simultanéité.

Nœuds réservés

Si votre cluster utilise des nœuds réservés, la modification du type de nœud ne modifie pas automatiquement vos réservations : les réservations existantes restent liées au type de nœud d'origine jusqu'à la fin de leur durée. Avant de migrer un cluster qui utilise des nœuds réservés, consultezPoints à prendre en compte avant de modifier le type de nœud sur un cluster qui utilise des instances réservées.

Opérations de cluster

Après avoir créé un cluster, vous pouvez effectuer des opérations de cluster pour optimiser les performances, contrôler les coûts et garantir une haute disponibilité. Les opérations de cluster vous permettent de redimensionner, de suspendre, de reprendre ou même de recréer des clusters en fonction de l'évolution de vos besoins en matière d'entreposage de données.

Les cas d'utilisation courants incluent la mise à l'échelle de la capacité de calcul pour les pics de charge de travail, la suspension des clusters pendant les périodes d'inactivité pour réduire les coûts et la recréation de clusters avec différentes configurations ou dans différentes zones de disponibilité pour la reprise après sinistre. Les sections suivantes décrivent en détail l'exécution de diverses opérations de cluster pour gérer efficacement votre environnement Amazon Redshift.

Création d'un cluster

Avec Amazon Redshift, vous pouvez créer un cluster alloué pour lancer un nouvel entrepôt de données. Un cluster alloué est un ensemble de ressources informatiques appelées nœuds, qui sont organisées en un seul système MPP (Massively Parallel Processing).

Avant de créer un cluster, listez Clusters Amazon Redshift provisionnés et Clusters et nœuds dans Amazon Redshift.

Pour créer un cluster

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters. Les clusters associés à votre compte dans la AWS région actuelle sont répertoriés. Un sous-ensemble des propriétés de chaque cluster s'affiche dans les colonnes de la liste.
3. Choisissez Créer un cluster pour créer un cluster.
4. Suivez les instructions sur la page de la console pour entrer les propriétés dans Configuration du cluster.

   L'étape suivante décrit une console Amazon Redshift qui s'exécute dans un nœud compatible avec les types de Région AWS nœuds RG ou RA3. Pour obtenir la liste des types de Régions AWS nœuds RG ou RA3 compatibles, consultez les sections Disponibilité des types de nœuds RG dans AWS les régions et disponibilité des types de nœuds RA3 dans les AWS régions dans le guide de gestion Amazon Redshift.

Si vous ne savez pas quelle taille donner à votre cluster, choisissez Help me choose (Aidez-moi à choisir). Cette opération lance un calculateur de dimensionnement qui vous pose des questions sur la taille et les caractéristiques d'interrogation des données que vous prévoyez de stocker dans votre entrepôt des données. Si vous connaissez la taille requise de votre cluster (c'est-à-dire le type et le nombre de nœuds), choisissez I'll choose (Je vais choisir). Choisissez ensuite le Node type (Type de nœud) et le nombre de Nodes (Nœuds) pour dimensionner votre cluster pour la preuve de concept.

> **Note**
>
> Si votre organisation est éligible et que votre cluster est créé dans une Région AWS où Amazon Redshift sans serveur n'est pas disponible, vous pourrez peut-être créer un cluster dans le cadre du programme d'essai gratuit d'Amazon Redshift. Choisissez Production ou Essai gratuit pour répondre à la question Quelle est l'utilisation prévue de ce cluster ? Lorsque vous choisissez l'essai gratuit, vous créez une configuration avec le type de nœud ra3.large. Pour plus d'informations sur le choix d'un essai gratuit, consultez Essai gratuit d'Amazon Redshift. Pour obtenir la liste des Régions AWS endroits où Amazon Redshift Serverless est disponible, consultez les points de terminaison répertoriés pour l'API Redshift Serverless dans le. Référence générale d'Amazon Web Services

5. Dans la section Configuration de la base de données, spécifiez une valeur pour Nom de l'utilisateur administrateur. Pour Mot de passe administrateur, choisissez l'une des options suivantes :

   - Générez un mot de passe : utilisez un mot de passe généré par Amazon Redshift.
   - Ajouter manuellement un mot de passe d'administrateur : utilisez votre propre mot de passe.
   - Gérez les informations d'identification d'administrateur dans AWS Secrets Manager : Amazon Redshift les utilise AWS Secrets Manager pour générer et gérer votre mot de passe d'administrateur. L'utilisation AWS Secrets Manager pour générer et gérer le secret de votre mot de passe entraîne des frais. Pour plus d'informations sur AWS Secrets Manager les tarifs, consultez la section AWS Secrets Manager Tarification.

6. (Facultatif) Suivez les instructions sur la page de la console pour entrer les propriétés dans Autorisations du cluster. Fournissez des autorisations de cluster si votre cluster a besoin d'accéder à d'autres AWS services pour vous, par exemple pour charger des données depuis Amazon S3.

7. Choisissez Créer un cluster pour créer le cluster. Le cluster peut prendre plusieurs minutes pour être prêt à être utilisé.

Configurations supplémentaires

Lorsque vous créez un cluster, vous pouvez spécifier des propriétés supplémentaires afin de le personnaliser. Vous trouverez plus de détails sur certaines de ces propriétés dans la liste suivante.

Type d’adresse IP

Choisissez le type d’adresse IP de votre cluster. Vous pouvez choisir de faire en sorte que vos ressources communiquent uniquement via le protocole d’adressage IPv4 ou choisir le mode double pile, qui permet à vos ressources de communiquer à la fois via IPv4 et IPv6. Cette fonctionnalité n'est disponible que dans les régions AWS GovCloud (US-East) et AWS GovCloud (US-West). Pour plus d'informations sur AWS les régions, voir Régions et zones de disponibilité.

Cloud privé virtuel (VPC)

Choisissez un VPC qui possède un groupe de sous-réseaux de cluster. Une fois que le cluster a été créé, le groupe de sous-réseaux de cluster ne peut pas être modifié.

Groupes de paramètres

Choisissez un groupe de paramètres de cluster à associer au cluster. Si vous n’en choisissez pas, le cluster utilise le groupe de paramètres par défaut.

Chiffrement

Choisissez si vous voulez chiffrer toutes les données au sein du cluster et ses instantanés. Si vous laissez le paramètre par défaut, Aucun, le chiffrement n’est pas activé. Si vous souhaitez activer le chiffrement, choisissez si vous souhaitez utiliser AWS Key Management Service (AWS KMS) ou un module de sécurité matériel (HSM), puis configurez les paramètres associés. Pour plus d’informations sur le chiffrement dans Amazon Redshift, consultez Chiffrement de base de données Amazon Redshift.

- KMS

  Choisissez Utiliser AWS Key Management Service (AWS KMS) si vous souhaitez activer le chiffrement et l'utiliser AWS KMS pour gérer votre clé de chiffrement. Sélectionnez également la clé à utiliser. Vous pouvez sélectionner une clé par défaut, une clé issue du compte actuel ou une clé issue d’un autre compte.

> **Note**
>
> Si vous souhaitez utiliser une clé d'un autre AWS compte, entrez le nom de ressource Amazon (ARN) correspondant à la clé à utiliser. Vous devez avoir l'autorisation d'utiliser la clé. Pour plus d'informations sur l'accès aux clés AWS KMS, consultez la section Contrôle de l'accès à vos clés dans le Guide du AWS Key Management Service développeur.

Pour plus d'informations sur l'utilisation des clés de AWS KMS chiffrement dans Amazon Redshift, consultez. Chiffrement en utilisant AWS KMS

- HSM

  Choisissez HSM si vous voulez activer le chiffrement et utiliser un module de sécurité matérielle (HSM) pour gérer votre clé de chiffrement.

  Si vous choisissez HSM, choisissez les valeurs de Connexion HSM et Certificat de client HSM. Ces valeurs sont requises pour Amazon Redshift et le module HSM de façon à former une connexion approuvée au travers de laquelle la clé de cluster peut être transmise. La connexion et le certificat de client HSM doivent être configurés dans Amazon Redshift avant que vous ne lanciez un cluster. Pour plus d'informations sur la configuration des connexions et des certificats de clients HSM, consultez Chiffrement à l'aide de modules de sécurité matérielle.

Suivi de maintenance

Vous pouvez choisir si la version de cluster utilisée doit être Actuelle, Finale ou parfois Préliminaire.

Surveillance

Vous pouvez choisir de créer ou non des CloudWatch alarmes.

Configurer un instantané inter-région

Vous pouvez choisir d'activer des instantanés inter-régions.

Période de conservation de l'instantané automatique

Vous pouvez choisir le nombre de jours de conservation de ces instantanés dans un délai maximum de 35 jours. Si le type de nœud est DC2, vous pouvez choisir zéro (0) jour pour ne pas créer d'instantanés automatiques.

Période de conservation de l’instantané manuel

Vous pouvez choisir le nombre de jours ou l’option `Indefinitely` pour conserver ces instantanés.

Ressources de calcul supplémentaires pour des optimisations automatiques

Vous pouvez choisir d'allouer des ressources de calcul supplémentaires pour effectuer des optimisations automatiques, même pendant les périodes d'utilisation intensive. Pour plus d'informations, consultez la section Allocation de ressources de calcul supplémentaires pour l'optimisation automatique des bases de données dans le manuel Amazon Redshift Database Developer Guide.

Création d’une alarme d’espace disque

Vous pouvez surveiller l’utilisation de l’espace disque et définir des alarmes pour être averti lorsque l’espace disque dépasse un seuil spécifié pour un cluster. La création d’une alarme d’utilisation de l’espace disque vous permet de gérer de manière proactive la capacité de stockage et d’éviter les problèmes liés à un espace disque insuffisant, tels que les échecs de requêtes ou les erreurs d’ingestion de données. La procédure suivante vous guide au cours du processus de création d’une alarme d’utilisation de l’espace disque.

Pour créer une alarme relative à l’utilisation de l’espace disque pour un cluster

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Alarmes.
3. Pour Actions, choisissez Créer une alarme. La page Créer une alarme apparaît.
4. Suivez les instructions indiquées sur la page.
5. Sélectionnez Créer une alerte.

Affichage d’un cluster

L’affichage d’un cluster vous permet de surveiller et de gérer la configuration, l’état et les indicateurs de performance de votre cluster. En consultant les détails du cluster, vous pouvez obtenir des informations sur l’utilisation des ressources, les temps d’exécution des requêtes et l’état du système. La procédure suivante illustre comment accéder aux informations de cluster.

Pour afficher un cluster

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters. Les clusters associés à votre compte dans la AWS région actuelle sont répertoriés. Un sous-ensemble des propriétés de chaque cluster s'affiche dans les colonnes de la liste. Si vous n'avez pas de clusters, choisissez Créer un cluster pour en créer un.
3. Choisissez le nom du cluster dans la liste pour afficher plus de détails sur un cluster.

Modification d'un cluster

Lorsque vous modifiez un cluster, les modifications apportées aux options suivantes sont appliquées immédiatement :

- Groupes de sécurité VPC
- Accessible publiquement
- Mot de passe d'utilisateur administrateur
- Connexion HSM
- Certificat de client HSM
- Détails de maintenance
- Snapshot preferences (Préférences d'instantané)

Les modifications apportées aux options suivantes ne prennent effet qu'après le redémarrage du cluster :

- Identifiant du cluster

  Amazon Redshift redémarre le cluster automatiquement lorsque vous modifiez le champ Cluster identifier (Identifiant du cluster).
- Routage VPC amélioré

  Amazon Redshift redémarre le cluster automatiquement lorsque vous modifiez le champ Enhanced VPC routing (Routage VPC amélioré).
- Groupe de paramètres du cluster

- Type d’adresse IP

  Cette fonctionnalité n'est disponible que dans les régions AWS GovCloud (US-East) et AWS GovCloud (US-West). Pour plus d'informations sur AWS les régions, voir Régions et zones de disponibilité.

Si vous diminuez la période de conservation des instantanés automatiques, ceux existants dont les paramètres tombent en dehors de la nouvelle période de conservation sont supprimés. Pour plus d’informations, consultez Instantanés et sauvegardes Amazon Redshift.

Pour obtenir plus d’informations sur les propriétés des clusters, consultez Configurations supplémentaires.

Pour modifier un cluster

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters.
3. Choisissez le cluster à modifier.
4. Choisissez Modifier. La page Edit cluster (Modifier le cluster) s’affiche.
5. Mettez à jour les propriétés du cluster. Vous pouvez modifier notamment les propriétés suivantes :

   - Identifiant du cluster
   - Conservation des instantanés
   - Relocalisation du cluster

   Pour modifier les paramètres de Réseau et sécurité, Maintenance et Configurations de base de données, la console fournit des liens vers l’onglet de détails de cluster approprié.
6. Sélectionnez Enregistrer les modifications.

Redimensionnement d’un cluster

Au fur et à mesure que vos performances et capacités d’entrepôt des données changent, vous pouvez redimensionner votre cluster pour tirer le meilleur parti des options de calcul et de stockage d’Amazon Redshift.

Lorsque vous redimensionnez un cluster, vous spécifiez un certain nombre de nœuds ou un type de nœud différent de la configuration actuelle du cluster. Pendant le redimensionnement du cluster, vous ne pouvez exécuter aucune écriture ni aucune read/write requête sur le cluster ; vous ne pouvez exécuter que des requêtes de lecture.

Pour plus d'informations sur le redimensionnement des clusters, y compris à travers le processus de redimensionnement des clusters à l'aide de différentes approches, consultez Redimensionnement d'un cluster.

Pour redimensionner un cluster

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters.
3. Choisissez le cluster à redimensionner.
4. Pour Actions, choisissez Redimensionner. La page Redimensionner le cluster s'affiche.
5. Suivez les instructions indiquées sur la page. Vous pouvez redimensionner le cluster maintenant, une fois à un moment donné, ou augmenter et diminuer sa taille selon un programme.
6. Selon vos choix, choisissez Resize now (Redimensionner maintenant) ou Schedule resize (Planifier le redimensionnement).

Si vous avez des nœuds réservés, vous pouvez passer à des nœuds réservés RG ou RA3. Vous pouvez le faire lorsque vous utilisez la console pour effectuer une restauration à partir d'un instantané ou pour effectuer un redimensionnement Elastic. Vous pouvez utiliser la console pour vous guider dans ce processus. Pour plus d'informations sur la mise à niveau vers les types de nœuds RG ou RA3, consultez la section Mise à niveau vers les types de nœuds RG ou RA3.

Lorsque vous effectuez une opération de redimensionnement pour passer d'un type de DC2.large nœud à un type de RA3.large nœud, Amazon Redshift convertit automatiquement les clés de tri entrelacées en clés de tri composées. Cette conversion permet d'accéder à la fonctionnalité de mise à l'échelle de la simultanéité, qui ne prend pas en charge les requêtes sur les tables avec des clés de tri entrelacées. Bien que cette conversion automatique garantisse la compatibilité avec les fonctionnalités RA3, elle peut avoir un impact sur les modèles de performances de vos requêtes existants.

Si vous souhaitez conserver les clés de tri entrelacées après la mise à niveau vers les nœuds RA3, vous pouvez recréer vos tables avec la configuration de clé de tri souhaitée une fois l'opération de

redimensionnement terminée. Cependant, le choix de cette option signifie que vous ne pourrez pas utiliser la mise à l'échelle de la simultanéité pour ces tables.

Une opération de redimensionnement se décline en deux types :

- Elastic resize (Redimensionnement élastique) : vous pouvez ajouter ou supprimer des nœuds de votre cluster. Vous pouvez également modifier le type de nœud, par exemple des nœuds DC2 aux nœuds RG ou RA3. Un redimensionnement élastique s'effectue généralement rapidement, en dix minutes en moyenne. C'est pourquoi nous le recommandons en tant que première option. Lorsque vous effectuez un redimensionnement élastique, cela redistribue les tranches de données. Les tranches de données sont des partitions auxquelles de la mémoire et de l'espace disque sont alloués dans chaque nœud. Le redimensionnement élastique est approprié pour :
  - Add or reduce nodes in an existing cluster, but you don't change the node type (Ajouter ou réduire des nœuds dans un cluster existant, mais sans modifier le type de nœud) : ceci est généralement appelé un redimensionnement sur place. Lorsque vous effectuez ce type de redimensionnement, certaines requêtes en cours d'exécution se terminent, mais d'autres peuvent être supprimées dans le cadre de l'opération.
  - Change the node type for a cluster (Modifier le type de nœud d'un cluster) : lorsque vous modifiez le type de nœud, un instantané est créé et les données sont redistribuées à partir du cluster source vers un cluster composé du nouveau type de nœud. Au terme de cette opération, les requêtes en cours d'exécution sont supprimées. Tout comme le redimensionnement sur place, cette opération se termine rapidement.
- Classic resize (Redimensionnement classique) : vous pouvez changer le type de nœud, le nombre de nœuds ou les deux, de manière similaire au redimensionnement élastique. Le redimensionnement classique prend plus de temps, mais il peut être utile dans les cas où la modification du nombre de nœuds ou du type de nœud vers lequel migrer ne correspond pas aux limites du redimensionnement élastique. Cela peut par exemple s'appliquer lorsque la modification du nombre de nœuds est vraiment importante.

Rubriques

- Elastic resize (Redimensionnement élastique)
- Classic resize (Redimensionnement Classic)

Elastic resize (Redimensionnement élastique)

Lorsque vous ajoutez ou supprimez des nœuds du même type, une opération de redimensionnement élastique se déroule selon les étapes suivantes :

1. Le redimensionnement élastique prend un instantané du cluster. No-backup les tables ne sont prises en charge que pour les nœuds DC2. Pour les clusters RG et RA3, aucune table de sauvegarde n'est incluse dans le snapshot. Pour de plus amples informations, veuillez consulter Exclusion des tables des instantanés. Si votre cluster ne dispose pas d'instantané récent, car vous avez désactivé les instantanés automatiques, l'opération de sauvegarde peut prendre plus de temps. (Pour réduire au maximum le temps avant le début de l'opération de redimensionnement, nous vous recommandons d'activer les instantanés automatiques ou de créer un instantané manuel avant de démarrer le redimensionnement.) Lorsque vous démarrez un redimensionnement élastique et qu'une opération d'instantané est en cours, le redimensionnement élastique peut échouer si l'opération d'instantané ne se termine pas en quelques minutes. Pour plus d'informations, consultez Instantanés et sauvegardes Amazon Redshift.
2. L'opération fait migrer les métadonnées du cluster. Le cluster n'est pas disponible pendant quelques minutes. La majorité des requêtes sont temporairement interrompues et les connexions restent ouvertes. Il est toutefois possible que certaines requêtes soient supprimées. Cette étape est courte.
3. Les connexions de séance sont réactivées et les requêtes reprennent leur exécution.
4. Le redimensionnement élastique redistribue les données vers les tranches de nœuds en arrière-plan. Le cluster est disponible pour les opérations de lecture et d'écriture, mais certaines requêtes peuvent prendre plus de temps à s'exécuter.
5. Une fois l'opération terminée, Amazon Redshift envoie une notification d'événement.

Lorsque vous utilisez le redimensionnement élastique pour modifier le type de nœud, cela fonctionne de la même manière que lorsque vous ajoutez ou retirez des nœuds du même type. Tout d'abord, un instantané est créé. Un nouveau cluster cible est provisionné avec les dernières données de l'instantané, et les données sont transférées vers le nouveau cluster en arrière-plan. Pendant cette période, les données sont en lecture seule. Lorsque le redimensionnement est presque terminé, Amazon Redshift met à jour le point de terminaison pour désigner le nouveau cluster, et toutes les connexions au cluster source sont supprimées.

Il est peu probable qu'un redimensionnement élastique échoue. Cependant, en cas de panne, la restauration se fait automatiquement dans la majorité des cas sans intervention manuelle.

Si vous avez des nœuds réservés, par exemple des nœuds réservés DC2, vous pouvez effectuer une mise à niveau vers des nœuds réservés RA3 lorsque vous effectuez un redimensionnement. Vous pouvez le faire lorsque vous effectuez un redimensionnement élastique ou lorsque vous utilisez la console pour effectuer une restauration à partir d'un instantané. Cette console vous guide tout au long de ce processus. Pour plus d'informations sur la mise à niveau vers les types de nœuds RG ou RA3, consultez la section Mise à niveau vers les types de nœuds RG ou RA3.

Le redimensionnement élastique ne trie pas les tables ni ne récupère l'espace disque, et n'est donc pas un substitut d'une opération VACUUM. Pour plus d'informations, consultez Exécution de l'opération VACUUM sur les tables.

Le redimensionnement élastique présente les contraintes suivantes :

- Clusters de redimensionnement élastique et de partage de données – Lorsque vous ajoutez ou supprimez des nœuds sur un cluster qui est un producteur pour le partage de données, vous ne pouvez pas vous y connecter à partir des consommateurs pendant qu'Amazon Redshift migre les métadonnées du cluster. De même, si vous effectuez un redimensionnement élastique et que vous choisissez un nouveau type de nœud, le partage des données est indisponible pendant que les connexions sont supprimées et transférées vers le nouveau cluster cible. Dans les deux types de redimensionnement élastique, le producteur est indisponible pendant plusieurs minutes.
- Data transfer from a shared snapshot (Transfert de données à partir d'un instantané partagé) : pour exécuter un redimensionnement élastique sur un cluster qui transfère des données à partir d'un instantané partagé, au moins une sauvegarde doit être disponible pour le cluster. Vous pouvez afficher vos sauvegardes dans la liste des instantanés de la console Amazon Redshift, la commande de la CLI `describe-cluster-snapshots` ou l'opération d'API `DescribeClusterSnapshots`.
- Restriction de plate-forme : le redimensionnement élastique n'est disponible que pour les clusters qui utilisent la EC2-VPC plate-forme. Pour de plus amples informations, veuillez consulter Utiliser EC2 pour créer votre cluster.
- Storage considerations (Considérations en matière de stockage) : assurez-vous que votre nouvelle configuration de nœuds dispose de suffisamment de stockage pour les données existantes. Vous devrez peut-être ajouter des nœuds supplémentaires ou modifier la configuration.
- Source vs target cluster size (Taille de cluster source vs cible) : le nombre et le type de nœuds que vous pouvez redimensionner avec le redimensionnement élastique sont déterminées par le nombre de nœuds du cluster source et le type de nœud choisi pour le cluster redimensionné. Pour déterminer les configurations potentielles disponibles, vous pouvez utiliser la console. Ou vous pouvez utiliser la `describe-node-configuration-options` AWS CLI commande

avec l'`action-type resize-cluster`option. Pour en savoir plus sur la modification des métadonnées à l'aide de la console Amazon Redshift, consultez Redimensionnement d'un cluster.

L'exemple de commande de CLI suivant décrit les options de configuration disponibles. Dans cet exemple, le cluster nommé `mycluster` est un cluster `rg.4xl` à 8 nœuds.

```
aws redshift describe-node-configuration-options --cluster-identifier mycluster --
region eu-west-1 --action-type resize-cluster
```

Cette commande renvoie une liste d'options avec les types de nœud recommandés, le nombre de nœuds et l'utilisation du disque pour chaque option. Les configurations renvoyées peuvent varier selon le cluster d'entrée spécifique. Vous pouvez choisir l'une de ces configurations lorsque vous spécifiez les options de la commande CLI `resize-cluster`.

- Ceiling on additional nodes (Plafond sur les nœuds supplémentaires) : le redimensionnement élastique a des limites sur les nœuds que vous pouvez ajouter à un cluster. Par exemple, un cluster RG ou RA3 prend en charge le redimensionnement élastique jusqu'à quatre fois le nombre de nœuds. À titre d'exemple, vous pouvez ajouter un nœud à un cluster rg.4xl à 4 nœuds pour en faire un cluster à cinq nœuds, ou ajouter d'autres nœuds jusqu'à ce qu'il atteigne seize.

  > **Note**
  >
  > Les limites de croissance et de réduction sont basées sur le type de nœud d'origine et le nombre de nœuds du cluster d'origine ou de son dernier redimensionnement classique. Si un redimensionnement élastique dépasse les limites de croissance ou de réduction, utilisez un redimensionnement classique.

  Avec certains types de nœuds rg et ra3, vous pouvez augmenter le nombre de nœuds jusqu'à quatre fois le nombre existant. Concrètement, supposons que votre cluster se compose de nœuds ra3.4xlarge ou ra3.16xlarge. Vous pouvez utiliser le redimensionnement élastique pour augmenter à 32 le nombre de nœuds dans un cluster à 8 nœuds. Sinon, vous pouvez choisir une valeur en dessous de la limite. (Gardez à l'esprit que la possibilité de quadrupler le cluster dépend de la taille du cluster source.) Si votre cluster a des nœuds ra3.xlplus, la limite est le double.

  Tous les types de nœuds rg et ra3 permettent de réduire le nombre de nœuds à un quart du nombre existant. Par exemple, vous pouvez réduire la taille d'un cluster avec des nœuds ra3.4xlarge de 12 nœuds à 3, ou à un nombre au-dessus du minimum.

Le tableau suivant répertorie les limites d'augmentation et de réduction pour chaque type de nœud prenant en charge le redimensionnement élastique.

Type de nœud d'origine	Limite d'augmentation	Limite de réduction
rg.12 x large	4x	Jusqu'à un quart du nombre
rg.4 x large	4x	Jusqu'à un quart du nombre
rg.xlarge	2x	Jusqu'à la moitié du nombre
rg.large	2x	Jusqu'à la moitié du nombre
ra3.16xlarge	4x (de 4 à 16 nœuds, par exemple)	Jusqu'à un quart du nombre (de 16 à 4 nœuds, par exemple)
ra3.4xlarge	4x	Jusqu'à un quart du nombre
ra3.xlplus	2x (de 4 à 8 nœuds, par exemple)	Jusqu'à un quart du nombre
ra3.large	2x	Jusqu'à la moitié du nombre
dc2.8xlarge	2x	Jusqu'à la moitié du nombre (de 16 à 8 nœuds, par exemple)
dc2.large	2x	Jusqu'à la moitié du nombre

Note

Choix des types de nœuds existants lorsque vous redimensionnez un cluster RG ou RA3 : si vous tentez de redimensionner un cluster contenant des nœuds RG ou RA3 vers un autre type de nœud, tel que DC2, un message d'avertissement de validation apparaît dans la console et l'opération de redimensionnement ne sera pas terminée. En effet, le redimensionnement vers des types de nœuds existants n'est pas pris en charge. Cela vise à empêcher un client d'effectuer un redimensionnement vers un type de nœud obsolète

ou sur le point de l'être. Cela s'applique à la fois au redimensionnement élastique et au redimensionnement classique.

Classic resize (Redimensionnement Classic)

Le redimensionnement classique gère les cas où la modification de la taille du cluster ou du type de nœud n'est pas conforme au redimensionnement élastique. Lorsque vous effectuez un redimensionnement classique, Amazon Redshift crée un cluster cible et y migre vos données et métadonnées depuis le cluster source.

Le redimensionnement classique vers RG ou RA3 peut offrir une meilleure disponibilité

Le redimensionnement classique a été amélioré lorsque le type de nœud cible est RG ou RA3. Pour ce faire, utilisez une opération de sauvegarde et de restauration entre le cluster source et le cluster cible. Lorsque le redimensionnement commence, le cluster source redémarre et est indisponible pendant quelques minutes. Le cluster est ensuite disponible pour des opérations de lecture et d'écriture pendant que le redimensionnement continue en arrière-plan.

Vérification de votre cluster

Pour garantir les meilleures performances et les meilleurs résultats lorsque vous effectuez un redimensionnement classique vers un cluster RG ou RA3, complétez cette liste de contrôle. Si vous ne suivez pas la liste de contrôle, vous risquez de ne pas bénéficier de certains des avantages du redimensionnement classique avec des nœuds RG ou RA3, tels que la possibilité d'effectuer des opérations de lecture et d'écriture.

1. La taille des données doit être inférieure à 2 pétaoctets. (Un pétaoctet équivaut à 1 000 téraoctets.) Pour valider la taille de vos données, créez un instantané et vérifiez sa taille. Vous pouvez également exécuter la requête suivante pour vérifier la taille :

   ```
   SELECT
   sum(case when lower(diststyle) like ('%key%') then size else 0 end) distkey_blocks,
   sum(size) as total_blocks,
   ((distkey_blocks/(total_blocks*1.00)))*100 as Blocks_need_redist
   FROM svv_table_info;
   ```

   La table `svv_table_info` n'est visible que par les super-utilisateurs.

2. Avant de lancer un redimensionnement classique, assurez-vous de disposer d'un instantané manuel qui ne date pas de plus de 10 heures. Si ce n'est pas le cas, prenez un instantané.
3. L'instantané utilisé pour effectuer le redimensionnement classique ne peut pas être utilisé à des fins de restauration de table ou autres.
4. Le cluster doit se trouver dans un VPC.

Opérations de tri et de distribution résultant d'un redimensionnement classique vers RG ou RA3

Lors du redimensionnement classique vers RG ou RA3, les tables avec une distribution KEY migrées en tant que distribution EVEN sont reconverties dans leur style de distribution d'origine. La durée de cette opération dépend de la taille des données et de l'activité de votre cluster. Les charges de travail liées aux requêtes sont traitées en priorité par rapport à la migration des données. Pour plus d'informations, consultez Styles de distribution. Les lectures et les écritures dans la base de données fonctionnent au cours de ce processus de migration, mais le traitement des requêtes peut prendre plus de temps. Toutefois, la mise à l'échelle de la simultanéité peut améliorer les performances dans cette période en ajoutant des ressources pour les charges de travail liées aux requêtes. Vous pouvez voir la progression de la migration des données en consultant les résultats dans les vues SYS_RESTORE_STATE et SYS_RESTORE_LOG. Vous trouverez plus d'informations sur la surveillance ci-dessous.

Une fois le cluster entièrement redimensionné, le comportement de tri suivant se produit :

- Si le redimensionnement entraîne la présence d'un plus grand nombre de tranches dans le cluster, les tables de distribution KEY ne sont partiellement pas triées, mais les tables EVEN restent triées. De plus, les informations relatives à la quantité de données triées peuvent ne pas être à jour, directement après le redimensionnement. Après avoir récupéré les clés, l'opération automatic vacuum trie la table au fil du temps.
- Si le redimensionnement entraîne moins de tranches dans le cluster, les tables de distribution KEY ne partiellement non triées. L'opération automatic vacuum trie la table au fil du temps.

Pour plus d'informations sur l'opérations automatic table vacuum, consultez Exécution de l'opération VACUUM sur les tables. Pour plus d'informations sur les tranches dans les nœuds de calcul, consultez Architecture système de l'entrepôt des données.

Étapes de redimensionnement classiques lorsque le cluster cible est RG ou RA3

Le redimensionnement classique comprend les étapes suivantes, lorsque le type de cluster cible est RG ou RA3 et que vous répondez aux conditions requises détaillées dans la section précédente.

1. Migration initiée du cluster source vers le cluster cible. Lorsque le nouveau cluster cible est provisionné, Amazon Redshift envoie une notification d'événement indiquant que le redimensionnement a commencé. Il redémarre votre cluster existant, ce qui ferme toutes les connexions. Si votre cluster existant est un cluster producteur d'unités de partage des données, les connexions avec les clusters consommateur sont également fermées. Le redémarrage prend quelques minutes.
2. Après le redémarrage, la base de données est disponible en lecture et en écriture. De plus, le partage de données reprend, ce qui prend quelques minutes supplémentaires.
3. Les données sont migrées vers le cluster cible. Lorsque le type de nœud cible est RG ou RA3, les lectures et les écritures sont disponibles pendant la migration des données.
4. Lorsque le processus de redimensionnement est presque terminé, Amazon Redshift met à jour le point de terminaison vers le cluster cible et toutes les connexions sont supprimées. Le cluster cible devient le producteur pour le partage des données.
5. Le redimensionnement se termine. Amazon Redshift envoie une notification d'événement.

Vous pouvez afficher la progression du redimensionnement dans la console Amazon Redshift. Le temps nécessaire au redimensionnement d'un cluster dépend de la quantité de données.

> **Note**
>
> Choix des types de nœuds existants lorsque vous redimensionnez un cluster RG ou RA3 : si vous tentez de redimensionner un cluster contenant des nœuds RG ou RA3 vers un autre type de nœud, tel que DC2, un message d'avertissement de validation apparaît dans la console et l'opération de redimensionnement ne sera pas terminée. En effet, le redimensionnement vers des types de nœuds existants n'est pas pris en charge. Cela vise à empêcher un client d'effectuer un redimensionnement vers un type de nœud obsolète ou sur le point de l'être. Cela s'applique à la fois au redimensionnement élastique et au redimensionnement classique.

Surveillance d'un redimensionnement classique lorsque le cluster cible est RG ou RA3

Pour surveiller un redimensionnement classique d'un cluster provisionné en cours, y compris la distribution KEY, utilisez SYS_RESTORE_STATE. Il indique le pourcentage d'achèvement de la table en cours de conversion. Vous devez être un super-utilisateur pour accéder aux données.

Supprimez les tables dont vous n'avez pas besoin lorsque vous effectuez un redimensionnement classique. Ainsi, les tables existantes peuvent être distribuées plus rapidement.

Étapes de redimensionnement classiques lorsque le cluster cible n'est pas RG ou RA3

Le redimensionnement classique consiste en ce qui suit, lorsque le type de nœud cible est autre que RG ou RA3, comme DC2, par exemple.

1. Migration initiée du cluster source vers le cluster cible. Lorsque le nouveau cluster cible est provisionné, Amazon Redshift envoie une notification d'événement indiquant que le redimensionnement a commencé. Il redémarre votre cluster existant, ce qui ferme toutes les connexions. Si votre cluster existant est un cluster producteur d'unités de partage des données, les connexions avec les clusters consommateur sont également fermées. Le redémarrage prend quelques minutes.

   Notez que toute relation de base de données, telle qu'une table ou une vue matérialisée, créée avec `BACKUP NO` n'est pas conservée lors du redimensionnement classique. Pour plus d'informations, consultez CREATE MATERIALIZED VIEW.
2. Après le redémarrage, la base de données est disponible en lecture seule. Le partage de données reprend, ce qui prend quelques minutes supplémentaires.
3. Les données sont migrées vers le cluster cible. La base de données reste en lecture seule.
4. Lorsque le processus de redimensionnement est presque terminé, Amazon Redshift met à jour le point de terminaison vers le cluster cible et toutes les connexions sont supprimées. Le cluster cible devient le producteur pour le partage des données.
5. Le redimensionnement se termine. Amazon Redshift envoie une notification d'événement.

Vous pouvez afficher la progression du redimensionnement dans la console Amazon Redshift. Le temps nécessaire au redimensionnement d'un cluster dépend de la quantité de données.

> **Note**
>
> Le redimensionnement d'un cluster contenant une grande quantité de données peut prendre des jours, voire des semaines, lorsque le cluster cible n'est pas RG ou RA3, ou s'il ne répond pas aux conditions requises pour un cluster cible RA3 détaillées dans la section précédente. Notez également que la capacité de stockage utilisée pour le cluster peut augmenter après un redimensionnement classique. Il s'agit d'un comportement normal du système lorsque le cluster dispose de tranches de données supplémentaires à la suite du redimensionnement classique. Cette utilisation de capacité supplémentaire peut se produire même lorsque le nombre de nœuds du cluster est inchangé.

Redimensionnement élastique vs redimensionnement classique

La table suivante compare le comportement entre les deux types de redimensionnement.

Comportement	Elastic resize (Redimensionnement élastique)	Classic resize (Redimensionnement Classic)	Commentaires
Conservation des données système	Le redimensionnement élastique conserve les données des journaux système.	Le redimensionnement classique ne conserve pas les tables et les données système.	Si la journalisation des audits est activée dans votre cluster source, vous pouvez continuer à accéder

Comportement	Elastic resize (Redimensionnement élastique)	Classic resize (Redimensionnement Classic)	Comme res
			aux journaux dans Amazon S3 ou dans Amazon S3 CloudWatch, après un redimensionnement. Vous pouvez conserver ou supprimer ces journaux, selon ce que vos stratégies de données spécifient.

Comportement	Elastic resize (Redimensionnement élastique)	Classic resize (Redimensionnement Classic)	Commentaires
Modification des types de nœuds	Redimensionnement élastique, lorsque le type de nœud ne change pas : In-place redimensionnez, et la plupart des requêtes sont conservées. Pour le redimensionnement élastique, avec un nouveau type de nœud sélectionné : un nouveau cluster est créé. Les requêtes sont supprimées à la fin du processus de redimensionnement.	Pour le redimensionnement classique : un nouveau cluster est créé. Les requêtes sont supprimées lors du processus de redimensionnement.	

Comportement	Elastic resize (Redimensionnement élastique)	Classic resize (Redimensionnement Classic)	Comme res
Conservation des sessions et des requêtes	Le redimensionnement élastique conserve les sessions et les requêtes lorsque le type de nœud est identique dans le cluster source et le cluster cible. Si vous choisissez un nouveau type de nœud, les requêtes sont supprimées.	Le redimensionnement classique ne conserve pas les sessions et les requêtes. Les requêtes sont supprimées.	Lorsque des requêtes sont supprimées, une dégradation des performances est possible. Il est préférable d'effectuer une opération de redimensionnement pendant une période de faible utilisation.

Comportement	Elastic resize (Redimensionnement élastique)	Classic resize (Redimensionnement Classic)	Comme res
Annulation d'une opération de redimensionnement	Il n'est pas possible d'annuler un redimensionnement élastique.	Vous pouvez annuler une opération de redimensionnement avant qu'elle se termine. Pour ce faire, choisissez Cancel resize (Annuler le redimensionnement) dans les détails du cluster de la console Amazon Redshift.	Le temps nécessaire pour annuler un redimensionnement dépend de la phase de l'opération de redimensionnement où vous vous trouvez quand vous annulez. Lorsque vous faites cela, le cluster n'est

Comportement	Elastic resize (Redimensionnement élastique)	Classic resize (Redimensionnement Classic)	Commeres
			pas disponible tant que l'opération d'annulation n'est pas terminée. Si l'opération de redimensionnement est en phase finale, vous ne pouvez pas l'annuler. Pour le redimensionnement classique vers

Comportement	Elastic resize (Redimensionnement élastique)	Classic resize (Redimensionnement Classic)	Commeres
			un cluster RG ou RA3, vous ne pouvez pas annuler.

Planification d’un redimensionnement

Vous pouvez planifier des opérations de redimensionnement pour votre cluster afin de l’augmenter pour anticiper une utilisation élevée ou de le réduire pour diminuer les coûts. La planification fonctionne à la fois pour le redimensionnement élastique et le redimensionnement classique. Vous pouvez configurer une planification dans la console Amazon Redshift. Pour plus d’informations, consulte Redimensionnement d’un cluster dans la section Gestion des clusters à l’aide de la console. Vous pouvez également utiliser AWS CLI les opérations de l'API Amazon Redshift pour planifier un redimensionnement. Pour plus d'informations, consultez la section create-scheduled-action dans la référence des AWS CLI commandes ou dans la référence des API CreateScheduledActionAmazon Redshift.

Capture instantanée, restauration et redimensionnement

Le redimensionnement élastique est la méthode la plus rapide pour redimensionner un cluster Amazon Redshift. Si le redimensionnement élastique n’est pas une option et que vous avez besoin d’un accès quasiment constant en écriture à votre cluster, utilisez les opérations de capture instantanée et de restauration décrites dans la section suivante. Cette approche requiert que les données écrites sur le cluster source une fois que l’instantané a été pris soient copiées manuellement sur le cluster cible après le basculement. En fonction de la durée de la copie, vous devrez peut-être répéter l’opération plusieurs fois jusqu’à ce que vous ayez les mêmes données dans les deux

clusters. Ensuite, vous pourrez effectuer le basculement vers le cluster cible. Ce processus peut avoir un impact négatif sur les requêtes existantes jusqu'à ce que l'ensemble complet des données soit disponible dans le cluster cible. Toutefois, il réduit au maximum le temps pendant lequel vous ne pouvez pas écrire dans la base de données.

L'approche via les instantanés, la restauration et le redimensionnement Classic utilise le processus suivant :

1. Prenez un instantané de votre cluster existant. Le cluster existant est le cluster source.
2. Notez l'heure de prise de l'instantané. Cette opération signifie que vous pourrez identifier plus tard le point où vous devrez reprendre les processus d'extraction, de transformation et de chargement (ETL) pour charger les éventuelles données post-instantané dans la base de données cible.
3. Restaurez l'instantané dans un nouveau cluster. Ce nouveau cluster est le cluster cible. Vérifiez que l'exemple de données existe dans le cluster cible.
4. Redimensionnez le cluster cible. Choisissez les nouveaux type de nœud, nombre de nœuds et autres paramètres du cluster cible.
5. Passez en revue les charges de vos processus ETL qui se sont produits après que vous avez pris un instantané du cluster source. Veillez à recharger les mêmes données, dans le même ordre, dans le cluster cible. Si vous avez des charges de données en cours, répétez ce processus plusieurs fois jusqu'à ce que les données soient les mêmes dans les clusters source et cible.
6. Arrêtez toutes les requêtes en cours d'exécution sur le cluster source. Pour ce faire, vous pouvez redémarrer le cluster, ou vous connecter en tant que super-utilisateur et utiliser les commandes PG_CANCEL_BACKEND et PG_TERMINATE_BACKEND. Le redémarrage du cluster est la solution la plus simple pour vous assurer que le cluster n'est pas disponible.
7. Renommez le cluster source. Par exemple, renommez-le de `examplecluster` en `examplecluster-source`.
8. Renommez le cluster cible afin d'utiliser le nom du cluster source avant de le renommer. Par exemple, renommez le cluster cible en `examplecluster`. À partir de cet instant, toutes les applications qui utilisent le point de terminaison contenant `examplecluster` se connectent au cluster cible.
9. Supprimez le cluster source après que vous avez basculé sur le cluster cible et vérifiez que tous les processus fonctionnent comme prévu.

Sinon, vous pouvez renommer les clusters source et cible avant de recharger les données dans le cluster cible. Cette approche fonctionne si vous n'êtes pas soumis à une exigence selon laquelle tous

les systèmes et rapports dépendants doivent être immédiatement à jour avec ceux du cluster cible. Dans ce cas, l'étape 6 est déplacée à la fin du processus décrit précédemment.

Le processus consistant à renommer le cluster n'est nécessaire que si vous voulez que les applications continuent à utiliser le même point de terminaison pour se connecter au cluster. S'il ne s'agit pas de l'une de vos exigences, vous pouvez à la place mettre à jour toutes les applications qui se connectent au cluster afin d'utiliser le point de terminaison du cluster cible sans modifier le nom du cluster.

La réutilisation d'un nom de cluster présente deux avantages. Premièrement, vous n'avez pas besoin de mettre à jour les chaînes de connexion d'application, car le point de terminaison ne change pas, même si le cluster sous-jacent change. Ensuite, les éléments connexes tels que les CloudWatch alarmes Amazon et les notifications Amazon Simple Notification Service (Amazon SNS) sont liés au nom du cluster. Ce lien signifie que vous pouvez continuer à utiliser les mêmes alarmes et notifications que celles que vous avez configurées pour le cluster. Cette poursuite de l'utilisation est principalement une préoccupation dans les environnements de production où vous voulez avoir la possibilité de redimensionner le cluster sans avoir à reconfigurer les éléments connexes, tels que les alarmes et les notifications.

Renommer un cluster

Vous pouvez renommer un cluster si vous souhaitez que le cluster utilise un autre nom. Comme le point de terminaison de votre cluster inclut le nom du cluster (également appelé identificateur de cluster), le point de terminaison se met à utiliser le nouveau nom une fois que l'opération de modification du nom se termine. Par exemple, si vous avez un cluster nommé `examplecluster` et que vous le renommez `newcluster`, le point de terminaison utilisera l'identificateur `newcluster`. Toutes les applications qui se connectent au cluster doivent être mises à jour avec le nouveau point de terminaison.

Vous pouvez renommer un cluster si vous voulez modifier le cluster auquel se connectent vos applications sans devoir changer le point de terminaison de ces applications. Dans ce cas, vous devez d'abord renommer le cluster d'origine, puis modifier le deuxième cluster pour réutiliser le nom du cluster d'origine avant de le renommer. Cela est nécessaire, car l'identifiant de cluster doit être unique au sein de votre compte et de la région (le cluster d'origine et le second cluster ne peuvent pas avoir le même nom). Vous pouvez agir ainsi si vous restaurez un cluster à partir d'un instantané et ne voulez pas modifier les propriétés de connexion d'applications dépendantes.

> **Note**
>
> Si vous supprimez le cluster d'origine, vous êtes responsable de la suppression des instantanés de cluster indésirables.

Lorsque vous renommez un cluster, l'état du cluster devient `renaming` jusqu'à la fin du processus. L'ancien nom DNS qui a été utilisé par le cluster est immédiatement supprimé, même s'il peut demeurer mis en cache pendant quelques minutes. Le nouveau nom DNS du cluster renommé devient effectif au bout de 10 minutes environ. Le cluster renommé n'est pas disponible jusqu'à ce que le nouveau nom ne devienne effectif. Le cluster est redémarré et toutes les connexions existantes au cluster sont supprimées. Une fois l'opération terminée, le point de terminaison est modifié pour utiliser le nouveau nom. Pour cette raison, vous devez arrêter l'exécution des requêtes avant de démarrer la définition du nouveau nom et la redémarrer une fois le nouveau nom créé.

Les instantanés de cluster sont conservés, et tous les instantanés associés à un cluster demeurent associés à ce cluster après qu'il a été renommé. Supposons que vous disposiez d'un cluster qui dessert votre base de données de production et que ce cluster ait plusieurs instantanés. Si vous renommez le cluster, puis le remplacez dans l'environnement de production par un instantané, le cluster que vous avez renommé continue de conserver les instantanés existants qui lui sont associés.

CloudWatch Les alarmes Amazon et les notifications d'événements Amazon Simple Notification Service (Amazon SNS) sont associées au nom du cluster. Si vous renommez le cluster, vous devez mettre à jour ces informations en conséquence. Vous pouvez mettre à jour les CloudWatch alarmes dans la CloudWatch console, et vous pouvez mettre à jour les notifications d'événements Amazon SNS dans la console Amazon Redshift dans le volet Événements. Les données de charge et de requête du cluster continuent d'afficher les données antérieures et postérieures à l'attribution du nouveau nom. Cependant, les données de performance sont réinitialisées une fois le processus d'attribution de nouveau nom terminé.

Pour plus d'informations, consultez Modification d'un cluster.

Mise à niveau de la version d'un cluster

Vous pouvez effectuer une mise à niveau de la version de maintenance d'un cluster qui a une valeur de Statut de publication de Nouvelle version disponible. Lorsque vous mettez à niveau la version de maintenance, vous pouvez choisir de mettre à niveau immédiatement ou la mise à niveau lors de la prochaine fenêtre de maintenance.

> **Important**
>
> Si vous mettez à niveau immédiatement, votre cluster sera hors ligne jusqu'à ce que la mise à niveau soit terminée.

Pour vous mettre à niveau vers une nouvelle version de cluster

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters.
3. Choisissez le cluster à mettre à niveau.
4. Pour Actions, choisissez Mettre à niveau la version du cluster. La page Mettre à niveau la version du cluster.
5. Suivez les instructions indiquées sur la page.
6. Choisissez Mettre à niveau la version du cluster.

Suspension et reprise d'un cluster

Si vous disposez d'un cluster qui ne doit être disponible qu'à des moments spécifiques, vous pouvez le mettre en pause et le reprendre ultérieurement. Pendant que le cluster est suspendu, la facturation à la demande est suspendue. Seul le stockage du cluster entraîne des frais. Pour plus d'informations sur la tarification, consultez la Page de tarification Amazon Redshift.

Lorsque vous mettez en pause un cluster, Amazon Redshift crée un instantané, commence à mettre fin aux requêtes et met le cluster en pause. Si vous supprimez un cluster suspendu sans demander un instantané final, vous ne pouvez pas restaurer le cluster. Vous ne pouvez pas annuler ou restaurer après une pause ou reprendre une opération après son lancement.

Vous pouvez suspendre et reprendre un cluster sur la console Amazon Redshift, avec ou avec les opérations AWS CLI d'API Amazon Redshift.

Vous pouvez planifier des actions pour interrompre et reprendre un cluster. Lorsque vous utilisez la nouvelle console Amazon Redshift pour créer une planification périodique pour interrompre et reprendre, deux actions planifiées sont créées pour la plage de dates que vous choisissez. Les noms d'actions planifiées sont suffixés par `-pause` et `-resume`. La longueur totale du nom doit correspondre à la taille maximale d'un nom d'action planifiée.

Vous ne pouvez pas mettre en pause les types de clusters suivants :

- EC2-Classic clusters.
- Clusters qui ne sont pas actifs, par exemple un cluster en cours de modification.
- Clusters du module de sécurité matériel (HSM)
- Clusters dont les instantanés automatisés sont désactivés.

Lorsque vous décidez de mettre un cluster en pause, tenez compte des éléments suivants :

- Les connexions ou requêtes au cluster ne sont pas disponibles.
- Vous ne pouvez pas voir les informations de surveillance des requêtes d'un cluster mis en pause sur la console Amazon Redshift.
- Vous ne pouvez pas modifier un cluster suspendu. Les actions planifiées sur le cluster ne sont pas effectuées. Il s'agit notamment de créer des instantanés, de redimensionner les clusters et d'effectuer des opérations de maintenance de cluster.
- Les métriques matérielles ne sont pas créées. Mettez à jour vos CloudWatch alarmes si vous avez défini des alarmes en fonction de mesures manquantes.
- Vous ne pouvez pas copier les derniers instantanés automatisés d'un cluster suspendu vers des instantanés manuels.
- Pendant qu'un cluster est en pause, il ne peut pas être repris tant que l'opération de pause n'est pas terminée.
- Lorsque vous mettez en pause un cluster, la facturation est suspendue. Toutefois, l'opération de pause se termine généralement en 15 minutes, selon la taille du cluster.
- Les journaux d'audit sont archivés et ne sont pas restaurés à la reprise.
- Après la suspension d'un cluster, les traces et les journaux peuvent ne pas être disponibles pour résoudre les problèmes survenus avant la suspension.
- Si vous gérez vos informations d'identification d'administrateur à l'aide de votre cluster AWS Secrets Manager et que vous le suspendez, le secret de votre cluster ne sera pas supprimé et vous continuerez à être facturé pour ce secret. Pour plus d'informations sur la gestion de votre mot de passe administrateur Redshift avec AWS Secrets Manager, consultez. Gestion des mots de passe d'administration Amazon Redshift à l'aide de AWS Secrets Manager
- No-backup les tables du cluster sont restaurées lors de la reprise pour les types d'instances RG et RA3. Elles ne sont pas restaurées lors de la reprise pour les types d'instances DC2. Pour plus d'informations sur les tables sans sauvegarde, consultez Exclusion des tables des instantanés.

Lorsque vous reprenez un cluster, tenez compte des éléments suivants :

- La version de cluster du cluster repris est mise à jour vers la version de maintenance basée sur la fenêtre de maintenance du cluster.
- Si vous supprimez le sous-réseau associé à un cluster en pause, vous pouvez avoir un réseau incompatible. Dans ce cas, restaurez votre cluster à partir du dernier instantané.
- Si vous supprimez une adresse IP élastique pendant que le cluster est suspendu, une nouvelle adresse IP élastique est demandée.
- Si Amazon Redshift ne parvient pas à reprendre le cluster avec son interface réseau Elastic précédente, Amazon Redshift essaie d'en allouer un nouveau.
- Lorsque vous reprenez un cluster, les adresses IP de votre nœud peuvent changer. Vous devrez peut-être mettre à jour vos paramètres VPC pour prendre en charge ces nouvelles adresses IP pour des fonctionnalités telles que COPY depuis Secure Shell (SSH) ou COPY depuis Amazon EMR.
- Si vous essayez de reprendre un cluster qui n'est pas suspendu, l'opération de reprise renvoie une erreur. Si l'opération de reprise fait partie d'une action planifiée, modifiez ou supprimez l'action planifiée pour éviter les erreurs futures.
- Selon la taille du cluster, la reprise d'un cluster peut prendre plusieurs minutes avant que les requêtes puissent être traitées. En outre, les performances de la requête peuvent être affectées pendant un certain temps pendant que le cluster est réhydraté une fois la reprise terminée.

Redémarrage d'un cluster

Le redémarrage d'un cluster est une opération de cluster qui redémarre le cluster avec la même configuration qu'avant le redémarrage. Vous pouvez redémarrer un cluster pour appliquer les mises à jour de maintenance en attente, réinitialiser les modifications de configuration, résoudre certains problèmes ou résoudre les problèmes du cluster. Le redémarrage d'un cluster peut contribuer à garantir des performances, une sécurité et une stabilité optimales de l'environnement Amazon Redshift. La procédure suivante fournit des étapes détaillées pour redémarrer un cluster Amazon Redshift.

Lorsque vous redémarrez un cluster, l'état du cluster est défini sur `rebooting` et un événement de cluster est créé lorsque le redémarrage est terminé. Toute modification du cluster en attente est appliquée à ce redémarrage.

Pour redémarrer un cluster

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters.
3. Choisissez le cluster à redémarrer.
4. Pour Actions, choisissez Redémarrer le cluster. La page Redémarrer le cluster s’affiche.
5. Choisissez Redémarrer le cluster.

Relocalisation d’un cluster

Avec l’option de relocation (relocalisation) dans Amazon Redshift vous autorisez Amazon Redshift à déplacer un cluster vers une autre zone de disponibilité (AZ) sans perdre de données ni modifier vos applications. Avec la relocalisation, vous pouvez continuer les opérations en cas d’interruption de service sur votre cluster avec un impact minimal.

Lorsque la relocalisation des clusters est activée, Amazon Redshift peut relocaliser les clusters dans certaines situations. Cela se produit notamment lorsque des problèmes dans la zone de disponibilité empêchent le fonctionnement optimal du cluster, ou pour améliorer la disponibilité du service. Vous pouvez également appeler la fonction de relocalisation lorsque les contraintes de ressources dans une zone de disponibilité donnée perturbent les opérations du cluster. Vous pouvez, par exemple, reprendre ou redimensionner un cluster. Amazon Redshift propose la fonction de relocalisation sans frais supplémentaires.

Lorsqu’un cluster Amazon Redshift est déplacé vers une nouvelle zone de disponibilité, le nouveau cluster a le même point de terminaison que le cluster d’origine. Vos applications peuvent se reconnecter au point de terminaison et poursuivre les opérations sans modifications ni perte de données. Cependant, la relocalisation n’est pas toujours possible à cause des contraintes de ressources potentielles d’une zone de disponibilité.

La relocalisation du cluster Amazon Redshift est prise en charge pour les types d'instance RG et RA3. Les types d'instance RG et RA3 utilisent le stockage géré Redshift (RMS) comme couche de stockage durable. La dernière copie des données d'un cluster est toujours disponible dans les autres zones de disponibilité d'une AWS région. En d’autres termes, vous pouvez déplacer un cluster Amazon Redshift vers une autre zone de disponibilité sans aucune perte de données.

Lorsque vous activez la relocalisation pour votre cluster, Amazon Redshift migre votre cluster derrière un proxy. Cela permet un accès indépendant de l’emplacement aux ressources de calcul d’un cluster.

Une migration provoque le redémarrage du cluster. Lorsqu'un cluster est déplacé vers une autre zone de disponibilité, le service est interrompu le temps que le nouveau cluster soit remis en ligne dans la nouvelle zone. Cependant, vous n'avez pas besoin d'apporter de modifications à vos applications car le point de terminaison du cluster reste inchangé, même après son déplacement dans la nouvelle zone de disponibilité.

La relocalisation des clusters est activée par défaut sur les clusters RG ou RA3 récemment créés ou restaurés dont le groupe de sous-réseaux comprend plusieurs zones de disponibilité. Amazon Redshift attribue le port 5439 par défaut lors de la création d'un cluster alloué. Vous pouvez passer à un autre port dans la plage de ports 5431-5455 ou 8191-8215. (Ne passez pas à un port situé en dehors des plages. Cela entraîne une erreur.) Pour modifier le port par défaut d'un cluster provisionné, utilisez la console Amazon Redshift ou l'API AWS CLI Amazon Redshift. Pour modifier le port par défaut d'un groupe de travail sans serveur, utilisez l'API Amazon Redshift Serverless AWS CLI ou l'API Amazon Redshift Serverless.

Si vous activez la relocalisation et que vous utilisez actuellement l'adresse IP du nœud leader pour accéder à votre cluster ou au routage VPC amélioré, veillez à modifier cet accès. À la place, utilisez l'adresse IP associée au point de terminaison de cloud privé virtuel (VPC) du cluster. Pour trouver l'adresse IP du cluster, recherchez et utilisez le point de terminaison du VPC dans la section Network and security (Réseau et sécurité) de la page de détails du cluster. Pour obtenir plus de détails sur le point de terminaison du VPC, connectez-vous à la console Amazon VPC.

Vous pouvez également utiliser la commande AWS Command Line Interface (AWS CLI) `describe-vpc-endpoints` pour obtenir l'interface réseau élastique associée au point de terminaison. Vous pouvez utiliser la commande `describe-network-interfaces` pour obtenir l'adresse IP associée. Pour plus d'informations sur les AWS CLI commandes Amazon Redshift, consultez la section Commandes disponibles dans la AWS CLI référence des commandes.

Limitations

Lorsque vous utilisez l'option de relocalisation d'Amazon Redshift, tenez compte des limitations suivantes :

- Il est possible que la relocalisation des clusters ne fonctionne pas dans certains cas suite aux limitations potentielles des ressources dans une zone de disponibilité donnée. Le cas échéant, Amazon Redshift ne modifie pas le cluster d'origine.
- La relocalisation n'est pas prise en charge sur les familles d'instances DC2.
- Vous ne pouvez pas effectuer de relocalisation d'une AWS région à l'autre.

- La relocalisation d'Amazon Redshift utilise par défaut le numéro de port 5439. Vous pouvez également passer à un autre port situé dans la plage 5431-5455 ou 8191-8215.

Gestion des déplacements à l'aide de la console

Vous pouvez gérer les paramètres de relocalisation des clusters à l'aide de la console Amazon Redshift.

Désactivation de la relocalisation lors de la création d'un cluster

Procédez comme suit pour désactiver la relocalisation lors de la création d'un cluster.

Pour désactiver la relocalisation d'un cluster

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters.
3. Choisissez l'option Create cluster (Créer un cluster) pour créer un cluster. Pour plus d'informations sur la création d'un cluster, consultez Commencer avec les entrepôts de données alloués Amazon Redshift dans le Guide de démarrage Amazon Redshift.
4. Sous Sauvegarde, choisissez Activer pour Relocalisation du cluster. La relocalisation est activée par défaut.
5. Choisissez Créer un cluster.

Modification du déplacement d'un cluster existant

Procédez comme suit pour modifier le paramètre de relocalisation d'un cluster existant.

Pour modifier le paramètre de relocalisation d'un cluster existant

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters. Les clusters associés à votre compte dans la AWS région actuelle sont répertoriés. Un sous-ensemble des propriétés de chaque cluster s'affiche dans les colonnes de la liste.
3. Dans la liste des clusters, choisissez le nom du cluster que vous souhaitez modifier. La page des détails du cluster s'affiche.

4. Cliquez sur l'onglet Maintenance et choisissez Edit (Modifier) dans la section Backup details (Détails de la sauvegarde).
5. Sous Sauvegarde, choisissez Activé. La relocalisation est activée par défaut.
6. Choisissez Modifier le cluster.

Relocalisation d'un cluster

Utilisez la procédure suivante pour relocaliser manuellement un cluster vers une autre zone de disponibilité. Cela est particulièrement utile lorsque vous souhaitez tester votre configuration réseau dans des zones de disponibilité secondaires ou lorsque vous rencontrez des contraintes de ressources dans la zone de disponibilité actuelle.

Pour relocaliser un cluster vers une autre zone de disponibilité

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters. Les clusters associés à votre compte dans la AWS région actuelle sont répertoriés. Un sous-ensemble des propriétés de chaque cluster s'affiche dans les colonnes de la liste.
3. Choisissez le nom du cluster que vous souhaitez relocaliser dans la liste. La page des détails du cluster s'affiche.
4. Pour Actions, choisissez Relocate (Relocaliser). La page Relocate cluster (Relocaliser le cluster) s'affiche.
5. Vous pouvez également choisir une Availability Zone (Zone de disponibilité). Si vous ne choisissez pas de zone de disponibilité, Amazon Redshift en choisit une pour vous.

Amazon Redshift démarre la relocalisation et indique le cluster comme étant relocalisé. Une fois la relocalisation terminée, le statut du cluster devient Available (Disponible).

Gestion de la réinstallation à l'aide de la CLI Amazon Redshift

Vous pouvez gérer les paramètres de relocalisation du cluster à l'aide de l'interface de ligne de commande (CLI) AWS .

À l'aide de l' AWS interface de ligne de commande, l'exemple de commande suivant crée un cluster Amazon Redshift nommé pour **`mycluster`** lequel la relocalisation est activée.

```
aws redshift create-cluster --cluster-identifier mycluster --number-of-nodes 2 --
master-username enter a username --master-user-password enter a password --node-type
 ra3.4xlarge --port 5439 --no-availability-zone-relocation
```

Si votre cluster actuel utilise un port différent, vous devez le modifier de sorte qu'il utilise un port compris dans la plage de ports 5431-5455 ou 8191-8215 avant de le modifier pour activer la relocalisation. La valeur par défaut est 5439. L'exemple de commande suivant modifie le port si celui qu'utilise votre cluster n'est pas compris dans la plage donnée.

```
aws redshift modify-cluster --cluster-identifier mycluster --port 5439
```

L'exemple de commande suivant inclut le paramètre availability-zone-relocation sur le cluster Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier mycluster --availability-zone-
relocation
```

L'exemple de commande suivant désactive le paramètre availability-zone-relocation sur le cluster Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier mycluster --no-availability-zone-
relocation
```

L'exemple de commande suivant invoque la relocalisation du cluster Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier mycluster --availability-zone us-
east-1b
```

Définition d'une limite d'utilisation sur un cluster

Vous pouvez ajouter jusqu'à quatre limites d'utilisation pour contrôler l'utilisation de chacun des éléments suivants :

- Mise à l'échelle de la simultanéité
- Optimisations automatiques exécutées à l'aide de ressources de calcul supplémentaires
- Utilisation de Redshift Spectrum
- Cross-Region partage de données

Définition d'une limite d'utilisation pour un cluster provisionné

Voici la procédure à suivre pour définir une limite d'utilisation sur un cluster provisionné :

Pour définir une limite d'utilisation pour un cluster

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Accédez au cluster provisionné pour lequel vous souhaitez définir une limite.
3. Sur la page de détails du cluster, sélectionnez Gérer la limite d'utilisation dans le menu déroulant Actions. Vous pouvez également sélectionner l'onglet Maintenance d'un cluster, puis faire défiler l'écran vers le bas et sélectionner Créer des limites d'utilisation.
4. Sélectionnez Ajouter une limite pour la limite d'utilisation que vous souhaitez définir. Vous pouvez ajouter jusqu'à 4 limites pour une fonctionnalité donnée.
5. Définissez une période pour la limite d'utilisation, qui est quotidienne, hebdomadaire ou mensuelle.
6. Définissez une limite d'utilisation.

   - Pour le dimensionnement simultané et les optimisations automatiques exécutées en utilisant des limites de ressources de calcul supplémentaires, la limite d'utilisation est le temps passé par Amazon Redshift à utiliser la fonctionnalité au cours de la période donnée. Dans ce cas, la limite d'utilisation est définie en heures et en minutes.
   - Pour Redshift Spectrum, la limite d'utilisation est la quantité de données numérisées depuis Amazon S3. Dans ce cas, la limite d'utilisation est définie en téraoctets (To).
   - Pour le partage de données entre régions, la limite d'utilisation est la quantité de données transférées de la région productrice vers les régions consommatrices que les consommateurs peuvent interroger. Dans ce cas, la limite d'utilisation est définie en téraoctets (To).
7. Définissez l'action à exécuter par Amazon Redshift lorsque votre cluster atteint la limite. Les actions sont les suivantes :

   - Connectez-vous à la table système - Ajoute un enregistrement à la vue système SYS_QUERY_HISTORY. Vous pouvez interroger la colonne usage_limit dans cette vue pour déterminer si une requête a dépassé la limite.
   - Alerte - Utilise Amazon SNS pour configurer les abonnements aux notifications et envoyer des notifications en cas de dépassement d'une limite. Vous pouvez choisir une rubrique Amazon SNS existante, créer une nouvelle rubrique ou continuer sans rubrique.

- Désactiver la fonctionnalité - Désactive la fonctionnalité. Vous pouvez également choisir d'utiliser Amazon SNS pour envoyer une notification. Les utilisateurs peuvent continuer à utiliser le cluster pour d'autres tâches.

Les deux premières actions sont informatives, mais la dernière désactive l'utilisation de la fonctionnalité.

8. En bas de la page, choisissez Enregistrer les modifications pour enregistrer cette limite. Si vous définissez plusieurs limites à la fois, l'option Enregistrer les modifications les enregistrera toutes en même temps.

Arrêt et suppression d’un cluster

Vous pouvez arrêter votre cluster si vous voulez qu’il cesse de s’exécuter et d’entraîner des frais. Lorsque vous l’arrêtez, vous pouvez, le cas échéant, créer un instantané final. Si vous créez un instantané final, Amazon Redshift crée un instantané manuel de votre cluster avant de l’arrêter. Si vous envisagez de mettre en service un nouveau cluster avec les données et la configuration de celui que vous supprimez, vous avez besoin d’un instantané manuel. En utilisant un instantané manuel, vous pouvez restaurer l’instantané ultérieurement et reprendre l’utilisation du cluster.

Si vous n’avez plus besoin du cluster et de ses données, vous pouvez l’arrêter sans créer un instantané final. Dans ce cas, le cluster et les données sont supprimés définitivement.

Que vous arrêtiez ou pas votre cluster avec un instantané manuel final, tous les instantanés automatiques associés au cluster sont supprimés une fois que le cluster est arrêté. Les instantanés manuels associés au cluster sont conservés. Les instantanés manuels qui sont conservés, y compris l’instantané final facultatif, sont facturés au prix de stockage Amazon Simple Storage Service si vous n’avez pas d’autres clusters en cours d’exécution lorsque vous arrêtez le cluster ou si vous dépasserez le stockage gratuit disponible qui est fourni à vos clusters Amazon Redshift en cours d’exécution. Pour plus d’informations sur les frais de stockage des instantanés, consultez la page de tarification Amazon Redshift.

La suppression d'un cluster entraîne également la suppression de tous les AWS Secrets Manager secrets associés.

Pour supprimer un cluster

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/

2. Dans le menu de navigation, choisissez Clusters.
3. Choisissez le cluster à supprimer.
4. Pour Actions, choisissez Supprimer. La page Supprimer un cluster s'affiche.
5. Choisissez Supprimer le cluster.

> **Note**
>
> Lorsque vous supprimez un cluster et que vous choisissez de créer un instantané final, Amazon Redshift arrête la demande de suppression si une opération de restauration est en cours sur le cluster. Dans ce cas, vous pouvez supprimer le cluster sans instantané final, ou vous pouvez le supprimer avec un instantané final une fois la restauration terminée.

Instantanés et sauvegardes Amazon Redshift

Les instantanés sont des sauvegardes du cluster à un instant donné. Il existe deux types d'instantanés : automatisé et manuel. Amazon Redshift stocke ces instantanés en interne dans Amazon S3 en utilisant une connexion SSL (Secure Sockets Layer) chiffrée.

Amazon Redshift prend automatiquement des instantanés incrémentaux qui effectuent le suivi des modifications du cluster depuis l'instantané automatique précédent. Les instantanés automatiques conservent toutes les données requises pour restaurer un cluster à partir d'un instantané. Vous pouvez créer une planification d'instantané pour contrôler le moment où les instantanés automatiques sont créés, ou vous pouvez créer un instantané manuel à tout moment.

Lorsque vous restaurez à partir d'un instantané, Amazon Redshift crée un nouveau cluster et le rend disponible avant que toutes les données ne soient chargées ; en conséquence, vous pouvez commencer à interroger le nouveau cluster immédiatement. Le cluster diffuse les données à la demande à partir de l'instantané en réponse aux requêtes actives, puis charge le reste des données à l'arrière-plan.

Lorsque vous lancez un cluster, vous pouvez définir la période de conservation des instantanés automatiques et manuels. Vous pouvez modifier la période de conservation par défaut des instantanés automatiques et manuels en modifiant le cluster. Vous pouvez modifier la période de conservation d'un instantané manuel lorsque vous créez l'instantané ou en modifiant l'instantané.

Vous pouvez suivre la progression des instantanés en consultant les détails des instantanés dans le ou en appelant describe-cluster-snapshots dans la CLI ou dans l'action API. Console de gestion

AWSDescribeClusterSnapshots Pour un instantané en cours, sont affichées les informations telles que la taille de l'instantané incrémentiel, la vitesse de transfert, le temps passé et la durée restante estimée.

Pour vous assurer que vos sauvegardes sont toujours disponibles pour votre cluster, Amazon Redshift stocke les instantanés dans un compartiment Amazon S3 géré en interne par Amazon Redshift. Pour gérer les frais de stockage, évaluez combien de jours vous devez conserver les instantanés automatisés et configurez leur période de conservation en conséquence. Supprimez tous instantanés manuels dont vous n'avez plus besoin. Pour de plus amples informations sur les coûts de stockage des sauvegardes, consultez la page Tarification Amazon Redshift.

Vous pouvez également créer et restaurer des instantanés à l'aide AWS Backup d'un service entièrement géré qui vous aide à centraliser et à automatiser la protection des données dans l'ensemble AWS des services, dans le cloud et sur site. Pour plus d'informations, consultez AWS Backup intégration avec Amazon Redshift. Pour plus d'informations AWS Backup, voir Qu'est-ce que c'est AWS Backup ? dans le Guide AWS Backup du développeur.

Utilisation des instantanés et des sauvegardes dans Amazon Redshift sans serveur

Amazon Redshift sans serveur, comme un cluster alloué, vous permet d'effectuer une sauvegarde en tant que représentation à un instant donné des objets et des données dans l'espace de noms. Il existe deux types de sauvegardes dans Amazon Redshift sans serveur : les instantanés créés manuellement et les points de récupération qu'Amazon Redshift sans serveur crée automatiquement. Vous trouverez plus d'informations sur l'utilisation des instantanés pour Amazon Redshift sans serveur sur Instantanés et points de récupération.

Vous pouvez également restaurer un instantané de cluster alloué dans un espace de noms sans serveur. Pour plus d'informations, consultez Restauration d'un espace de noms sans serveur à partir d'un instantané.

Instantanés automatiques

Lorsque les instantanés automatiques sont activés pour un cluster, Amazon Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Amazon Redshift prend un instantané environ toutes les 8 heures ou tous les 5 Go par nœud de modifications de données, selon la première de ces deux éventualités. Si vos données sont supérieures à 5 Go * le nombre de nœuds, le délai le plus court entre deux créations automatiques d'instantanés est de 15 minutes. Vous pouvez également créer une planification d'instantané pour contrôler le moment où les instantanés automatiques sont créés. Si vous utilisez des programmations personnalisées, le délai minimum

entre deux instantanés automatisés est d'une heure. Les instantanés automatiques sont activés par défaut lorsque vous créez un cluster.

> **Note**
>
> Amazon Redshift prend des instantanés automatisés d'un cluster de producteurs de partage de données suspendu. Comme les consommateurs peuvent écrire à un producteur suspendu, ces instantanés capturent ces écritures de partage de données et fournissent un point de récupération. Auparavant, Amazon Redshift ne prenait pas de snapshots automatisés de ces clusters lorsqu'ils étaient en pause. Ces instantanés suivent le calendrier et la période de conservation des instantanés automatisés existants du cluster, et aucune action n'est requise. Pour un cluster suspendu qui n'est pas un producteur de partage de données, Amazon Redshift ne prend pas de snapshots automatisés pendant que le cluster est suspendu.

Les instantanés automatiques sont supprimés après une période de conservation. La période de conservation par défaut est d'un jour, mais vous pouvez la modifier en utilisant la console Amazon Redshift ou par programmation en utilisant la CLI ou l'API Amazon Redshift.

Pour désactiver les instantanés automatiques, définissez la période de conservation sur zéro. Si vous désactivez les instantanés automatiques, Amazon Redshift cesse de prendre des instantanés et supprime les instantanés automatiques existants pour le cluster. Vous ne pouvez pas désactiver les instantanés automatiques pour les types de nœuds RG ou RA3. Vous pouvez définir une période de rétention automatique de type de nœud RG ou RA3 comprise entre 1 et 35 jours.

Seul Amazon Redshift peut supprimer un instantané automatisé ; vous ne pouvez pas les supprimer manuellement. Amazon Redshift supprime les instantanés automatisés à la fin de leur période de conservation, lorsque vous désactivez les instantanés automatisés pour le cluster ou lorsque vous supprimez le cluster. Amazon Redshift conserve le dernier instantané automatisé jusqu'à ce que vous désactiviez les instantanés automatisés ou supprimiez le cluster.

Si vous souhaitez conserver un instantané automatique pendant une période plus longue, vous pouvez en créer une copie en tant qu'instantané manuel. L'instantané automatique et conserver jusqu'à la fin de la période de conservation, mais l'instantané manuel correspondant est conservé jusqu'à ce que vous le supprimiez manuellement ou jusqu'à la fin de la période de conservation.

Planifications d’un instantané automatique

Pour contrôler précisément le moment où les instantanés sont pris, vous pouvez créer une planification d’instantané et attacher celle-ci à un ou plusieurs clusters. Lorsque vous modifiez une planification d’instantané, la planification est modifiée pour tous les clusters associés. Si aucune planification d’instantané n’est attachée à un cluster, ce dernier utilise la planification d’instantané automatisé par défaut.

Une planification d’instantané est un ensemble de règles de planification. Vous pouvez définir une règle de planification simple basée sur un intervalle spécifié, par exemple, toutes les 8 heures ou toutes les 12 heures. Vous pouvez également ajouter des règles pour prendre des instantanés certains jours de la semaine, à des heures spécifiques ou pendant des périodes spécifiques. Les règles peuvent également être définies à l'aide d'expressions Unix-like cron.

Format de la planification d’instantané

Sur la console Amazon Redshift, vous pouvez créer une planification d’instantané. Ensuite, vous pouvez attacher une planification à un cluster pour déclencher la création d’un instantané système. Une planification peut être attachée à plusieurs clusters et vous pouvez créer plusieurs définitions cron dans une planification pour déclencher un instantané.

Vous pouvez définir une planification pour vos instantanés en utilisant une syntaxe cron. La définition de ces plannings utilise une syntaxe Unix-like cron modifiée. Vous spécifiez l’heure en heure UTC (temps universel coordonné). Vous pouvez créer des planifications avec une fréquence maximum d’une heure et une précision minimum d’une minute.

Les expressions cron modifiées Amazon Redshift se composent de 3 champs obligatoires, séparés par des espaces.

Syntaxe

```
cron(Minutes Hours Day-of-month Month Day-of-week Year)
```

Champs	Valeurs	Caractères génériques
Minutes	0–59	, - * /
Heures	0 – 23	, - * /

Champs	Valeurs	Caractères génériques
Day-of-month	1–31	, - * ? / L W
Mois	1 à 12 ou JAN-DEC	, - * /
Day-of-week	1 à 7 ou SUN-SAT	, - * ? L #
Année	1970-2199	, - * /

Caractères génériques

- Le caractère générique , (virgule) inclut des valeurs supplémentaires. Dans le champ `Day-of-week`, `MON,WED,FRI` correspond à lundi, mercredi et vendredi. Le nombre total de valeurs est limité à 24 par champ.
- Le caractère générique - (tiret) spécifie des plages. Dans le champ `Hour`, 1–15 correspond aux heures 1 à 15 du jour spécifié.
- Le caractère générique * (astérisque) inclut toutes les valeurs du champ. Dans le champ `Hours`, * inclut chaque heure.
- Le caractère générique / (barre oblique) spécifie les incréments. Dans le champ `Hours`, vous pouvez saisir **`1/10`** pour spécifier toutes les 10 heures à partir de la première heure de la journée (par exemple, 01 h 00, 11 h 00 et 21 h 00).
- Le caractère générique ? (point d'interrogation) indique l'un ou l'autre. Dans le `Day-of-month` champ, tu pouvais saisir 7, et si tu ne te souciais pas du jour de la semaine le septième, tu pourrais entrer ? sur le Day-of-week terrain.
- Le caractère générique L dans les champs ou spécifie le dernier jour du mois ou de la semaine.`Day-of-monthDay-of-week`
- Le caractère générique W dans le champ spécifie un jour de la semaine. `Day-of-month` Dans le champ `Day-of-month`, `3W` spécifie le jour le plus proche du troisième jour de semaine du mois.
- Le caractère générique # dans le Day-of-week champ indique une certaine instance du jour de la semaine spécifié dans un délai d'un mois. Par exemple, 3#2 correspond au deuxième mardi du mois : le 3 fait référence à mardi, car c'est le troisième jour de chaque semaine, et le 2 fait référence à la deuxième journée de ce type dans le mois.

> **Note**
>
> Si vous utilisez un caractère « # », vous ne pouvez définir qu'une seule expression dans le champ « day-of-week » (jour de la semaine). Par exemple, « 3#1,6#3 » n'est pas valide, car il est interprété comme deux expressions.

Restrictions

- Vous ne pouvez pas spécifier les champs `Day-of-month` et `Day-of-week` de la même expression cron. Si vous spécifiez une valeur dans l'un de ces champs, vous devez utiliser un signe ? (point d'interrogation) dans l'autre.
- Les programmes d'instantanés ne prennent pas en charge les fréquences suivantes :
  - Instantanés programmés à une fréquence supérieure à 1 par heure.
  - Instantanés programmés à une fréquence inférieure à 1 par jour (24 heures).

  Si des planifications se chevauchent et entraînent la planification de plusieurs instantanés dans une fenêtre d'une heure, une erreur de validation se produit.

Lors de la création d'une planification, vous pouvez utiliser les exemples de chaînes cron suivants.

Minutes	Heures	Jour de la semaine	Signification
0	14- 20/1	TUE	Mardi, toutes les heures entre 14 h 00 et 20 h 00.
0	21	MON-FRI	Tous les soirs à 21 h 00 du lundi au vendredi.
30	0/6	SAT-SUN	Le samedi et le dimanche, toutes les 6 heures, 30 minutes

Minutes	Heures	Jour de la semaine	Signification			
			après minuit (00 h 30). Le résultat est un instantané chaque jour à 00 h 30, 06 h 30, 12 h 30 et 18 h 30.			
30	12/4	*	Tous les jours, toutes les 4 heures à partir de 12 h 30. Cela équivaut à 12 h 30, 16 h 30, 20 h 30.			

Par exemple, pour une exécution quotidienne toutes les 2 heures à partir de 15 h 15. Cela équivaut à 15 h 15, 17 h 15, 19 h 15, 21 h 15, 23 h 15, spécifiez :

```
cron(15 15/2 *)
```

Vous pourrez créer plusieurs définitions de planification cron dans une planification. Par exemple, la AWS CLI commande suivante contient deux programmes cron dans un seul programme.

```
create-snapshot-schedule --schedule-identifier "my-test" --schedule-definition "cron(0
 17 SAT,SUN)" "cron(0 9,17 MON-FRI)"
```

Instantanés manuels

Vous pouvez prendre un instantané manuel à tout moment. Par défaut, les instantanés manuels sont conservés indéfiniment, même après la suppression de votre cluster. Vous pouvez spécifier la période de conservation lorsque vous créez un instantané manuel ou vous pouvez changer la période de conservation en modifiant l'instantané. Pour plus d'informations sur la modification de la durée de conservation, consultez Modification de la période de conservation d'un instantané manuel.

Si un instantané est supprimé, vous ne pouvez pas démarrer de nouvelles opérations qui référencent cet instantané. Cependant, si une opération de restauration est en cours, elle s'exécute intégralement.

Amazon Redshift dispose d'un quota qui limite le nombre total de clichés manuels que vous pouvez créer ; ce quota est fixé par AWS compte et par région. AWS Le quota par défaut est répertorié dans Quotas et limites d'Amazon Redshift.

Stockage d'instantanés

Comme les instantanés entraînent des frais de stockage, il est important que vous les supprimiez lorsque vous n'en avez plus besoin. Amazon Redshift supprime les instantanés automatisés et manuels à la fin de leurs périodes de conservation respectives. Vous pouvez également supprimer les instantanés manuels à l'aide de la Console de gestion AWS ou de la commande CLI batch-delete-cluster-snapshots.

Vous pouvez modifier la période de conservation d'un instantané manuel en modifiant ses paramètres.

Vous pouvez obtenir des informations sur la quantité de stockage consommée par vos instantanés à l'aide de la console Amazon Redshift ou de la commande describe-storage de la CLI.

Exclusion des tables des instantanés

Par défaut, toutes les tables permanentes définies par l'utilisateur sont incluses dans les instantanés. Si une table, par exemple une table intermédiaire, n'a pas besoin d'être sauvegardée, vous pouvez réduire considérablement le temps nécessaire à la création d'instantanés et à la restauration à partir d'instantanés. Vous réduisez également l'espace de stockage sur Amazon S3 à l'aide d'une table sans sauvegarde. Pour créer une table sans sauvegarde, incluez le paramètre BACKUP NO lorsque vous créez la table. Pour plus d'informations, consultez CREATE TABLE et CREATE TABLE AS dans le Manuel du développeur de base de données Amazon Redshift.

> **Note**
>
> No-backup les tables ne sont pas prises en charge pour les clusters provisionnés RG ou RA3 et les groupes de travail Amazon Redshift Serverless. Une table marquée comme non sauvegardée dans un cluster RG ou RA3 ou un groupe de travail sans serveur est traitée comme une table permanente qui sera toujours sauvegardée lors de la prise d'un instantané, et toujours restaurée lors de la restauration à partir d'un instantané. Pour éviter les coûts

liés aux instantanés pour les tables sans sauvegarde, tronquez-les avant de prendre un instantané.

Création d'un instantané manuel

Vous pouvez créer un instantané manuel d'un cluster dans la liste des instantanés comme suit. Sinon, vous pouvez effectuer un instantané d'un cluster dans le volet de configuration du cluster. Pour plus d'informations, consultez Instantanés et sauvegardes Amazon Redshift.

> **Note**
>
> No-backup les tables ne sont pas prises en charge pour les clusters provisionnés RG ou RA3 et les groupes de travail Amazon Redshift Serverless. Une table marquée comme non sauvegardée dans un cluster RG ou RA3 ou un groupe de travail sans serveur est traitée comme une table permanente qui sera toujours sauvegardée lors de la prise d'un instantané, et toujours restaurée lors de la restauration à partir d'un instantané. Pour éviter les coûts liés aux instantanés pour les tables sans sauvegarde, tronquez-les avant de prendre un instantané.

Pour créer un snapshot manuel

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters, Snapshots (Instantanés), puis choisissez l'onglet Create snapshot (Créer un instantané). La page d'instantané permettant de créer un instantané manuel s'affiche.
3. Entrez les propriétés de la définition de l'instantané, puis choisissez Create snapshot (Créer un instantané). L'instantané n'est pas toujours disponible immédiatement.

Création d'une planification d'instantané

Amazon Redshift effectue régulièrement des instantanés incrémentiels automatiques de vos données et les enregistre dans Amazon S3. De plus, vous pouvez effectuer des instantanés manuels de vos données quand vous le souhaitez.

Toutes les tâches d'instantanés dans la console Amazon Redshift démarrent à partir de la liste des instantanés. Vous pouvez filtrer la liste en fonction d'une plage de temps, du type d'instantané et du cluster associé à l'instantané. De plus, vous pouvez trier la liste par date, taille et type d'instantané. Selon le type d'instantané que vous sélectionnez, il est possible que vous puissiez choisir parmi différentes options pour utiliser l'instantané.

Pour contrôler précisément le moment où les instantanés sont pris, vous pouvez créer une planification d'instantané et attacher celle-ci à un ou plusieurs clusters. Vous pouvez attacher une planification lorsque vous créez un cluster ou en modifiant le cluster existant. Pour plus d'informations, consultez Planifications d'un instantané automatique.

Pour créer une planification d'instantané

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters, Snapshots (Instantanés), puis choisissez l'onglet Snapshot schedules (Planifications d'instantanés). Les planifications d'instantanés sont affichées.
3. Choisissez Add schedule (Ajouter une planification) pour afficher la page permettant d'ajouter une planification.
4. Entrez les propriétés de la définition de la planification, puis choisissez Add schedule (Ajouter une planification).
5. Sur la page qui apparaît, vous pouvez attacher des clusters à votre nouvelle planification d'instantané, puis choisir OK.

Partage d'un instantané

Vous pouvez partager un instantané manuel existant avec d'autres comptes AWS clients en autorisant l'accès à l'instantané. Vous pouvez en autoriser jusqu'à 20 pour chaque instantané et 100 pour chaque clé AWS Key Management Service (AWS KMS). En d'autres termes, si vous avez 10 instantanés chiffrés à l'aide d'une seule clé KMS, vous pouvez autoriser 10 AWS comptes à restaurer chaque instantané, ou d'autres combinaisons qui ajoutent jusqu'à 100 comptes et ne dépassent pas 20 comptes pour chaque instantané. Une personne connectée comme utilisateur dans l'un des comptes autorisés peut alors décrire l'instantané ou le restaurer pour créer un nouveau cluster Amazon Redshift sous son compte. Par exemple, si vous utilisez des comptes AWS clients distincts pour la production et les tests, un utilisateur peut se connecter à l'aide du compte de production et partager un instantané avec les utilisateurs du compte de test. Une personne connectée comme

utilisateur d’un compte tests peut alors restaurer l’instantané pour créer un nouveau cluster, détenu par le compte tests, à des fins de tests ou de diagnostic.

Un instantané manuel appartient en permanence au compte AWS client sous lequel il a été créé. Seuls les utilisateurs du compte détenteurs de l’instantané peuvent autoriser d’autres comptes à accéder à l’instantané ou à révoquer les autorisations. Les utilisateurs des comptes autorisés peuvent uniquement décrire ou restaurer un instantané qu’ils ont partagé ; ils ne peuvent pas copier ou supprimer des instantanés qu’ils ont partagés. Une autorisation reste en vigueur jusqu’à ce que le propriétaire de l’instantané la révoque. Si une autorisation est révoquée, l’utilisateur précédemment autorisé perd la visibilité de l’instantané et ne peut pas lancer de nouvelles actions faisant référence à l’instantané. Si le compte est en train de restaurer l’instantané lorsque l’accès est révoqué, la restauration s’exécute jusqu’à la fin. Vous ne pouvez pas supprimer un instantané pendant qu’il a des autorisations actives ; vous devez d’abord révoquer toutes les autorisations.

AWS les comptes clients sont toujours autorisés à accéder aux instantanés détenus par le compte. Les tentatives d’autorisation ou de révocation de l’accès au compte propriétaire entraînent une erreur. Vous ne pouvez pas restaurer ou décrire un instantané appartenant à un compte AWS client inactif.

Une fois que vous avez autorisé l'accès à un compte AWS client, aucun utilisateur de ce compte ne peut effectuer d'action sur l'instantané, sauf s'il assume un rôle dans le cadre de politiques le permettant.

- Les utilisateurs du compte propriétaire de l’instantané ne peuvent autoriser et révoquer l’accès à un instantané que s’ils assument un rôle avec une politique IAM qui leur permet d’exécuter ces actions avec une spécification de ressource incluant l’instantané. Par exemple, la politique suivante permet à un utilisateur ou à un rôle dans le AWS compte `012345678912` d'autoriser d'autres comptes à accéder à un instantané nommé `my-snapshot20130829` :

  JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
          "redshift:AuthorizeSnapshotAccess",
          "redshift:RevokeSnapshotAccess"
          ],
      "Resource":[
```

```
          "arn:aws:redshift:us-east-1:012345678912:snapshot:*/my-
snapshot20130829"
         ]
    }
  ]
}
```

- Les utilisateurs d'un AWS compte avec lequel un instantané a été partagé ne peuvent pas effectuer d'actions sur cet instantané s'ils ne disposent pas des autorisations les autorisant. Vous pouvez le faire en attribuant la politique à un rôle et en assumant ce rôle.
  - Pour afficher ou décrire un instantané, ils doivent avoir une politique IAM autorisant l'action `DescribeClusterSnapshots`. Le code suivant en présente un exemple :

    JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
          "redshift:DescribeClusterSnapshots"
          ],
      "Resource":[
           "*"
          ]
    }
  ]
}
```

  - Pour restaurer un instantané, un utilisateur doit assumer un rôle avec une politique IAM permettant l'action `RestoreFromClusterSnapshot` et ayant un élément de ressource qui couvre à la fois le cluster qu'il crée et l'instantané. Par exemple, si un utilisateur du compte `012345678912` a partagé l'instantané `my-snapshot20130829` avec le compte `219876543210`, pour pouvoir créer un cluster en restaurant l'instantané, un utilisateur du compte `219876543210` doit assumer un rôle avec un politique telle que la suivante :

    JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
```

```
    {
      "Effect":"Allow",
      "Action":[
          "redshift:RestoreFromClusterSnapshot"
          ],
      "Resource":[
           "arn:aws:redshift:us-east-1:012345678912:snapshot:*/my-
snapshot20130829",
           "arn:aws:redshift:us-east-1:219876543210:cluster:from-another-
account"
          ]
    }
  ]
}
```

- Une fois que l'accès à un instantané a été révoqué depuis un AWS compte, aucun utilisateur de ce compte ne peut accéder à l'instantané. Cela s’applique même si ces comptes ont des politiques IAM qui autorisent des actions sur la ressource d’instantané précédemment partagée.

Partage d’un instantané de cluster à l’aide de la console

Sur la console, vous pouvez autoriser d’autres utilisateurs à accéder à un instantané manuel que vous possédez et vous pouvez révoquer ultérieurement cet accès, lorsqu’il n’est plus nécessaire.

Pour partager un instantané avec un autre compte

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters, Instantanés, puis choisissez l’instantané manuel à partager.
3. Pour Actions, choisissez Manual snapshot settings (Paramètres d’instantané manuel) pour afficher les propriétés de l’instantané manuel.
4. Entrez le ou les comptes à partager dans la section Gérer l’accès, puis choisissez Enregistrer.

Considérations en matière de sécurité pour le partage d’instantanés chiffrés

Lorsque vous donnez accès à un instantané chiffré, Redshift exige que la clé gérée par le client KMS d’ AWS utilisée pour créer l’instantané soit partagée avec le ou les comptes qui effectuent la restauration. Si la clé n’est pas partagée, la tentative de restauration de l’instantané entraîne

une erreur d'accès refusé. Le compte récepteur n'a pas besoin d'autorisations supplémentaires pour restaurer un instantané partagé. Lorsque vous autorisez l'accès aux instantanés et que vous partagez la clé, l'identité autorisant l'accès doit avoir les autorisations `kms:DescribeKey` sur la clé qui a été utilisée pour chiffrer l'instantané. Cette autorisation est décrite plus en détail dans Autorisations AWS KMS. Pour plus d'informations, consultez DescribeKeyla documentation de référence de l'API Amazon Redshift.

La stratégie de clé gérée par le client peut être mise à jour par programme ou dans la console AWS Key Management Service .

> **Note**
>
> Si vous utilisez une clé KMS par défaut, vous n'avez pas besoin d'effectuer des actions ou de modifier quoi que ce soit dans AWS KMS pour partager un instantané.

Autoriser l'accès au AWS Clé KMS pour un instantané chiffré

Pour partager la clé gérée par le client AWS KMS pour un instantané chiffré, mettez à jour la politique en matière de clés en effectuant les étapes suivantes :

1. Mettez à jour la stratégie de clé KMS avec l'Amazon Resource Name (ARN) du compte AWS que vous partagez en tant que `Principal` dans la stratégie de clé KMS.
2. Autoriser l'action `kms:Decrypt`.

Dans l'exemple de stratégie de clé suivant, l'utilisateur `111122223333` est le propriétaire de la clé KMS et l'utilisateur `444455556666` est le compte avec lequel la clé est partagée. Cette politique clé permet au AWS compte d'accéder à l'exemple de clé KMS en incluant l'ARN pour l'identité du AWS compte racine de l'utilisateur en `444455556666` tant `Principal` que politique, et en autorisant l'`kms:Decrypt`action.

JSON

```
{
    "Id": "key-policy-1",
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/KeyUser",
                    "arn:aws:iam::444455556666:root"
                ]
            },
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Une fois l'accès accordé à la clé KMS gérée par le client, le compte qui restaure le snapshot chiffré doit créer un rôle Gestion des identités et des accès AWS (IAM), ou un utilisateur, s'il n'en possède pas déjà un. En outre, ce AWS compte doit également associer une politique IAM à ce rôle ou à cet utilisateur IAM qui lui permet de restaurer un instantané de base de données chiffré à l'aide de votre clé KMS.

Pour plus d'informations sur l'octroi d'accès à une AWS KMS clé, voir Autoriser les utilisateurs d'autres comptes à utiliser une clé KMS dans le guide du AWS Key Management Service développeur.

Pour un aperçu des principales politiques, consultez Comment Amazon Redshift les utilise. AWS KMS

Copie d’un instantané automatique

Les instantanés automatiques sont supprimés automatiquement à l’expiration de leur période de conservation, lorsque vous désactivez les instantanés automatiques ou lorsque vous supprimez un cluster. Si vous souhaitez conserver un instantané automatique, vous pouvez le copier dans un instantané manuel.

Pour copier un instantané automatique

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/

2. Dans le menu de navigation, choisissez Clusters, Instantanés, puis choisissez l’instantané à copier.
3. Pour Actions, choisissez Copier un instantané automatisé pour copier l’instantané.
4. Mettez à jour les propriétés du nouvel instantané, puis choisissez Copier.

Copier un instantané vers un autre AWS Région

Vous pouvez configurer Amazon Redshift pour copier automatiquement les instantanés (automatisés ou manuels) d'un cluster vers une autre région. AWS Lorsqu'un instantané est créé dans la AWS région principale du cluster, il est copié dans une AWS région secondaire. Les deux AWS régions sont connues respectivement sous le nom de AWS région source et AWS région de destination. Si vous stockez une copie de vos instantanés dans une autre AWS région, vous pouvez restaurer votre cluster à partir de données récentes si quelque chose affecte la AWS région principale. Vous pouvez configurer votre cluster pour copier des instantanés dans une seule AWS région de destination à la fois. Pour obtenir une liste des régions Amazon Redshift, reportez-vous à Régions et points de terminaison dans Référence générale d'Amazon Web Services.

Lorsque vous autorisez Amazon Redshift à copier automatiquement des instantanés vers une autre AWS région, vous spécifiez la région de destination AWS dans laquelle les instantanés seront copiés. Pour les instantanés automatisés, vous pouvez également spécifier la période de conservation pour les conserver dans la AWS région de destination. Une fois qu'un instantané automatique est copié dans la AWS région de destination et qu'il atteint la période de conservation de cette région, il est supprimé de la AWS région de destination. Cela permet de limiter l’utilisation des instantanés. Pour conserver les instantanés automatisés plus ou moins longtemps dans la AWS région de destination, modifiez cette période de conservation.

La période de conservation que vous définissez pour les instantanés automatisés copiés dans la AWS région de destination est distincte de la période de conservation des instantanés automatiques dans la région source AWS . La période de conservation par défaut pour les instantanés copiés est de 7 jours. Cette période de sept jours s’applique uniquement aux instantanés automatiques. Dans les AWS régions source et de destination, les instantanés manuels sont supprimés à la fin de la période de conservation des instantanés ou lorsque vous les supprimez manuellement.

Vous pouvez désactiver la copie d’instantané automatique d’un cluster à tout moment. Lorsque vous désactivez cette fonctionnalité, les instantanés ne sont plus copiés de la AWS région source vers la région de destination AWS . Tous les instantanés automatisés copiés dans la AWS région de destination sont supprimés lorsqu'ils atteignent la limite de durée de conservation, sauf si vous

en créez manuellement des copies instantanées. Ces instantanés manuels, ainsi que tous les instantanés manuels copiés depuis la région de destination, sont conservés dans AWS la région de destination AWS jusqu'à ce que vous les supprimiez manuellement.

Pour modifier la AWS région de destination dans laquelle vous copiez les instantanés, désactivez d'abord la fonction de copie automatique. Réactivez-la ensuite, en spécifiant la nouvelle région AWS de destination.

Une fois qu'un instantané est copié dans la AWS région de destination, il devient actif et disponible à des fins de restauration.

Pour copier des instantanés de clusters AWS KMS chiffrés vers une autre AWS région, créez une autorisation permettant à Amazon Redshift d'utiliser une clé gérée par le client dans la région de destination. AWS Choisissez ensuite cette autorisation lorsque vous activez la copie des instantanés dans la AWS région source. Pour plus d’informations sur la configuration des autorisations de copie d’instantané, consultez Copier AWS KMS—instantanés chiffrés vers un autre Région AWS.

Restauration d’un cluster à partir d’un instantané

Un instantané contient des données issues de n’importe quelle base de données exécutée sur votre cluster. Il contient également des informations sur votre cluster, y compris le nombre de nœuds, le type de nœud et le nom de l’administrateur. Si vous restaurez votre cluster à partir d’un instantané, Amazon Redshift utilise les informations du cluster pour en créer un nouveau. Ensuite, il restaure toutes les bases de données à partir des données de l’instantané.

> **Note**
>
> No-backup les tables ne sont pas prises en charge pour les clusters provisionnés RG ou RA3 et les groupes de travail Amazon Redshift Serverless. Une table marquée comme non sauvegardée dans un cluster RG ou RA3 ou un groupe de travail sans serveur est traitée comme une table permanente qui sera toujours sauvegardée lors de la prise d'un instantané, et toujours restaurée lors de la restauration à partir d'un instantané.

Pour le nouveau cluster créé à partir de l’instantané d’origine, vous pouvez choisir la configuration, par exemple le type de nœud et le nombre de nœuds. Le cluster est restauré dans la même région AWS et la même zone de disponibilité, sauf si vous spécifiez une autre zone de disponibilité dans votre demande. Lorsque vous restaurez un cluster à partir d’un instantané, vous pouvez, si vous le souhaitez, choisir une piste de maintenance compatible pour le nouveau cluster.

> **Note**
>
> Lorsque vous restaurez un instantané dans un cluster avec une configuration différente, l'instantané doit être issu d'un cluster dont la version est 1.0.10013 ou ultérieure.

Lorsqu'une restauration est en cours, les événements sont généralement émis dans l'ordre suivant :

1. RESTORE_STARTED : REDSHIFT-EVENT-2008 envoyé lorsque le processus de restauration commence.
2. RESTORE_SUCCEDED — REDSHIFT-EVENT-3003 envoyé lorsque le nouveau cluster a été créé.

   Le cluster est disponible pour les requêtes.
3. DATA_TRANSFER_COMPLETED : REDSHIFT-EVENT-3537 envoyé lorsque le transfert de données est terminé.

> **Note**
>
> Les clusters RG et RA3 émettent uniquement des événements RESTORE_STARTED et RESTORE_SUCCEDED. Aucun transfert de données explicite ne doit être effectué après la réussite d'un RESTORE, car les types de nœuds RG et RA3 stockent les données dans le stockage géré Amazon Redshift. Avec les nœuds RG et RA3, les données sont transférées en continu entre les nœuds RG et RA3 et le stockage géré par Amazon Redshift dans le cadre du traitement normal des requêtes. Les nœuds RG et RA3 mettent en cache les données chaudes localement et conservent automatiquement les blocs les moins fréquemment demandés dans le stockage géré Amazon Redshift.

Vous pouvez suivre la progression d'une restauration en appelant l'opération DescribeClustersAPI ou en consultant les détails du cluster dans le Console de gestion AWS. Pour une restauration en cours, sont affichées les informations telles que la taille des données de l'instantané, la vitesse de transfert, le temps passé et la durée restante estimée. Pour une description de ces mesures, voir RestoreStatus.

Vous ne pouvez pas utiliser un instantané pour restaurer l'état antérieur d'un cluster actif.

> **Note**
>
> Lorsque vous restaurez un instantané sur un nouveau cluster, les groupe de sécurité et groupe de paramètres par défaut sont utilisés, sauf si vous spécifiez des valeurs différentes.

Vous pouvez choisir de restaurer un instantané dans un cluster avec une autre configuration pour les raisons suivantes :

- Lorsqu'un cluster est composé de types de nœud plus petits et que vous souhaitez les regrouper dans un type de nœud plus important avec moins de nœuds.
- Lorsque vous avez surveillé votre charge de travail et déterminé la nécessité de passer à un type de nœud avec davantage d'UC et de stockage.
- Lorsque vous souhaitez mesurer les performances des charges de travail de test avec différents types de nœud.

La restauration comporte les contraintes suivantes :

- La nouvelle configuration de nœud doit inclure suffisamment de stockage pour les données existantes. Même lorsque vous ajoutez des nœuds, votre nouvelle configuration peut manquer de stockage en raison de la manière dont les données sont redistribuées.
- L'opération de restauration vérifie si l'instantané a été créé sur une version de cluster compatible avec la version du nouveau cluster. Si le nouveau cluster a un niveau de version trop précoce, alors l'opération de restauration échoue et renvoie d'autres informations dans un message d'erreur.
- Les configurations possibles (nombre de nœuds et type de nœud) par rapport auxquelles vous pouvez effectuer la restauration sont déterminées par le nombre de nœuds dans le cluster d'origine et le type de nœud cible du nouveau cluster. Pour déterminer les configurations possibles disponibles, vous pouvez utiliser la console Amazon Redshift ou la `describe-node-configuration-options` AWS CLI commande avec. `action-type restore-cluster` Pour plus d'informations sur la restauration avec la console Amazon Redshift, consultez Restauration d'un cluster à partir d'un instantané.

Les étapes suivantes prennent un cluster avec plusieurs nœuds et l'intègre à un type de nœud plus important avec un nombre de nœuds plus petit à l'aide de l' AWS CLI. Pour cet exemple, nous allons commencer par un cluster source composé de 24 nœuds . Dans le cas présent, supposons que nous

ayons créé un instantané de ce cluster et que nous souhaitions le restaurer dans un type de nœud plus important.

1. Exécutez la commande suivante pour obtenir les détails de notre cluster composé de 24 nœuds.

```
aws redshift describe-clusters --region eu-west-1 --cluster-identifier
 mycluster-123456789012
```

2. Exécutez la commande suivante pour obtenir les détails de l'instantané.

```
aws redshift describe-cluster-snapshots --region eu-west-1 --snapshot-identifier
 mycluster-snapshot
```

3. Exécutez la commande suivante afin de décrire les options disponibles pour cet instantané.

```
aws redshift describe-node-configuration-options --snapshot-identifier mycluster-
snapshot --region eu-west-1 --action-type restore-cluster
```

   Cette commande renvoie une liste d'options avec les types de nœud recommandés, le nombre de nœuds et l'utilisation du disque pour chaque option. Dans le cadre de cet exemple, la commande précédente répertorie les configurations de nœud possibles suivantes. Nous avons choisi de restaurer dans un cluster à quatre nœuds.

```
{
    "NodeConfigurationOptionList": [
        {
            "NodeType": "ra3.16xlarge",
            "NumberOfNodes": 2,
            "EstimatedDiskUtilizationPercent": 0.1
        },
        {
            "NodeType": "ra3.16xlarge",
            "NumberOfNodes": 4,
            "EstimatedDiskUtilizationPercent": 0.05
        },
        {
            "NodeType": "ra3.4xlarge",
            "NumberOfNodes": 8,
            "EstimatedDiskUtilizationPercent": 0.03
        },
        {
```

```
            "NodeType": "ra3.4xlarge",
            "NumberOfNodes": 10,
            "EstimatedDiskUtilizationPercent": 0.02
        },
        {
            "NodeType": "ra3.4xlarge",
            "NumberOfNodes": 12,
            "EstimatedDiskUtilizationPercent": 0.02
        },
        {
            "NodeType": "ra3.xlplus",
            "NumberOfNodes": 8,
            "EstimatedDiskUtilizationPercent": 0.11
        },
        {
            "NodeType": "ra3.xlplus",
            "NumberOfNodes": 16,
            "EstimatedDiskUtilizationPercent": 0.06
        }
    ]
}
```

4. Exécutez la commande suivante pour restaurer l'instantané dans la configuration de cluster que nous avons choisie. Une fois ce cluster restauré, nous avons le même contenu que le cluster source, mais les données ont été consolidées dans quatre `ra3.16xlarge` nœuds.

```
aws redshift restore-from-cluster-snapshot --region eu-west-1 --snapshot-identifier
 mycluster-snapshot --cluster-identifier mycluster-123456789012-x --node-type
 ra3.16xlarge --number-of-nodes 4
```

Si vous avez des nœuds réservés, par exemple des nœuds réservés RA3, vous pouvez passer à des nœuds réservés RG. Vous pouvez le faire lorsque vous effectuez une restauration à partir d'un instantané ou lorsque vous effectuez un redimensionnement élastique. Vous pouvez utiliser la console pour vous guider dans ce processus. Pour plus d'informations sur la mise à niveau vers les nœuds RG, consultez la section Mise à niveau vers les types de nœuds RG ou RA3.

Pour restaurer le cluster à partir d'un instantané sur la console

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/

2. Dans le menu de navigation, choisissez Clusters, Instantanés, puis choisissez l'instantané à restaurer.
3. Choisissez Restaurer à partir d'un instantané pour afficher la Configuration du cluster et les Détails du cluster pour le nouveau cluster à créer à l'aide des informations de l'instantané.
4. Mettez à niveau les propriétés du nouveau cluster, puis choisissez Restaurer un cluster à partir d'un instantané.

Après avoir restauré l'instantané de votre cluster, l'entrepôt de données restauré est chiffré avec la même clé AWS KMS personnalisée qu'il utilisait au moment de la prise de l'instantané. Si l'instantané ne possédait pas de clé KMS personnalisée, la logique de chiffrement des sauvegardes d'Amazon Redshift dépend des facteurs suivants :

- Type d'entrepôt des données Amazon Redshift dans lequel vous restaurez l'instantané.
- Type de chiffrement du cluster au moment de la prise de l'instantané.

Pour savoir comment votre entrepôt de données est chiffré une fois que vous l'avez restauré à partir de votre instantané de cluster, consultez la table suivante :

Type de destination	Type de chiffrement de l'instantané	Type de chiffrement de destination
Cluster alloué	Chiffré avec un Clé gérée par AWS	Chiffré avec un Clé gérée par AWS
Cluster alloué	Chiffré avec un Clé détenue par AWS	Chiffré avec un Clé détenue par AWS
Espace de noms sans serveur	Chiffré avec un Clé gérée par AWS	Chiffré avec un Clé détenue par AWS
Espace de noms sans serveur	Chiffré avec un Clé détenue par AWS	Chiffré avec un Clé détenue par AWS

Si vous avez AWS Secrets Manager géré le mot de passe administrateur de votre cluster au moment où l'instantané a été pris, vous devez continuer AWS Secrets Manager à l'utiliser pour gérer le mot de passe administrateur. Vous pouvez désactiver l'utilisation d'un secret après avoir restauré le cluster

en mettant à jour les informations d'identification d'administrateur du cluster sur la page de détails du cluster.

Si vous avez des nœuds réservés, vous pouvez passer à des nœuds réservés RG. Vous pouvez le faire lorsque vous effectuez une restauration à partir d'un instantané ou lorsque vous effectuez un redimensionnement élastique. Vous pouvez utiliser la console pour vous guider dans ce processus. Pour plus d'informations sur la mise à niveau vers les nœuds RG, consultez la section Mise à niveau vers les types de nœuds RG ou RA3.

Restauration d'une table à partir d'un instantané

Vous pouvez restaurer une table à partir d'un instantané au lieu de restaurer l'intégralité du cluster. Lorsque vous restaurez une table unique à partir d'un instantané, vous indiquez l'instantané source, la base de données, le schéma et le nom de la table, ainsi que la base de données cible, le schéma et un nouveau nom de table pour la table restaurée.

> **Note**
>
> No-backup les tables ne sont pas prises en charge pour les clusters provisionnés RG ou RA3 et les groupes de travail Amazon Redshift Serverless. Une table marquée comme non sauvegardée dans un cluster RG ou RA3 ou un groupe de travail sans serveur est traitée comme une table permanente qui sera toujours sauvegardée lors de la prise d'un instantané, et toujours restaurée lors de la restauration à partir d'un instantané. Cependant, la restauration sélective de tables sans sauvegarde n'est pas prise en charge.

Le nouveau nom de table ne peut pas être le nom d'une table existante. Pour remplacer une table existante par une table restaurée à partir d'un instantané, renommez ou supprimez la table existante avant de restaurer la table à partir de l'instantané.

La table cible est créée à l'aide des définitions de colonne de la table source, des attributs de table et des attributs de colonne à l'exception des clés étrangères. Pour éviter les conflits liés aux dépendances, la table cible n'hérite pas les clés étrangères de la table source. Toutes les dépendances, telles que les vues ou les autorisations accordées sur la table source, ne sont pas appliquées à la table cible.

Si le propriétaire de la table source existe, l'utilisateur de la base de données est le propriétaire de la table restaurée, à condition que l'utilisateur dispose des autorisations suffisantes pour devenir le

propriétaire d'une relation du schéma et de la base de données spécifiés. Sinon, la table restaurée appartient à l'administrateur qui a été créé lorsque le cluster a été lancé.

La table restaurée retourne à l'état où elle était au moment de la sauvegarde. Cela inclut les règles de visibilité des transactions, définies par l'adhésion d'Amazon Redshift au principe d'isolement sérialisable, qui signifie que les données sont immédiatement visibles des transactions en cours démarrées après la sauvegarde.

La restauration d'une table à partir d'un instantané présente les limitations suivantes :

- Vous ne pouvez restaurer une table que sur le cluster actif en cours d'exécution, et à partir d'un instantané de ce cluster.
- Vous ne pouvez restaurer qu'une seule table à la fois.
- Vous ne pouvez pas restaurer une table à partir d'un instantané de cluster pris avant un redimensionnement. Néanmoins, vous pouvez restaurer une table après un redimensionnement élastique si le type de nœud n'a pas changé.
- Toutes les dépendances, telles que les vues ou les autorisations accordées sur la table source, ne sont pas appliquées à la table cible.
- Si la sécurité au niveau des lignes est activée pour une table en cours de restauration, Amazon Redshift restaure la table dans les mêmes conditions, avec la sécurité au niveau des lignes activée.

Pour restaurer une table à partir d'un instantané

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters, puis choisissez le cluster que vous souhaitez utiliser pour restaurer une table.
3. Pour Actions, choisissez Restaurer une table pour afficher la page Restaurer une table.
4. Entrez les informations sur l'instantané, la table source et la table cible à utiliser, puis choisissez Restaurer la table.

Example Exemple : restauration d'une table à partir d'un instantané à l'aide du AWS CLI

L'exemple suivant utilise la `restore-table-from-cluster-snapshot` AWS CLI commande pour restaurer la `my-source-table` table à partir du `sample-database` schéma dumy-

`snapshot-id`. Vous pouvez utiliser cette AWS CLI commande `describe-table-restore-status` pour vérifier l'état de votre opération de restauration. L'exemple restaure l'instantané sur le cluster `mycluster-example` avec le nouveau nom de table `my-new-table`.

```
aws redshift restore-table-from-cluster-snapshot --cluster-identifier mycluster-
example
                                                 --new-table-name my-new-table
                                                 --snapshot-identifier my-snapshot-id
                                                 --source-database-name sample-
database
                                                 --source-table-name my-source-table
```

Restauration d'un espace de noms sans serveur à partir d'un instantané

La restauration d'un espace de noms sans serveur à partir d'un instantané remplace toutes les bases de données de l'espace de noms par les bases de données de l'instantané. Pour plus d'informations sur les instantanés sans serveur, consultez Instantanés et points de récupération. Amazon Redshift convertit automatiquement les tables avec des clés entrelacées en clés composées lorsque vous restaurez un instantané de cluster alloué dans un espace de noms Amazon Redshift sans serveur. Pour plus d'informations sur les clés de tri, consultez Utilisation des clés de tri.

Pour restaurer un instantané de votre cluster provisionné vers votre espace de noms sans serveur.

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters, Snapshots (Instantanés), puis choisissez l'instantané à utiliser.
3. Choisissez Restore from snapshot (Restaurer à partir d'un instantané), Restore to serverless namespace (Restaurer vers un espace de noms sans serveur).
4. Choisissez l'espace de noms vers lequel vous souhaitez restaurer.
5. Confirmez que vous souhaitez effectuer une restauration à partir de votre instantané. Choisissez restore (restaurer). Cette action remplace toutes les bases de données de l'espace noms sans serveur par les données de votre cluster provisionné.

Configuration d’une copie d’instantané entre régions pour un cluster non chiffré

Vous pouvez configurer Amazon Redshift pour copier les instantanés d'un cluster vers une autre région. AWS Pour configurer la copie d'instantanés entre régions, vous devez activer cette fonctionnalité de copie pour chaque cluster et configurer l'emplacement de copie des instantanés et la durée de conservation des instantanés automatisés ou manuels copiés dans la région de destination. AWS Lorsque la copie entre régions est activée pour un cluster, tous les nouveaux instantanés manuels et automatisés sont copiés dans la région spécifiée AWS . Les noms d’instantané copiés sont préfixés par **`copy:`**.

Pour configurer un instantané inter-région

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters, puis le cluster dont vous souhaitez déplacer les instantanés.
3. Pour Actions, choisissez Configure cross-region snapshot (Configurer un instantané entre régions).

   La boîte de dialogue Configure cross-Region (Configurer entre régions) apparaît.
4. Pour Copy snapshots (Copier les instantanés), choisissez Yes (Oui).
5. Dans AWS Région de destination, choisissez la AWS région dans laquelle vous souhaitez copier les instantanés.
6. Dans Période de conservation automatique des instantanés (jours), choisissez le nombre de jours pendant lesquels vous souhaitez que les instantanés automatisés soient conservés dans la AWS région de destination avant leur suppression.
7. Dans Période de conservation manuelle des instantanés, choisissez la valeur qui représente le nombre de jours pendant lesquels vous souhaitez que les instantanés manuels soient conservés dans la AWS région de destination avant leur suppression. Si vous choisissez Custom value (Valeur personnalisée), la période de conservation doit être comprise entre 1 et 3 653 jours.
8. Cliquez sur Enregistrer.

Configuration d'une copie instantanée entre régions pour un AWS KMS—cluster chiffré

Lorsque vous lancez un cluster Amazon Redshift, vous pouvez configurer une autorisation de copie des instantanés pour une clé racine de votre compte dans la Région AWS de destination. Si vous ne

configurez pas de subvention, les instantanés de la région de destination sont chiffrés à l'aide d'une clé AWS détenue par défaut. Vous permettez ainsi à Amazon Redshift d’effectuer des opérations de chiffrement dans la région AWS de destination.

La procédure suivante décrit le processus d'activation de la copie instantanée entre régions pour un cluster AWS KMS chiffré. Pour plus d’informations sur le chiffrement dans Amazon Redshift et les autorisations de copie d’instantanés, consultez Copier AWS KMS—instantanés chiffrés vers un autre Région AWS.

Pour configurer un instantané interrégional pour un AWS KMS—cluster chiffré

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters, puis le cluster dont vous souhaitez déplacer les instantanés.
3. Pour Actions, choisissez Configure cross-region snapshot (Configurer un instantané entre régions).

   La boîte de dialogue Configure cross-Region (Configurer entre régions) apparaît.
4. Pour Copy snapshots (Copier les instantanés), choisissez Yes (Oui).
5. Dans AWS Région de destination, choisissez la AWS région dans laquelle vous souhaitez copier les instantanés.
6. Dans Période de conservation automatique des instantanés (jours), choisissez le nombre de jours pendant lesquels vous souhaitez que les instantanés automatisés soient conservés dans la AWS région de destination avant leur suppression.
7. Dans Période de conservation manuelle des instantanés, choisissez la valeur qui représente le nombre de jours pendant lesquels vous souhaitez que les instantanés manuels soient conservés dans la AWS région de destination avant leur suppression. Si vous choisissez Custom value (Valeur personnalisée), la période de conservation doit être comprise entre 1 et 3 653 jours.
8. Cliquez sur Enregistrer.

Modification de la période de conservation d’un instantané manuel

Vous pouvez modifier la période de conservation d’un instantané manuel en modifiant ses paramètres.

Pour modifier la période de conservation d’un instantané manuel

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters, Snapshots (Instantanés), puis choisissez l’instantané manuel à modifier.
3. Pour Actions, choisissez Manual snapshot settings (Paramètres d’instantané manuel) pour afficher les propriétés de l’instantané manuel.
4. Entrez les propriétés révisées de la définition de l’instantané, puis choisissez Save (Enregistrer).

Modification de la période de conservation pour la copie d’instantanés entre régions

Après avoir configuré une copie d’instantanés entre régions, vous pouvez modifier les paramètres. Vous pouvez facilement modifier la période de conservation en sélectionnant un nouveau nombre de jours et en enregistrant les modifications.

> **Warning**
>
> Vous ne pouvez pas modifier la AWS région de destination une fois la copie instantanée entre régions configurée.
> Si vous souhaitez copier des instantanés dans une autre AWS région, désactivez d'abord la copie d'instantanés entre régions. Réactivez-le ensuite avec une nouvelle AWS région de destination et une nouvelle période de conservation. Tous les instantanés automatisés copiés sont supprimés après la désactivation de la copie des instantanés inter-région. Vous devez donc déterminer si vous souhaitez en conserver et les copier dans des instantanés manuels avant de désactiver la copie d’instantanés inter-région.

Pour modifier un instantané inter-région

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters, puis le cluster pour lequel vous souhaitez modifier des instantanés.
3. Pour Actions, choisissez Configurer un instantané inter-région pour afficher les propriétés de l’instantané.
4. Entrez les propriétés révisées de la définition de l’instantané, puis choisissez Save (Enregistrer).

Suppression d’un instantané manuel

Vous pouvez supprimer des instantanés manuels en sélectionnant un ou plusieurs instantanés dans la liste des instantanés.

Pour supprimer un instantané manuel

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters, Instantanés, puis choisissez l’instantané à supprimer.
3. Pour Actions, choisissez Delete snapshot (Supprimer un instantané) pour supprimer l’instantané.
4. Confirmez la suppression des instantanés répertoriés, puis choisissez Delete (Supprimer).

Enregistrement d'un cluster auprès du AWS Glue Data Catalog

Vous pouvez enregistrer des clusters entiers dans le AWS Glue Data Catalog et créer des catalogues gérés par AWS Glue. Vous pouvez accéder à ces catalogues avec n’importe quel moteur SQL prenant en charge l’API REST d’Apache Iceberg. Pour plus d'informations sur la création de Iceberg-compatible catalogues Apache à partir d'Amazon Redshift, consultez la section Compatibilité d'Apache Iceberg pour Amazon Redshift dans le manuel Amazon Redshift Database Developer Guide.

Pour enregistrer un cluster auprès du AWS Glue Data Catalog

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters. Les clusters associés à votre compte en cours Région AWS sont répertoriés. Un sous-ensemble des propriétés de chaque cluster s’affiche dans les colonnes de la liste. Si vous n’avez pas de clusters, choisissez Créer un cluster pour en créer un.
3. Choisissez le nom du cluster que vous voulez enregistrer.
4. Dans Actions, sélectionnez Enregistrer auprès de AWS Glue Data Catalog. La fenêtre contextuelle Enregistrer auprès du AWS Glue Data Catalog s’affiche.
5. Entrez l'ID de AWS compte sur lequel vous souhaitez enregistrer le cluster sous ID de compte de destination. Il s’agit de l’identifiant de compte qui contiendra le catalogue dans le AWS Glue Data Catalog.

6. Entrez un nom sous Enregistrer l’espace de noms en tant que. Ce sera le nom du cluster dans le catalogue de données.
7. Choisissez S’inscrire. Vous serez redirigé vers la AWS Lake Formation console.
8. Suivez le processus de création du catalogue dans AWS Lake Formation. Pour plus d’informations sur la création d’un catalogue, consultez Intégration des données Amazon Redshift dans le AWS Glue Data Catalog dans le Guide du développeur AWS Lake Formation .

Multi-AZ déploiement

Amazon Redshift prend en charge les déploiements de plusieurs zones de disponibilité (Multi-AZ) pour les clusters RG ou RA3 provisionnés. Grâce Multi-AZ aux déploiements, votre entrepôt de données Amazon Redshift peut continuer à fonctionner en cas de panne lorsqu'un événement inattendu se produit dans une zone de disponibilité. Un Multi-AZ déploiement déploie des ressources de calcul dans deux zones de disponibilité (AZ) et ces ressources de calcul sont accessibles via un seul point de terminaison. En cas de défaillance d’une zone de disponibilité tout entière, les ressources de calcul restantes dans la seconde zone de disponibilité sont disponibles pour poursuivre le traitement des charges de travail. Amazon Redshift facture les mêmes taux de calcul horaires pour RG ou RA3 lorsqu'il gère un Multi-AZ entrepôt de données. Les coûts de stockage restent les mêmes, car ils sont partagés entre toutes les zones de disponibilité d’une Région AWS.

Amazon Redshift prend actuellement en charge l’objectif de point de reprise (RPO) zéro, qui permet aux données d’être à jour en cas de panne. Grâce Multi-AZ au déploiement, Amazon Redshift améliore encore ses capacités de restauration existantes et réduit son objectif de temps de restauration (RTO). Cela est possible car un Multi-AZ déploiement peut récupérer plus rapidement après une panne ou un sinistre, élevant ainsi le contrat de niveau de service (SLA) Amazon Redshift à 99,99 % contre 99,9 % avec un entrepôt de données. Single-AZ

Configuration du Multi-AZ déploiement

Pour configurer un Multi-AZ déploiement, sélectionnez l'Multi-AZoption et spécifiez le nombre de nœuds de calcul à provisionner dans chaque zone de disponibilité. Amazon Redshift déploie automatiquement des ressources de calcul égales dans deux zones de disponibilité et toutes les ressources de calcul sont toujours disponibles pour le traitement en lecture et en écriture pendant le fonctionnement normal et peuvent contribuer de manière opportuniste à améliorer les performances en utilisant les ressources de calcul supplémentaires du cluster secondaire. Cela permet à un Multi-AZ déploiement de fonctionner comme un entrepôt de données unique avec un seul point de

terminaison, éliminant ainsi le besoin de modifier les applications en cas de sinistre. Bien qu'un Multi-AZ déploiement traite une requête individuelle en utilisant les ressources de calcul résidant dans une seule zone de disponibilité, il peut distribuer automatiquement le traitement de certaines requêtes simultanées aux deux zones de disponibilité, ce qui peut parfois, mais pas toujours, augmenter le débit global pour les charges de travail de simultanéité élevées. Il est important de garder à l'esprit la fonction principale de Multi-AZ, qui est de fournir une solution de haute disponibilité à votre cluster afin de garantir une restauration rapide après un arrêt imprévu ou une panne.

Si votre principale motivation est d'améliorer les performances de votre charge de travail analytique, nous vous recommandons d'autres solutions Multi-AZ, telles que :

- redimensionnement vers un type d'instance de nœud plus grand (redimensionnement des clusters)
- activation de la mise à l'échelle de la simultanéité sur votre cluster (mise à l'échelle de la simultanéité)
- utilisation d'une architecture de partage de données pour isoler les charges de travail (présentation du partage de données)

Vous pouvez également convertir un entrepôt de Single-AZ données existant en entrepôt de Multi-AZ données ou vice versa. Tout reste identique, si ce n’est que des ressources de calcul supplémentaires sont provisionnées dans la deuxième zone de disponibilité. Lors de la migration Multi-AZ depuis un Single-AZ cluster existant, il se peut que vous deviez doubler le nombre de nœuds de cluster nécessaires, afin de garantir le maintien des performances d'une seule requête.

En cas de panne dans une zone de disponibilité, Amazon Redshift continue de fonctionner en utilisant automatiquement les ressources de la zone de disponibilité restante. Toutefois, les connexions des utilisateurs peuvent être perdues et doivent être rétablies. En outre, les requêtes qui s’exécutaient dans la zone de disponibilité en défaillance peuvent échouer et doivent être retentées. Toutefois, vous pouvez vous reconnecter à votre cluster et replanifier les requêtes immédiatement, et Amazon Redshift traitera les requêtes dans la zone de disponibilité restante. Les requêtes émises au moment d'une panne ou après celle-ci peuvent subir des retards d'exécution lors de la restauration de l'entrepôt de Multi-AZ données.

> **Note**
>
> Pour obtenir de meilleures performances et une plus grande disponibilité, nous vous recommandons d'utiliser SNAPSHOT ISOLATION avec vos Multi-AZ clusters. Pour plus d’informations, consultez CREATE DATABASE.

Limitations

Un entrepôt de Multi-AZ données possède les mêmes fonctionnalités qu'un entrepôt de Single-AZ données, à l'exception des limitations suivantes qui s'appliquent à un entrepôt de Multi-AZ données :

- Vous ne pouvez pas créer d'entrepôt de Multi-AZ données non chiffré. Assurez-vous d'ajouter un chiffrement lors de la création d'un nouvel entrepôt de Multi-AZ données, de la conversion d'un entrepôt de Single-AZ données en entrepôt de Multi-AZ données ou de la conversion d'un entrepôt de Single-AZ données en entrepôt de Multi-AZ données.
- Vous ne pouvez créer un Multi-AZ déploiement à nœud unique pour aucun des types d'instances RG ou RA3. Choisissez 2 nœuds ou plus par zone de disponibilité lors de la création d'un Multi-AZ déploiement.
- Amazon Redshift ne prend pas en charge une configuration de sous-réseau capable de prendre en charge moins de trois zones de disponibilité. En d’autres termes, le groupe de sous-réseaux configuré nécessite trois sous-réseaux supplémentaires ou plus.
- Vous ne pouvez pas déplacer un Multi-AZ déploiement vers une autre zone de disponibilité. La relocalisation sera automatiquement déterminée et effectuée par Amazon Redshift lors de l'utilisation du Multi-AZ déploiement.
- Vous ne pouvez pas suspendre ou reprendre un Multi-AZ déploiement.
- Vous ne pouvez pas exécuter votre Multi-AZ déploiement en dehors des plages de ports prises en charge 5431 à 5455 et 8191 à 8215.
- Vous ne pouvez pas utiliser les vues STL, SVCS, SVL, SVV, STV avec les Multi-AZ déploiements car elles ne prennent en charge que les vues de surveillance du système (vues SYS_*). Modifiez vos requêtes de surveillance pour utiliser les vues de surveillance du système (vues SYS_*).
- Vous ne pouvez pas associer une adresse IP Elastic à un cluster existant lorsque Multi-AZ cette option est activée.
- Vous ne pouvez pas convertir un cluster auquel est attachée une adresse IP Elastic de Single-AZ à Multi-AZ.
- Le Multi-AZ déploiement d'Amazon Redshift est disponible dans les versions suivantes : Régions AWS

> **Note**
>
> Les instances RG sont disponibles dans certaines régions. Reportez-vous à la section Disponibilité du type de nœud RG dans AWS les régions.

- USA Est (Ohio) (us-east-2)
- USA Est (Virginie du Nord) (us-east-1)
- USA Ouest (Oregon) (us-west-2)
- Afrique (Le Cap) (af-south-1)
- Asie-Pacifique (Hong Kong) (ap-east-1)
- Asie-Pacifique (Taipei) (ap-east-2)
- Asie-Pacifique (Hyderabad) (ap-south-2)
- Asie-Pacifique (Jakarta) (ap-southeast-3)
- Asie-Pacifique (Malaisie) (ap-southeast-5)
- Asie-Pacifique (Melbourne) (ap-southeast-4)
- Asie-Pacifique (Mumbai) (ap-south-1)
- Asie-Pacifique (Osaka) (ap-northeast-3)
- Asie-Pacifique (Séoul) (ap-northeast-2)
- Asie-Pacifique (Singapour) (ap-southeast-1)
- Asie-Pacifique (Sydney) (ap-southeast-2)
- Asie-Pacifique (Nouvelle Zélande) (ap-southeast-6)
- Asie-Pacifique (Thaïlande) (ap-southeast-7)
- Asie-Pacifique (Tokyo) (ap-northeast-1)
- Canada (Centre) (ca-central-1)
- Chine (Beijing) cn-north-1
- Chine (Ningxia) cn-northwest-1
- Europe (Francfort) (eu-central-1)
- Europe (Irlande) (eu-west-1)
- Europe (Londres) (eu-west-2)
- Europe (Milan) (eu-south-1)
- Europe (Paris) (eu-west-3)
- Europe (Espagne) (eu-south-2)
- Europe (Stockholm) (eu-north-1)
- Europe (Zurich) (eu-central-2)

- Israël (Tel Aviv) (il-central-1)
- Mexique (Centre) (mx-central-1)
- Moyen-Orient (Bahreïn) (me-south-1)
- Moyen-Orient (Émirats arabes unis) (me-central-1)
- Amérique du Sud (São Paulo) (sa-east-1)
- AWS GovCloud (US-East) (us-gov-east-1)
- AWS GovCloud (US-West) (gouvernement des États-Unis - Ouest - 1)

- Multi-AZ Les entrepôts de données accessibles au public prennent en charge un groupe de sécurité VPC de moins que Single-AZ les Multi-AZ entrepôts accessibles en privé.

Configuration Multi-AZ lors de la création d'un nouveau cluster

Amazon Redshift Multi-AZ prend en charge deux zones de disponibilité à la fois. Amazon Redshift sélectionne automatiquement les zones de disponibilité en fonction de la configuration sélectionnée du groupe de sous-réseaux. Vous pouvez convertir un entrepôt de données existant à zone de disponibilité unique en entrepôt de Multi-AZ données ou le restaurer à partir d'un instantané pour le configurer en entrepôt de Multi-AZ données.

À l'aide de la console Amazon Redshift, vous pouvez facilement créer de nouveaux Multi-AZ déploiements. Pour créer un nouveau Multi-AZ déploiement à l'aide de la console Amazon Redshift, sélectionnez l' Multi-AZ option lors de la création de l'entrepôt de données. Spécifiez le nombre de nœuds de calcul requis dans une zone de disponibilité unique et Amazon Redshift déploiera ce nombre de nœuds dans chacune des deux zones de disponibilité. Tous les nœuds seront utilisés pour effectuer le traitement de la charge de travail en lecture et en écriture pendant le fonctionnement normal. Vous pouvez également utiliser la AWS CLI `create-cluster` commande pour créer un nouvel entrepôt de Multi-AZ données à l'aide du `multi-az` paramètre.

Vous pouvez convertir un entrepôt de Single-AZ données existant en entrepôt de Multi-AZ données à l'aide de la console Amazon Redshift ou de la AWS CLI `modify-cluster` commande utilisant le `multi-az` paramètre. Vous pouvez également effectuer une restauration à partir d'un instantané pour configurer un entrepôt de Single-AZ données en entrepôt de Multi-AZ données à l'aide de la console Amazon Redshift ou de la AWS CLI `restore-from-cluster-snapshot` commande utilisant le `multi-az` paramètre.

Multi-AZ le déploiement ne prend en charge que les types de nœuds RG ou RA3 qui utilisent Amazon Redshift Managed Storage (RMS). Amazon Redshift stocke les données dans RMS, qui utilise

Amazon S3 et est accessible dans toutes les zones de disponibilité en un Région AWS, sans avoir à répliquer les données au niveau d'Amazon Redshift.

Vous pouvez configurer Multi-AZ le déploiement lors de la création d'un nouveau cluster à l'aide de la console Amazon Redshift ou du AWS Command Line Interface.

Utilisation de la console

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Provisioned clusters dashboard (Tableau de bord des clusters provisionnés), puis choisissez Clusters. Les clusters actuels de votre compte Région AWS sont répertoriés. Un sous-ensemble des propriétés de chaque cluster s'affiche dans les colonnes de la liste.
3. Choisissez le bouton Créer un cluster pour ouvrir la page de création d'un cluster.
4. Saisissez les propriétés de votre cluster. Pour obtenir des informations générales sur la création d'un cluster, consultez Création d'un cluster.
5. Choisissez l'un des types de nœuds RG ou RA3 dans la liste déroulante des types de nœuds. L'option de configuration AZ n'est disponible que lorsque vous avez choisi un type de nœud RG ou RA3.
6. Dans Configuration AZ, choisissez Multi-AZ.
7. Sous Nombre de nœuds par zone de disponibilité, entrez au moins deux nœuds pour votre cluster.
8. Vous avez la possibilité de charger des exemples de données ou d'apporter vos propres données :

   - Dans Sample data (Exemples de données), choisissez Load sample data (Charger les exemples de données) pour charger l'exemple de jeu de données dans votre cluster Amazon Redshift. Amazon Redshift charge l'exemple de jeu de données Tickit dans la base de données dev et le schéma public par défaut. Amazon Redshift charge automatiquement l'exemple de jeu de données dans votre cluster Amazon Redshift. Vous pouvez commencer à utiliser l'éditeur de requêtes v2 pour interroger des données.
   - Pour apporter vos propres données à votre cluster Amazon Redshift, suivez les étapes dans Importation de vos propres données dans Amazon Redshift.
9. Faites défiler l'écran vers Additional configurations (Configurations supplémentaires), développez Network and security (Réseau et sécurité) et assurez-vous d'accepter le Cluster subnet group

(Groupe de sous-réseaux de cluster) par défaut ou d'en choisir un autre. Si vous choisissez un autre groupe de sous-réseaux de cluster, assurez-vous que le groupe de sous-réseaux que vous avez sélectionné comporte 3 zones de disponibilité.

10. Sous Additional configurations (Configurations supplémentaires), développez Database configurations (Configurations de base de données).
11. Pour utiliser une AWS KMS clé personnalisée au lieu de la clé AWS détenue par défaut, cliquez sur Personnaliser les paramètres de chiffrement sous Chiffrement de base de données.
12. Sous Choisir une clé KMS, vous pouvez choisir une AWS Key Management Service clé ou saisir un ARN. Vous pouvez également cliquer sur Créer une AWS Key Management Service clé dans la AWS Key Management Service console. Pour plus d'informations sur la création d'une clé KMS, consultez Création de clés dans le Guide du développeur AWS Key Management Service .
13. Cliquez surCreate cluster (Créer un cluster). Lorsque la création d'un cluster est réussie, vous pouvez consulter les détails sur la page des détails du cluster. Vous pouvez utiliser votre client SQL pour charger et interroger des données.

Utilisation de AWS Command Line Interface

À configurer Multi-AZ lors de la création d'un cluster à l'aide du AWS Command Line Interface

- À partir de AWS CLI là, utilisez la `create-cluster` commande et le `multi-az` paramètre comme suit.

```
aws redshift create-cluster
    --port 5439
    --master-username master
    --master-user-password #####
    --node-type rg.4xlarge
    --number-of-nodes 2
    --profile maz-test
    --endpoint-url https://redshift.eu-west-1.amazonaws.com
    --region eu-west-1
    --cluster-identifier test-maz
    --multi-az
    --maintenance-track-name CURRENT
    --encrypted
```

Configuration Multi-AZ d'un entrepôt de données restauré à partir d'un instantané

Pour créer un nouveau Multi-AZ cluster en le restaurant à partir d'un instantané, procédez comme suit.

Utilisation de la console

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters, Snapshots (Instantanés), puis choisissez l'instantané à utiliser.
3. Choisissez Restore snapshot (Restaurer un instantané), puis Restore to a provisioned cluster (Restaurer vers un cluster provisionné).
4. Saisissez les propriétés de votre cluster. Pour obtenir des informations générales sur la création d'un cluster, consultez Création d'un cluster.
5. Choisissez l'un des types de nœuds RG ou RA3 dans la liste déroulante des types de nœuds. L'option de configuration AZ n'est disponible que lorsque vous avez choisi un type de nœud RG ou RA3.
6. Dans Configuration AZ, choisissez Multi-AZ.
7. Sous Nombre de nœuds par zone de disponibilité, entrez au moins deux nœuds pour votre cluster.
8. Vous avez la possibilité de charger des exemples de données ou d'apporter vos propres données :

   - Dans Sample data (Exemples de données), choisissez Load sample data (Charger les exemples de données) pour charger l'exemple de jeu de données dans votre cluster Amazon Redshift. Amazon Redshift charge l'exemple de jeu de données Tickit dans la base de données dev et le schéma public par défaut. Amazon Redshift charge automatiquement l'exemple de jeu de données dans votre cluster Amazon Redshift. Vous pouvez commencer à utiliser l'éditeur de requêtes v2 pour interroger des données.
   - Pour apporter vos propres données à votre cluster Amazon Redshift, suivez les étapes dans Charger les données d'Amazon S3 vers Amazon Redshift.
9. Faites défiler l'écran vers Additional configurations (Configurations supplémentaires), développez Network and security (Réseau et sécurité) et assurez-vous d'accepter le Cluster subnet group (Groupe de sous-réseaux de cluster) par défaut ou d'en choisir un autre. Si vous choisissez un

autre groupe de sous-réseaux de cluster, assurez-vous que le groupe de sous-réseaux que vous avez sélectionné comporte 3 zones de disponibilité.

10. Sous Additional configurations (Configurations supplémentaires), développez Database configurations (Configurations de base de données).
11. Sous Chiffrement de base de données, pour utiliser une clé KMS personnalisée autre que la clé AWS détenue par défaut, cliquez sur Personnaliser les paramètres de chiffrement. Cette option est désélectionnée par défaut.
12. Sous Choisir une clé KMS, vous pouvez choisir une AWS Key Management Service clé ou saisir un ARN. Vous pouvez également cliquer sur Créer une AWS Key Management Service clé dans la AWS Key Management Service console. Pour plus d'informations sur la création d'une clé KMS, consultez Création de clés dans le Guide du développeur AWS Key Management Service .
13. Cliquez sur Restore cluster from snapshot (Restaurer le cluster à partir d'un instantané). Lorsque la restauration d'un cluster est réussie, vous pouvez consulter les détails sur la page des détails du cluster.

Utilisation de AWS Command Line Interface

- À partir de AWS CLI, utilisez la `restore-from-cluster-snapshot` commande comme suit.

```
aws redshift restore-from-cluster-snapshot
--region eu-west-1
--multi-az
--snapshot-identifier test-snap1
--cluster-identifier test-saz-11
--endpoint-url https://redshift.eu-west-1.amazonaws.com/
```

Conversion d'un entrepôt de Single-AZ données en entrepôt Multi-AZ de données

En convertissant un entrepôt de Single-AZ données en entrepôt de Multi-AZ données, votre entrepôt de données sera hautement disponible avec une garantie SLA de 99,99 %. Les performances d'une requête individuelle resteront les mêmes, même avec un entrepôt de Multi-AZ données. Pour des charges de travail à plus haute simultanéité, vous constaterez une augmentation du débit global, car Amazon Redshift peut exécuter des demandes à l'aide de ressources de calcul dans deux zones de disponibilité.

> **Note**
>
> Amazon Redshift ne vous permettra pas de fractionner les ressources de calcul existantes lors de la conversion de Single-AZ vers Multi-AZ, ou vice versa. Cette opération n'est pas prise en charge pour maintenir des performances de requête individuelles cohérentes.

Utilisation de la console

Pour convertir un Single-AZ cluster en entrepôt de Multi-AZ données à l'aide de la console

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Provisioned clusters dashboard (Tableau de bord des clusters provisionnés), puis choisissez Clusters. Les clusters actuels de votre compte Région AWS sont répertoriés. Un sous-ensemble des propriétés de chaque cluster s'affiche dans les colonnes de la liste.
3. Choisissez le cluster que vous souhaitez convertir en Multi-AZ déploiement. La page des détails du cluster s'affiche.
4. Dans la zone Actions, choisissez Activer Multi-AZ. Le récapitulatif des modifications s'affiche. Cliquez sur Activate Multi-AZ.
5. En cas d'erreur, effectuez l'une des opérations suivantes, puis cliquez sur Activer Multi-AZ.
   - Chiffrement du cluster : choisissez Propriétés pour modifier les paramètres de chiffrement dans la section Configuration de la base de données sous l'onglet Propriétés de la page de détails du cluster.
   - Groupe de sous-réseaux : choisissez Groupe de sous-réseaux pour modifier les paramètres de groupe de sous-réseaux du cluster en cliquant sur le lien du groupe de sous-réseaux. Si vous choisissez un autre groupe de sous-réseaux de cluster, assurez-vous que le groupe de sous-réseaux que vous avez sélectionné comporte 3 zones de disponibilité.
   - Paramètres du port : choisissez Propriétés pour modifier le paramètre de port dans la section Configuration de la base de données sous l'onglet Propriétés de la page de détails du cluster.
6. Vous pouvez utiliser votre client SQL pour charger et interroger des données.

Utilisation de AWS Command Line Interface

- À partir de AWS CLI, utilisez la `modify-cluster` commande et le `multi-az` paramètre comme suit.

```
aws redshift modify-cluster
    --profile maz-test
    --endpoint-url https://redshift.eu-west-1.amazonaws.com
    --region eu-west-1
    --cluster-identifier test-maz-11
    --multi-az
```

Vous ne pouvez pas utiliser les vues STL, SVCS, SVL, SVV ou STV avec les Multi-AZ déploiements car elles ne prennent en charge que les vues de surveillance du système (vues SYS_*). Modifiez vos requêtes de surveillance pour utiliser les vues de surveillance du système (vues SYS_*).

Conversion d'un entrepôt de Multi-AZ données en entrepôt Single-AZ de données

En convertissant un entrepôt de Multi-AZ données en entrepôt de Single-AZ données, votre entrepôt de données ne bénéficiera pas de la garantie SLA de 99,99 % proposée. Multi-AZ Les performances d'une requête individuelle resteront les mêmes, mais le débit global sera affecté, car les ressources de calcul de la deuxième zone de disponibilité ne seront pas disponibles. Vous avez la possibilité d'activer la mise à l'échelle de la simultanéité pour adapter automatiquement le débit pour des performances constantes, même avec Single-AZ.

> **Note**
>
> Amazon Redshift ne vous permettra pas de fractionner les ressources de calcul existantes lors de la conversion de Single-AZ vers Multi-AZ, ou vice versa. Cette opération n'est pas prise en charge pour maintenir des performances de requête individuelles cohérentes.

Utilisation de la console

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.

2. Dans le menu de navigation, choisissez Provisioned clusters dashboard (Tableau de bord des clusters provisionnés), puis choisissez Clusters. Les clusters actuels de votre compte Région AWS sont répertoriés. Un sous-ensemble des propriétés de chaque cluster s'affiche dans les colonnes de la liste.
3. Choisissez le cluster que vous souhaitez convertir en Multi-AZ déploiement. La page des détails du cluster s'affiche.
4. Pour Actions, choisissez Désactiver Multi-AZ. Le récapitulatif des modifications s'affiche. Cliquez sur Désactiver Multi-AZ.

Utilisation de AWS Command Line Interface

- À partir de AWS CLI, utilisez la `modify-cluster` commande et le `no-multi-az` paramètre comme suit.

```
aws redshift modify-cluster
    --profile maz-test
    --endpoint-url  https://redshift.eu-west-1.amazonaws.com
    --region eu-west-1
    --cluster-identifier test-maz-11
    --no-multi-az
```

Une fois votre entrepôt de données converti Single-AZ, il perdra la garantie SLA de 99,99. Le débit global est également affecté. Lorsque les modifications sont enregistrées, vous pouvez visualiser les détails sur la page des détails du cluster.

Redimensionnement d'un entrepôt Multi-AZ de données

Vous pouvez redimensionner un entrepôt de Multi-AZ données et spécifier un nombre de nœuds ou un type de nœud différent de la configuration actuelle de l'entrepôt de données.

Utilisation de la console

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Provisioned clusters dashboard (Tableau de bord des clusters provisionnés), puis choisissez Clusters. Les clusters actuels de votre compte Région

AWS sont répertoriés. Un sous-ensemble des propriétés de chaque cluster s’affiche dans les colonnes de la liste.

3. Choisissez le cluster dont vous souhaitez redimensionner l'entrepôt de Multi-AZ données. La page des détails du cluster s’affiche.
4. Pour Actions, choisissez Redimensionner. La page Redimensionner le cluster s’affiche.
5. Suivez les instructions indiquées sur la page. Vous pouvez redimensionner le cluster maintenant, une fois à un moment donné, ou augmenter et diminuer sa taille selon un programme.
6. Sous Nouvelles configurations, choisissez l'un des types de nœuds RG ou RA3 dans la liste déroulante des types de nœuds.
7. Cliquez sur Redimensionner le cluster.

Utilisation de AWS Command Line Interface

Pour redimensionner un entrepôt de Multi-AZ données à l'aide du AWS Command Line Interface

- À partir de AWS CLI, utilisez la `resize-cluster` commande pour modifier le nombre de nœuds pour une seule zone de disponibilité comme suit.

```
aws redshift resize-cluster \
    --cluster-identifier test-maz-11
    --cluster-type multi-node
    --node-type rg.4xlarge
    --number-of-nodes 6
```

Échec du Multi-AZ déploiement

Votre entrepôt de Multi-AZ données est un ensemble de ressources informatiques déployées simultanément dans deux zones de disponibilité. Les ressources de calcul déployées dans la zone de disponibilité principale sont désignées sous le terme de calcul principal et celles figurant dans les zones de disponibilité secondaires sont désignées sous le terme de calcul secondaire. Un entrepôt de Multi-AZ données peut être restauré automatiquement sans aucune intervention de l'utilisateur lors d'un événement peu probable, tel qu'une zone de disponibilité ou une panne d'infrastructure. Le processus de récupération implique le basculement du calcul principal vers le calcul secondaire et la désignation des ressources de calcul secondaire comme ressources de calcul principal. De plus, les nouvelles ressources de calcul secondaire sont provisionnées dans une troisième zone de disponibilité. Le processus de récupération automatique est mesuré en termes de RTO et de RPO.

- Objectif de délai de reprise (RTO) : temps nécessaire à un système pour revenir à un état de fonctionnement normal après un sinistre. En d'autres termes, le RTO mesure les temps d'arrêt.
- Objectif de point de reprise (RPO) : quantité de données pouvant être perdues (mesurée dans le temps). Pour un entrepôt de Multi-AZ données Amazon Redshift, le RPO est généralement égal à zéro car toutes les données sont stockées dans Amazon Redshift Managed Storage (RMS), soutenu par Amazon Simple Storage Service, qui est une solution hautement durable et disponible par défaut.

> **Note**
>
> Les performances d'une requête individuelle ne changent pas après un basculement. Le débit global de votre entrepôt des données est réduit pendant une courte période en raison de l'indisponibilité des ressources de calcul dans l'une des zones de disponibilité. Toutefois, Amazon Redshift acquerra automatiquement de la capacité dans une autre zone de disponibilité afin de garantir le rétablissement de la même capacité de traitement de l'entrepôt des données.

Outre le processus de récupération automatique, vous pouvez également déclencher ce processus manuellement pour votre entrepôt des données à l'aide de l'option Basculement du calcul principal. Vous pouvez utiliser cette approche pour tester la manière dont votre application Multi-AZ pourrait améliorer la haute disponibilité et la continuité.

Utilisation de la console

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Effectuez l'une des actions suivantes :
   - Dans le menu de navigation, choisissez Clusters. Sous Clusters, choisissez un cluster. La page des détails du cluster s'affiche.
   - Dans le tableau de bord du cluster, choisissez un cluster.
3. Dans Actions, choisissez Basculement du calcul principal.
4. Lorsque vous y êtes invité, cliquez sur Confirm (Confirmer).

Utilisation de AWS Command Line Interface

- À partir de AWS CLI, utilisez la `failover-primary-compute` commande comme suit.

```
aws redshift failover-primary-compute
    --profile maz-test
    --endpoint-url  https://redshift.eu-west-1.amazonaws.com
    --region eu-west-1
    --cluster-identifier test-maz-11
```

Une fois l'opération ci-dessus confirmée, Amazon Redshift effectuera les mêmes étapes qu'une récupération automatique après une défaillance de zone de disponibilité ou d'infrastructure. Ce processus entraînera l'indisponibilité des nœuds de calcul dans la zone de disponibilité principale et la désignation des ressources de calcul dans la zone de disponibilité secondaire en tant que calcul principal. Lorsque la restauration du cluster est terminée avec succès, Multi-AZ le déploiement devient disponible. Votre entrepôt de Multi-AZ données provisionnera également automatiquement le nouveau calcul secondaire dans une autre troisième zone de disponibilité dès qu'il sera disponible.

Au cours de ce processus, l'état du cluster sur la console s'affiche comme étant en cours de modification pendant tout le temps, car le cluster se rétablit automatiquement et reconfigure la Multi-AZ configuration de déploiement. Le cluster peut accepter de nouvelles connexions immédiatement. Les connexions existantes et les requêtes en transit peuvent être supprimées. Vous pouvez les tester à nouveau immédiatement.

Affichage des requêtes et des chargements pour les entrepôts Multi-AZ de données

Vous pouvez consulter les informations relatives aux requêtes exécutées au cours des 7 derniers jours, quels que soient le type, la taille et le statut (pause ou reprise) de votre cluster.

Les informations affichées sur la page Queries and loads (Requêtes et charges) sont renseignées avec des informations provenant des tables système Amazon Redshift (vues SYS_*). Ces informations vous permettent d'afficher des informations supplémentaires sur vos requêtes et offrent une durée de conservation de 7 jours consécutifs. Les diagnostics des requêtes sont accélérés, ce qui vous permet de filtrer les données par base de données, nom d'utilisateur ou type d'instruction SQL. Pour consulter ces filtres supplémentaires et les informations relatives à toutes les requêtes exécutées, tenez compte des prérequis suivants :

- Vous devez vous connecter à une base de données en choisissant Connect to database (Se connecter à la base de données).
- L'utilisateur de votre base de données doit disposer des rôles et autorisations sys:operator ou sys:monitor pour effectuer la surveillance des requêtes. Pour plus d'informations sur les rôles dans le système, consultez Rôles définis par le système Amazon Redshift dans le Guide du développeur de base de données Amazon Redshift.

Vous verrez ces filtres et informations de requête supplémentaires une fois que vous vous connectez à une base de données.

Pour afficher les données de performance des requêtes à partir des requêtes et des charges

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Requêtes et charges pour afficher la liste des requêtes pour votre compte.
3. Vous devrez peut-être vous connecter à une base de données pour voir un filtre supplémentaire. Si nécessaire, cliquez sur Connect à la base de données (Se connecter à la base de données) et suivez les instructions pour vous connecter à une base de données.

   Par défaut, la liste affiche les requêtes de tous vos clusters au cours des dernières 24 heures. Vous pouvez modifier la portée de la date affichée dans la console.

Pour afficher les données de performance des requêtes à partir de Query monitoring (Surveillance des requêtes)

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters. Sous Clusters, sélectionnez un cluster.
3. Choisissez Query monitoring (Surveillance des requêtes).
4. Selon la configuration ou la version de votre cluster, vous devrez peut-être vous connecter à une base de données pour voir des filtres supplémentaires. Si nécessaire, cliquez sur Connect à la base de données (Se connecter à la base de données) et suivez les instructions pour vous connecter à une base de données.

Surveillance d'une requête dans un Multi-AZ déploiement

Un Multi-AZ déploiement utilise des ressources de calcul qui sont déployées dans les deux zones de disponibilité et peuvent continuer à fonctionner si les ressources d'une zone de disponibilité donnée ne sont pas disponibles. Toutes les ressources de calcul seront utilisées à tout moment. Cela permet un fonctionnement complet sur deux zones de disponibilité de manière active-active pour les opérations de lecture et d'écriture.

Vous pouvez interroger les vues SYS_ dans le schéma pg_catalog pour surveiller l'exécution des requêtes dans un déploiement. Multi-AZ Les vues SYS_ affichent les activités d'exécution des requêtes ou les statistiques des clusters principaux et secondaires. Pour obtenir la liste des vues de surveillance, consultez Vues de surveillance.

Suivez ces étapes pour surveiller l'exécution des requêtes pour chaque zone de disponibilité du Multi-AZ déploiement :

1. Accédez à la console Amazon Redshift, connectez-vous à la base de données de votre Multi-AZ déploiement et exécutez des requêtes via l'éditeur de requêtes.
2. Exécutez n'importe quel exemple de requête sur le déploiement Multi-AZ d'Amazon Redshift.
3. Pour un Multi-AZ déploiement, vous pouvez identifier une requête et la zone de disponibilité dans laquelle elle est exécutée à l'aide de la colonne compute_type de la table SYS_QUERY_HISTORY. primary représente les requêtes exécutées sur le cluster principal du Multi-AZ déploiement, et secondaire représente les requêtes exécutées sur le cluster secondaire du Multi-AZ déploiement.

   La requête suivante utilise la colonne compute_type pour surveiller une requête.

```
select (compute_type) as compute_type, left(query_text, 50) query_text from
 sys_query_history order by start_time desc;

 compute_type | query_text
--------------+------------------------
   secondary  | select count(*) from t1;
```

Résiliation d'une requête pour un cluster

La procédure s'applique à la fois aux Single-AZ clusters Multi-AZ et aux clusters.

Pour résilier une requête

Vous pouvez également utiliser l'onglet Requêtes pour mettre fin à une requête en cours.

L'utilisateur de votre base de données doit disposer du rôle sys:operator et des autorisations pour terminer une requête en cours d'exécution. Pour plus d'informations sur les rôles dans le système, consultez Rôles définis par le système Amazon Redshift dans le Guide du développeur de base de données Amazon Redshift.

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez REQUÊTES, puis choisissez Requêtes et chargements pour afficher la liste des requêtes pour votre compte.
3. Choisissez dans la liste la requête en cours d'exécution qui doit être arrêtée, puis choisissez Arrêter la requête.

Surveiller les performances de cluster Amazon Redshift

Amazon Redshift fournit les métriques de performance et les données de telle sorte que vous puissiez suivre l'état d'intégrité et les performances de vos clusters et bases de données. Dans cette section, nous abordons les types de données que vous pouvez utiliser dans Amazon Redshift et, plus précisément, dans la console Amazon Redshift.

Les données de performance que vous pouvez utiliser dans la console Amazon Redshift se divisent en deux catégories :

- Amazon CloudWatch metrics : Amazon CloudWatch metrics vous aide à surveiller les aspects physiques de votre cluster, tels que l'utilisation du processeur, la latence et le débit. Les données des métriques s'affichent directement dans la console Amazon Redshift. Vous pouvez également le consulter dans la CloudWatch console. Vous pouvez également l'utiliser de toute autre manière que vous utilisez les métriques, par exemple avec le AWS SDK AWS CLI ou l'un des kits de développement logiciel.
- Query/Load données de performance — Les données de performance vous aident à surveiller l'activité et les performances de la base de données. Ces données sont agrégées dans la console Amazon Redshift pour vous aider à mettre facilement en corrélation ce que vous voyez dans les CloudWatch métriques avec des requêtes de base de données et des événements de chargement spécifiques. Vous pouvez aussi créer vos propres requêtes de performance personnalisées et les exécuter directement sur la base de données. Les données de performance des requêtes et des

charges s’affichent uniquement dans la console Amazon Redshift. Elles ne sont pas publiées en tant que métriques CloudWatch .

Les données de performance sont intégrées à la console Amazon Redshift, ce qui génère une expérience plus riche, comme illustré ci-après :

- Les données de performance associées à un cluster sont affichées de manière contextuelle lorsque vous visualisez un cluster, où vous pourriez en avoir besoin pour prendre des décisions concernant le cluster, comme le redimensionnement.
- Certaines mesures de performance sont affichées dans des unités dimensionnées de manière plus appropriée dans la console Amazon Redshift que. CloudWatch Par exemple,`WriteThroughput`, est affiché dans GB/s (par rapport à bytes/s dans CloudWatch), qui est une unité plus pertinente pour l'espace de stockage typique d'un nœud.
- Vous pouvez aisément afficher des données de performances pour les nœuds d’un cluster ensemble sur le même graphique. De cette manière, vous pouvez surveiller les performances de tous les nœuds d’un cluster. Vous pouvez également consulter les données de performances pour chaque nœud.

Amazon Redshift fournit des données de performances (à la fois CloudWatch des métriques et des données de requête et de chargement) sans frais supplémentaires. Les données de performance sont enregistrées toutes les minutes. Vous pouvez accéder aux valeurs historiques des données de performance dans la console Amazon Redshift. Pour obtenir des informations détaillées sur l'accès CloudWatch aux données de performances d'Amazon Redshift qui sont exposées sous forme de CloudWatch métriques, consultez Qu'est-ce que c'est ? CloudWatch dans le guide de CloudWatch l'utilisateur Amazon.

Données de performances dans Amazon Redshift

À l'aide CloudWatch des métriques d'Amazon Redshift, vous pouvez obtenir des informations sur l'état et les performances de votre cluster et consulter des informations au niveau des nœuds. Lorsque vous utilisez ces métriques, gardez à l’esprit que chaque métrique est associée à une ou plusieurs dimensions. Ces dimensions vous indiquent à quoi s’applique la métrique, c’est-à-dire le champ d’application de la métrique. Amazon Redshift comporte les deux dimensions suivantes :

- Les métriques ayant une dimension `NodeID` sont les métriques qui fournissent les données de performance des nœuds d’un cluster. Cet ensemble de métriques inclut les nœuds principaux et les nœuds de calcul. Exemples de métriques : `CPUUtilization`, `ReadIOPS`, `WriteIOPS`.

- Les métriques qui n'ont qu'une dimension `ClusterIdentifier` sont celles qui fournissent les données de performance des clusters. Exemples de métriques : `HealthStatus` et `MaintenanceMode`.

> **Note**
>
> Dans certains cas de métriques, une métrique spécifique à un cluster représente une agrégation du comportements de nœuds. Dans ces cas, soyez attentif à l'interprétation de la valeur de la métrique, car le comportement du nœud principal est regroupé avec celui du nœud de calcul.

Pour obtenir des informations générales sur CloudWatch les mesures et les dimensions, consultez CloudWatch les concepts du guide de CloudWatch l'utilisateur Amazon.

Pour une description plus détaillée des CloudWatch métriques pour Amazon Redshift, consultez les sections suivantes.

Rubriques

- Métriques Amazon Redshift
- Dimensions des métriques Amazon Redshift
- Données de performances de charge et de requête Amazon Redshift

Métriques Amazon Redshift

L'espace de noms `AWS/Redshift` inclut les métriques suivantes. Sauf indication contraire, les métriques sont collectées à intervalles d'une minute.

Métrique	Description
`CommitQueueLength`	Nombre de transactions en attente de validation à un moment donné dans le temps. Unités : nombre Dimensions : `ClusterIdentifier`

Métrique	Description
`ConcurrencyScaling ActiveClusters`	Nombre de clusters de mise à l'échelle de la simultanéité qui traitent activement des requêtes à un instant donné. Unités : nombre Dimensions : `ClusterIdentifier`
`ConcurrencyScaling Seconds`	Nombre de secondes utilisées par les clusters de mise à l'échelle de la simultanéité qui traitent activement des requêtes. Unités : nombre Dimensions : `ClusterIdentifier`
`CPUUtilization`	Pourcentage d'utilisation de la CPU. Pour les clusters, cette métrique représente une agrégation de toutes les valeurs d'utilisation par l'UC des nœuds (principal et calcul). Unités : pourcentage Dimensions: `ClusterIdentifier` , `NodeID` Dimensions : `ClusterIdentifier`
`DatabaseConnections`	Nombre de connexions de base de données d'un cluster. Unités : nombre Dimensions : `ClusterIdentifier`

Métrique	Description
`HealthStatus`	Indique l'état d'intégrité du cluster. Toutes les minutes, le cluster se connecte à sa base de données et exécute une requête simple. S'il est en mesure d'effectuer cette opération avec succès, le cluster est considéré comme sain. Sinon, le cluster est défectueux. Un état défectueux peut se produire lorsque la base de données du cluster subit une très lourde charge ou s'il y a un problème de configuration avec une base de données du cluster. **Note** Dans Amazon CloudWatch, cette métrique est signalée comme 1 ou 0 alors que dans la console Amazon Redshift, elle est affichée avec les mots `HEALTHY` ou `UNHEALTHY` pour des raisons pratiques. Lorsque cette métrique est affichée dans la console Amazon Redshift, les moyennes d'échantillonnage sont ignorées et seuls `HEALTHY` ou `UNHEALTHY` sont affichés. Sur Amazon CloudWatch, des valeurs différentes de 1 et 0 peuvent apparaître en raison d'un problème d'échantillonnage. Toute valeur inférieure à 1 pour `HealthStatus` est présentée en tant que 0 (`UNHEALTHY`). Unités : Count (1/0) (`HEALTHY`/`UNHEALTHY` dans la console Amazon Redshift) Dimensions : `ClusterIdentifier`

Métrique	Description
`MaintenanceMode`	Indique si le cluster est en mode maintenance. **Note** Dans Amazon CloudWatch, cette métrique est signalée comme 1 ou 0 alors que dans la console Amazon Redshift, elle est affichée avec les mots `ON` ou `OFF` pour des raisons pratiques. Lorsque cette métrique est affichée dans la console Amazon Redshift, les moyennes d'échantillonnage sont ignorées et seuls `ON` ou `OFF` sont affichés. Sur Amazon CloudWatch, des valeurs différentes de 1 et 0 peuvent apparaître en raison de problèmes d'échantillonnage. Toute valeur supérieure à 0 pour `MaintenanceMode` est présentée en tant que 1 (`ON`). Unités : Count (1/0) (`ON`/`OFF`dans la console Amazon Redshift). Dimensions : `ClusterIdentifier`
`MaxConfiguredConcurrencyScalingClusters`	Nombre maximum de clusters de mise à l'échelle de la simultanéité configurés à partir du groupe de paramètres. Pour plus d'informations, consultez Groupes de paramètres Amazon Redshift. Unités : nombre Dimensions : `ClusterIdentifier`
`NetworkReceiveThroughput`	Débit auquel le nœud ou cluster reçoit des données. Unités : Bytes/Second (MB/s dans la console Amazon Redshift) Dimensions: `ClusterIdentifier` , `NodeID` Dimensions : `ClusterIdentifier`

Métrique	Description
`NetworkTransmitThroughput`	Débit auquel le nœud ou cluster écrit des données. Unités : Bytes/Second (MB/s dans la console Amazon Redshift) Dimensions: `ClusterIdentifier` , `NodeID` Dimensions : `ClusterIdentifier`
`PercentageDiskSpaceUsed`	Pourcentage d'espace disque utilisé. Unités : pourcentage Dimensions : `ClusterIdentifier` Dimensions: `ClusterIdentifier` , `NodeID`
`QueriesCompletedPerSecond`	Nombre moyen de requêtes terminées par seconde. Communiqué par intervalles de 5 minutes. Cette métrique n'est pas prise en charge sur les clusters à un seul nœud. Unités : Count/Second Dimensions: `ClusterIdentifier` , `latency` Dimensions: `ClusterIdentifier` , `wlmid`
`QueryDuration`	Durée moyenne pour exécuter une requête. Communiqué par intervalles de 5 minutes. Cette métrique n'est pas prise en charge sur les clusters à un seul nœud. Unités : microsecondes Dimensions : `ClusterIdentifier` , `NodeID`, `latency` Dimensions: `ClusterIdentifier` , `latency` Dimensions : `ClusterIdentifier` , `NodeID`, `wlmid`

Métrique	Description
QueryRuntimeBreakdown	Durée totale des requêtes exécutées par étape de requête. Communiqué par intervalles de 5 minutes. Unités : millisecondes Dimensions : ClusterIdentifier, NodeID, étage Dimensions : ClusterIdentifier, scène
ReadIOPS	Nombre moyen d'opérations de lecture de disque par seconde. Unités : Count/Second Dimensions: ClusterIdentifier , NodeID Dimensions : ClusterIdentifier
ReadLatency	Durée moyenne des I/O opérations de lecture du disque. Unités : secondes Dimensions: ClusterIdentifier , NodeID Dimensions : ClusterIdentifier
ReadThroughput	Nombre moyen d'octets lus sur le disque par seconde. Unités : octets (GB/s dans la console Amazon Redshift) Dimensions: ClusterIdentifier , NodeID Dimensions : ClusterIdentifier
RedshiftManagedStorageTotalCapacity	Capacité de stockage géré totale. Unités : mégaoctets Dimensions : ClusterIdentifier

Métrique	Description
RgUniqueSnapshotStorage	Nombre de mégaoctets de blocs de données uniques stockés dans tous les instantanés manuels actifs de la famille d'instances RG. Unités : mégaoctets
TotalTableCount	Le nombre total de tables à un moment donné. Ce total inclut les tables permanentes, les tables temporaires, les tables de partage de données, les tables externes et les vues matérialisées. Les vues et les tables système ne sont pas incluses dans ce décompte. Unités : nombre Dimensions : ClusterIdentifier
WLMQueueLength	Nombre de requêtes en attente d’entrée dans la file d’attente de gestion de la charge de travail (WLM). Unités : nombre Dimensions: ClusterIdentifier , service class Dimensions: ClusterIdentifier , QueueName
WLMQueueWaitTime	Temps total pendant lequel les requêtes attendent dans la file d’attente de gestion des charges de travail. Communiqué par intervalles de 5 minutes. Unités : millisecondes. Dimensions: ClusterIdentifier , QueryPriority Dimensions: ClusterIdentifier , wlmid Dimensions: ClusterIdentifier , QueueName

Métrique	Description
WLMQueriesCompletedPerSecond	Nombre moyen de requêtes terminées par seconde pour une file d'attente de gestion de la charge de travail (WLM). Communiqué par intervalles de 5 minutes. Cette métrique n'est pas prise en charge sur les clusters à un seul nœud. Unités : Count/Second Dimensions: ClusterIdentifier , wlmid Dimensions: ClusterIdentifier , QueueName
WLMQueryDuration	Durée moyenne pour exécuter une requête pour une file d'attente de gestion de la charge de travail (WLM). Communiqué par intervalles de 5 minutes. Cette métrique n'est pas prise en charge sur les clusters à un seul nœud. Unités : microsecondes Dimensions: ClusterIdentifier , wlmid Dimensions: ClusterIdentifier , QueueName
WLMRunningQueries	Le nombre de requêtes s'exécutant depuis le cluster principal et le cluster de mise à l'échelle de simultanéité par file d'attente WLM. Unités : nombre Dimensions: ClusterIdentifier , wlmid Dimensions: ClusterIdentifier , QueueName
WriteIOPS	Nombre moyen d'opérations d'écriture par seconde. Unités : Count/Second Dimensions: ClusterIdentifier , NodeID Dimensions : ClusterIdentifier

Métrique	Description
`WriteLatency`	Durée moyenne des I/O opérations d'écriture sur disque. Unités : secondes Dimensions: `ClusterIdentifier` , `NodeID` Dimensions : `ClusterIdentifier`
`WriteThroughput`	Nombre moyen d’octets écrits sur le disque par seconde. Unités : octets (GB/s dans la console Amazon Redshift) Dimensions: `ClusterIdentifier` , `NodeID` Dimensions : `ClusterIdentifier`
`SchemaQuota`	Quota configuré pour un schéma. Unités : mégaoctets Dimensions : `ClusterIdentifier` , `Database`, `Schema` Periodic/Push: `Periodic` Fréquence : `5 minutes` Critères d’arrêt : schéma abandonné ou quota supprimé
`NumExceededSchemaQuotas`	Nombre de schémas avec des quotas dépassés. Unités : nombre Dimensions : `ClusterIdentifier` Periodic/Push: `Periodic` Fréquence : `5 minutes` Critères d'arrêt : N/A

Métrique	Description
`StorageUsed`	Espace disque ou de stockage utilisé par un schéma. Unités : mégaoctets Dimensions : `ClusterIdentifier` , `Database`, `Schema` Periodic/Push: `Periodic` Fréquence : `5 minutes` Critères d'arrêt : schéma abandonné ou quota supprimé
`PercentageQuotaUsed`	Pourcentage d'espace disque ou de stockage utilisé par rapport au quota de schéma configuré. Unités : pourcentage Dimensions : `ClusterIdentifier` , `Database`, `Schema` Periodic/Push: `Periodic` Fréquence : `5 minutes` Critères d'arrêt : schéma abandonné ou quota supprimé

Métrique	Description
UsageLimitAvailable	En fonction de FeatureType, UsageLimitAvailable renvoie les informations suivantes : • Si FeatureType c'est le casCONCURRENCY_SCALING , UsageLimitAvailable renvoie la durée totale qui peut être utilisée par la mise à l'échelle de la simultanéité par incrément s d'une minute. Ce temps ne compte pas comme temps disponible pour CONCURRENCY_SCALING_AUTO_TASK et vice versa. • Si FeatureType c'est le casCONCURRENCY_SCALIN G_AUTO_TASK , UsageLimitAvailable renvoie le temps total qui peut être utilisé par la mise à l'échelle de la simultané ité pour les tâches d'optimisation automatique. Ce temps ne compte pas comme temps disponible pour le CONCURREN CY_SCALING et vice versa. • Si FeatureType c'est le casEXTRA_COMPUTE_FOR_ AUTOMATIC_OPTIMIZATION , UsageLimitAvailable renvoie le temps total disponible à utiliser pour les tâches d'optimisation automatique. • Si FeatureType c'est le casCROSS_REGION_DATAS HARING , UsageLimitAvailable renvoie la quantité totale de données pouvant être numérisées par incréments de 1 To. • Si FeatureType c'est le casSPECTRUM, UsageLimitAvailable renvoie la quantité totale de données pouvant être numérisées par incréments de 1 To. Unités : minutes ou To Dimensions : ClusterIdentifier , FeatureType , UsageLimitId

Métrique	Description
UsageLimitConsumed	En fonction de FeatureType, UsageLimitConsumed renvoie les informations suivantes : • Si FeatureType c'est le casCONCURRENCY_SCALING , UsageLimitConsumed renvoie le temps total utilisé par la mise à l'échelle de la simultanéité par incréments d'une minute. Ce temps ne compte pas comme temps utilisé pour CONCURRENCY_SCALING_AUTO_TASK et vice versa. • Si FeatureType c'est le casCONCURRENCY_SCALING_AUTO_TASK , UsageLimitConsumed renvoie le temps total qui a été utilisé par la mise à l'échelle de la simultanéité pour les tâches d'optimisation automatique. Ce temps ne compte pas comme temps utilisé pour CONCURRENCY_SCALING et vice versa. • Si FeatureType c'est le casEXTRA_COMPUTE_FOR_AUTOMATIC_OPTIMIZATION , UsageLimitConsumed renvoie le temps total utilisé pour les tâches d'optimisation automatique. • Si FeatureType c'est le casCROSS_REGION_DATASHARING , UsageLimitConsumed renvoie la quantité totale de données numérisées par incréments de 1 To. • Si FeatureType c'est le casSPECTRUM, UsageLimitConsumed renvoie la quantité totale de données numérisées par incréments de 1 To. Unités : minutes ou To Dimensions : ClusterIdentifier , FeatureType , UsageLimitId

Dimensions des métriques Amazon Redshift

Les données Amazon Redshift peuvent être filtrées selon n'importe quelle dimension dans le tableau suivant.

Dimension	Description
`latency`	Les valeurs possibles sont les suivantes : • short – moins de 10 secondes • medium – entre 10 secondes et 10 minutes • long – plus de 10 minutes
`NodeID`	Filtre les données demandées qui sont spécifiques aux nœuds d'un cluster. `NodeID`Dest soit « Leader », soit « Shared », soit Compute-N « » où N est égal à 0, 1,... pour le nombre de nœuds du cluster. « Shared » signifie que le cluster a un seul nœud, c'est-à-dire le nœud principal, et que les nœuds de calcul sont associés. Les métriques pour `CPUUtilization` , `NetworkTransmitThroughput` et `ReadIOPS` sont communiquées uniquement pour le nœud principal et les nœuds de calcul. Les autres métriques qui utilisent la dimension `NodeId` sont communiquées uniquement pour les nœuds de calcul.
`ClusterIdentifier`	Les filtres ont demandé des données spécifiques au cluster. Les métriques spécifiques aux clusters incluent `HealthStatus` , `MaintenanceMode` et `DatabaseConnections` . Les métriques générales de cette dimension (par exemple `ReadIOPS`) qui sont également des métriques de nœuds représentent une agrégation des données des métriques de nœud. Veillez à interpréter ces métriques parce qu'elles regroupent un comportement de nœud principal et de nœuds de calcul.
`service class`	Identifiant d'une classe de service `WLM`.

Dimension	Description
`stage`	Étapes de l'exécution d'une requête. Les valeurs possibles sont les suivantes : • QueryPlanning : Temps passé à analyser et à optimiser les instructions SQL. • QueryWaiting: temps passé à attendre dans la file d'attente WLM. • QueryExecutingRead: temps passé à exécuter des requêtes de lecture. • QueryExecutingInsert: temps passé à exécuter des requêtes d'insertion. • QueryExecutingDelete: temps passé à exécuter des requêtes de suppression. • QueryExecutingUpdate: temps passé à exécuter des requêtes de mise à jour. • QueryExecutingCtas: temps passé à exécuter la création d'une table sous forme de requêtes. • QueryExecutingUnload: temps passé à exécuter des requêtes de déchargement. • QueryExecutingCopy: temps passé à exécuter des requêtes de copie. • QueryCommit: Temps passé à s'engager.
`wlmid`	Identifiant d'une file d'attente de gestion de la charge de travail.
`QueryPriority`	Priorité de la requête. Les valeurs possibles sont `CRITICAL`, `HIGHEST`, `HIGH`, `NORMAL`, `LOW` et `LOWEST`.
`QueueName`	Nom de la file d'attente de gestion des charges de travail.
`FeatureType`	Fonctionnalité limitée par une limite d'utilisation. Les valeurs possibles sont `CONCURRENCY_SCALING` , `CROSS_REGION_DATASHARING` et `SPECTRUM`.

Dimension	Description
`UsageLimitId`	Identifiant d'une limite d'utilisation.

Données de performances de charge et de requête Amazon Redshift

Outre les CloudWatch métriques, Amazon Redshift fournit des données sur les performances de requête et de chargement. Les données de performance de chargement et de requête peuvent vous aider à comprendre la relation entre les performances de base de données et les métriques de cluster. Par exemple, si vous remarquez que l'UC d'un cluster a des pics, vous pouvez trouver le pic dans le graphique de l'UC du cluster et afficher les requêtes qui s'exécutaient à ce moment-là. Inversement, si vous examinez une requête spécifique, les données des métriques (comme l'UC) s'affichent dans le contexte afin que vous puissiez comprendre l'impact de la requête sur les métriques de cluster.

Les données de performances de requête et de chargement ne sont pas publiées sous forme de CloudWatch mesures et ne peuvent être consultées que dans la console Amazon Redshift. Les données de performance de requête et de chargement sont générées à partir de requêtes avec les tables système de votre base de données (pour de plus amples informations, consultez Référence des tables système dans le Guide du développeur Amazon Redshift). Vous pouvez également générer vos propres requêtes de performances de base de données, mais nous vous recommandons de commencer par les données de performance de chargement et de requête présentées dans la console. Pour plus d'informations sur la mesure et la surveillance des performances de votre base de données par vous-même, consultez Gestion des performances dans le Guide du développeur Amazon Redshift.

Le tableau suivant décrit les différents aspects des données de requête et de chargement auxquels vous pouvez accéder dans la console Amazon Redshift.

Query/Load données	Description
Résumé des requêtes	Liste de requêtes sur une durée déterminée. La liste peut être triée sur des valeurs telles que l'ID de requête, la durée d'exécution et l'état. Affichez ces données dans l'onglet Surveillance des requêtes de la page de détails du cluster.

Query/Load données	Description
Détails de la requête	Fournit des détails sur une requête donnée, notamment : • Propriétés de la requête, telles que l'ID de requête, le type, le cluster sur lequel la requête a été exécutée et la durée d'exécution. • Détails tels que l'état de la requête et le nombre d'erreurs. • Instruction SQL exécutée. • Plan d'explication s'il est disponible. • Données de performances du cluster pendant l'exécution de la requête (pour de plus amples informations, consultez Affichage de l'historique des requêtes).
Résumé des charges	Répertorie toutes les charges sur une durée déterminée. La liste peut être triée sur des valeurs telles que l'ID de requête, la durée d'exécution et l'état. Affichez ces données dans l'onglet Surveillance des requêtes de la page de détails du cluster.
Détails de charge	Fournit des détails sur une opération de charge particulière, notamment : • Propriétés de la charge, telles que l'ID de requête, le type, le cluster sur lequel la requête a été exécutée et la durée d'exécution. • Détails tels que l'état de la charge et le nombre d'erreurs. • Instruction SQL exécutée. • Liste des fichiers chargés. • Données de performances du cluster pendant l'opération de chargemen t (pour de plus amples informations, consultez Affichage de l'historique des requêtes).

Consultation des données de performances

Cette section explique comment afficher les données de performance dans la console Amazon Redshift, lesquelles incluent les informations sur les performances du cluster et des requêtes. En outre, vous pouvez créer des alarmes sur les métriques du cluster directement à partir de la console Amazon Redshift.

Lorsque vous consultez les données de performance dans la console Amazon Redshift, vous les visualisez par cluster. Les graphiques des données de performances d'un cluster sont conçus pour vous permettre d'accéder aux données et répondre à vos questions de performance les plus courantes. Pour certaines données de performances (voir Données de performances dans Amazon Redshift), vous pouvez également utiliser CloudWatch pour personnaliser davantage vos graphiques de métriques. Par exemple, vous pouvez choisir des durées plus longues ou combiner des métriques de plusieurs clusters. Pour de plus amples informations sur l'utilisation de la console CloudWatch, veuillez consulter Statistiques de performance dans la CloudWatch console.

Regardez la vidéo suivante pour apprendre à surveiller, isoler et optimiser vos requêtes à l'aide des fonctions de surveillance des requêtes de la console Amazon Redshift : Surveillance des requêtes avec Amazon Redshift.

Rubriques

- Affichage des données de performances de cluster
- Affichage de l'historique des requêtes
- Affichage des données de performances de base de données
- Affichage de la simultanéité des charges de travail et données de mise à l'échelle de la simultanéité
- Affichage des données d'optimisation automatique
- Affichage des requêtes et des charges
- Affichage et analyse des détails des requêtes
- Afficher les performances de cluster pendant l'exécution des requêtes
- Affichage des métriques du cluster pendant les opérations de chargement
- Affichage du graphe de répartition de l'exécution de la charge de travail sur le cluster

Affichage des données de performances de cluster

En utilisant les métriques de cluster dans Amazon Redshift, vous pouvez effectuer les tâches de performance communes suivantes :

- Déterminer si les métriques de cluster sont anormales au-dessus d'une durée spécifiée et, si tel est le cas, identifier les requêtes responsables de cette augmentation.
- Vérifier si les requêtes historiques ou actuelles ont un impact sur les performances de cluster. SI vous identifiez une requête problématique, vous pouvez en consulter les détails, y compris les

performances du cluster pendant l'exécution de la requête. Vous pouvez utiliser ces informations pour diagnostiquer la lenteur de la requête et voir ce qu'il est possible de faire pour en améliorer les performances.

Pour consulter les données de performances

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters, puis choisissez le nom d'un cluster dans la liste pour ouvrir ses détails. Les détails du cluster sont affichés, ce qui peut inclure les onglets Performance du cluster, Surveillance des requêtes, Bases de données, Unités de partage des données, Planifications, Maintenance et Propriétés.
3. Choisissez l'onglet Performance de cluster pour obtenir des informations sur la performance, notamment les suivantes :

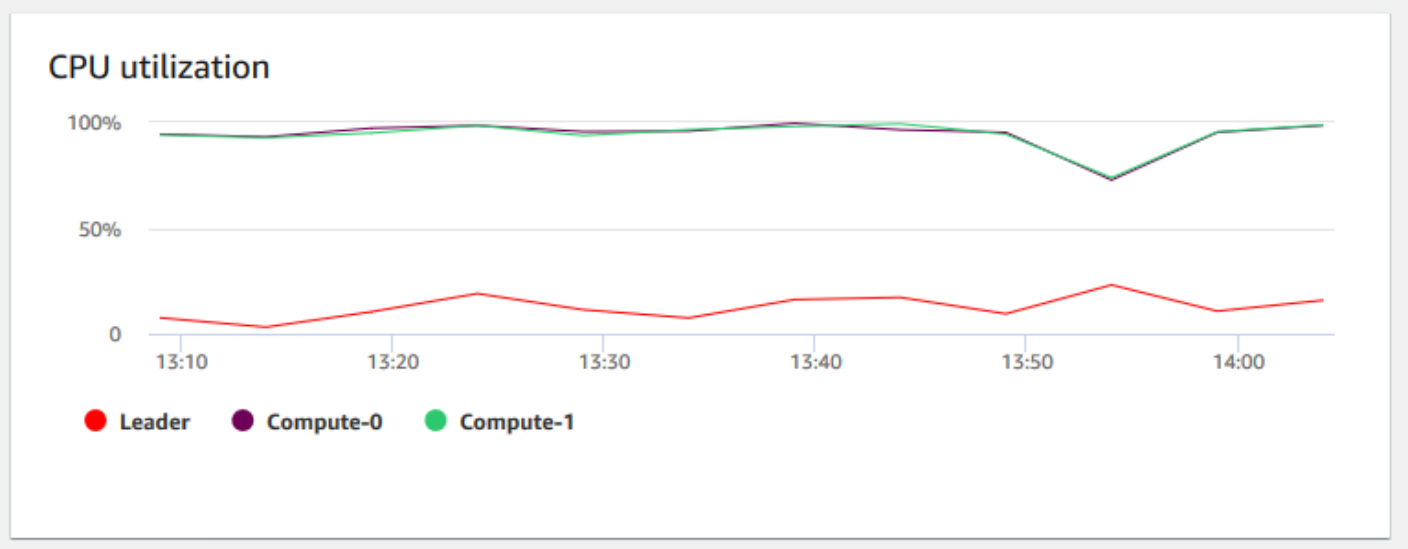
   - Utilisation de l'UC
   - Pourcentage d'espace disque utilisé
   - Connexions de la base de données
   - État de santé
   - Durée de requête
   - Débit de requête
   - Activité de mise à l'échelle de simultanéité

   De nombreuses autres métriques sont disponibles. Pour voir les métriques disponibles et choisir celles qui sont affichées, choisissez l'icône Préférences.

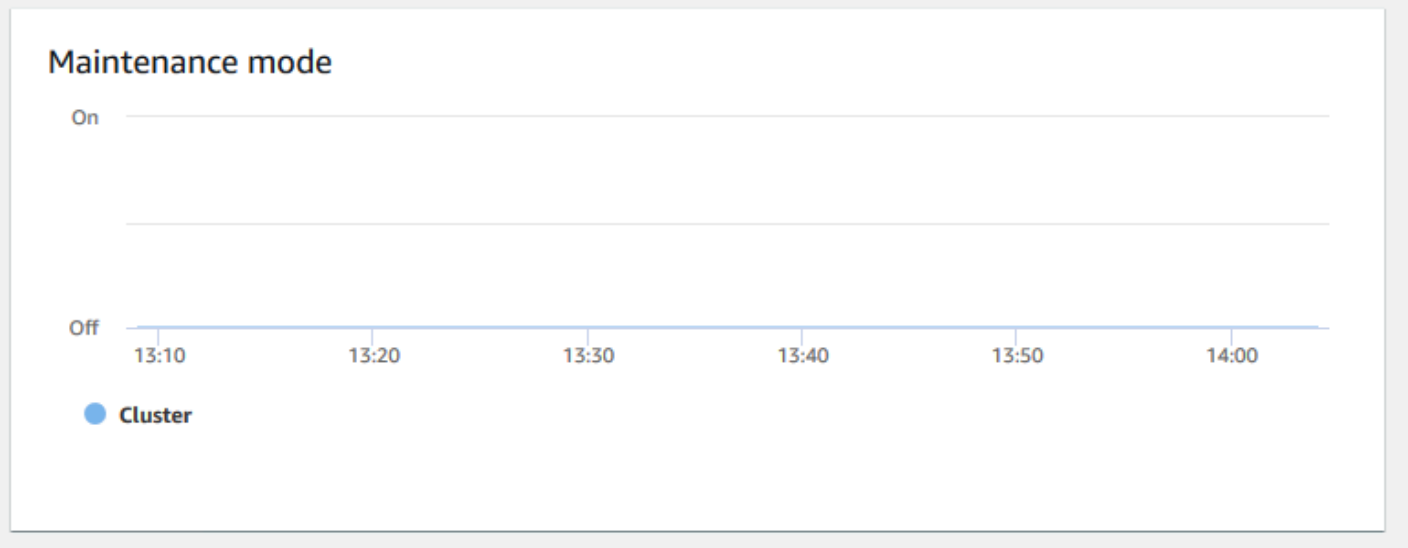
Graphiques de performances de cluster

Les exemples suivants illustrent certains des graphiques affichés dans la nouvelle console Amazon Redshift.

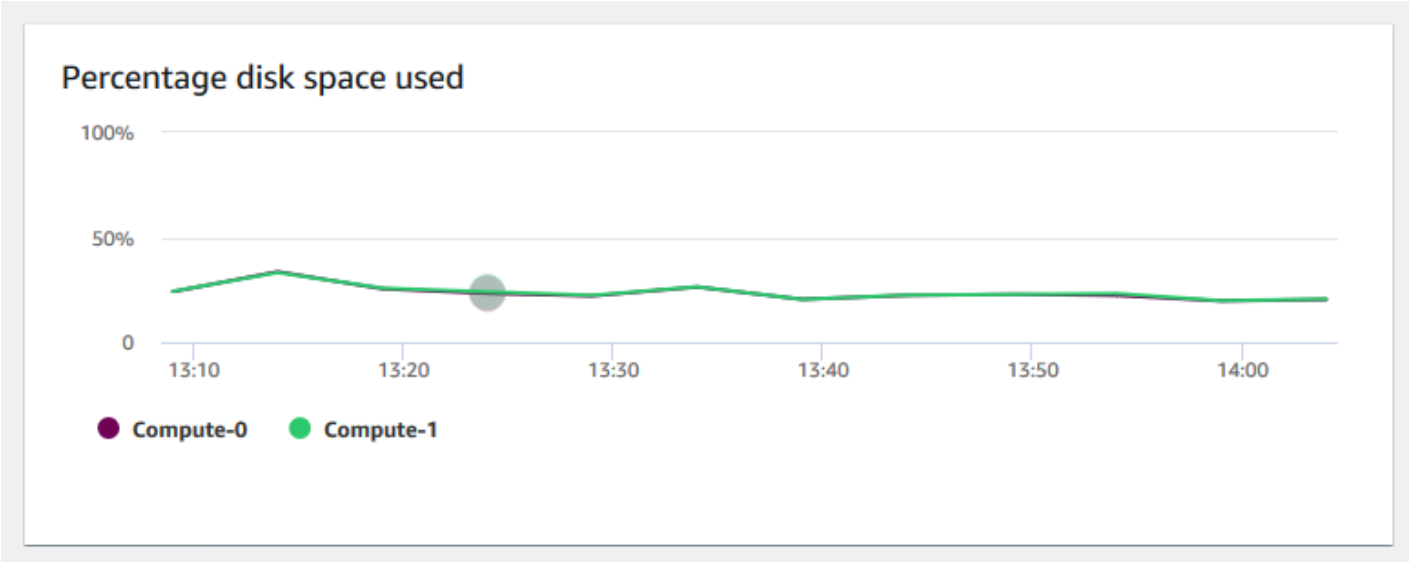
- Utilisation du CPU – Indique le pourcentage d'utilisation du CPU pour tous les nœuds (principal et calcul). Pour trouver une heure où l'utilisation du cluster est la plus faible avant de planifier la migration du cluster ou d'autres opérations consommant des ressources, surveillez ce graphique pour voir l'utilisation de l'UC par individu ou tous les nœuds.



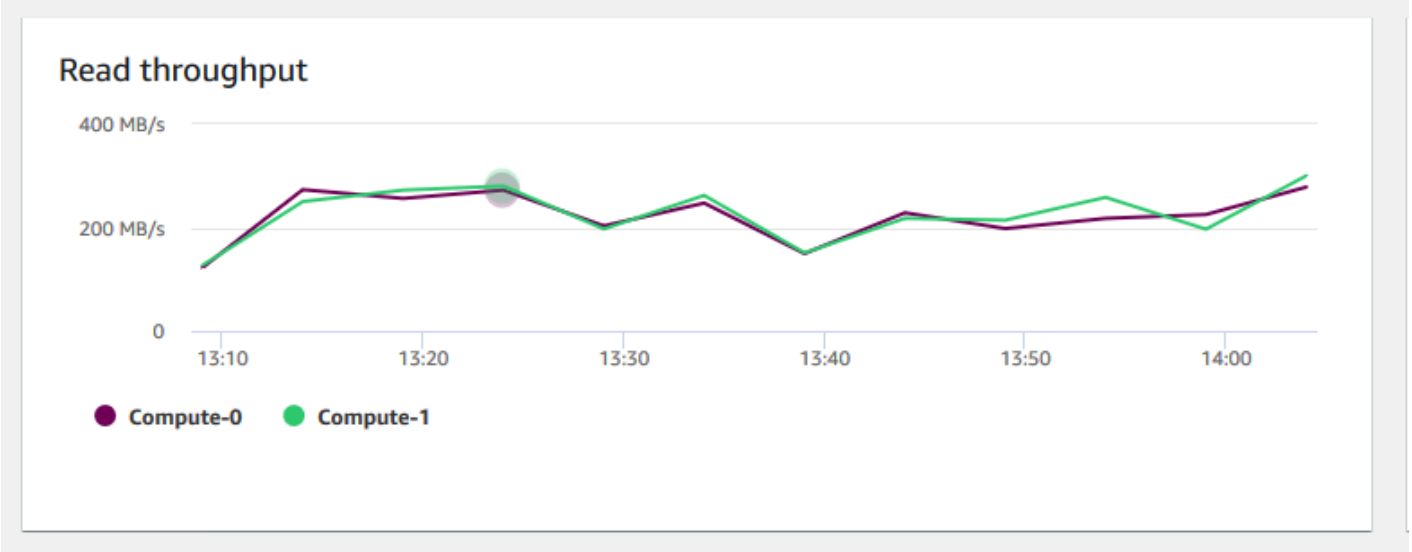
- Mode maintenance – Indique si le cluster est en mode maintenance à un moment donné à l'aide des indicateurs `On` et `Off`. Vous pouvez voir l'heure à laquelle le cluster est en cours de maintenance. Vous pouvez ensuite mettre en corrélation cette fois avec les opérations effectuées sur le cluster afin d'estimer ses temps d'arrêt futurs pour les événements récurrents.



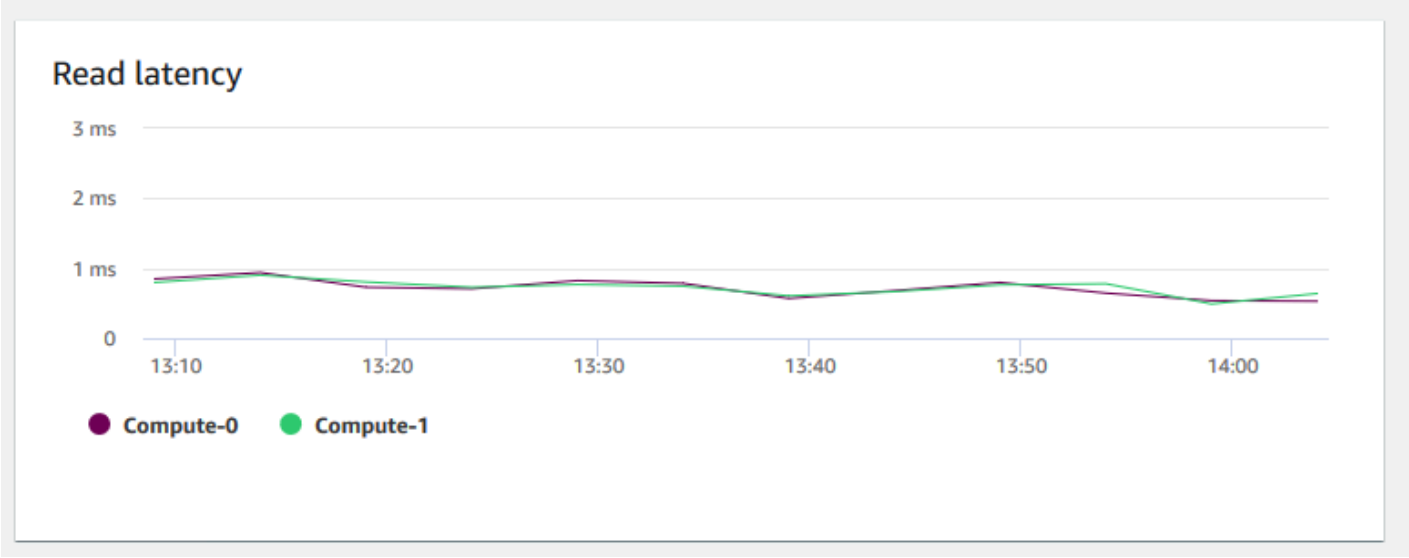
- Pourcentage d'espace disque utilisé – Indique le pourcentage d'utilisation de l'espace disque pour chaque nœud de calcul, et non pour le cluster dans son ensemble. Vous pouvez explorer ce graphique pour surveiller l'utilisation du disque. Les opérations de maintenance telles que VACUUM et COPY utilisent un espace de stockage temporaire intermédiaire pour leurs opérations de tri, ce qui entraîne généralement un pic d'utilisation du disque.



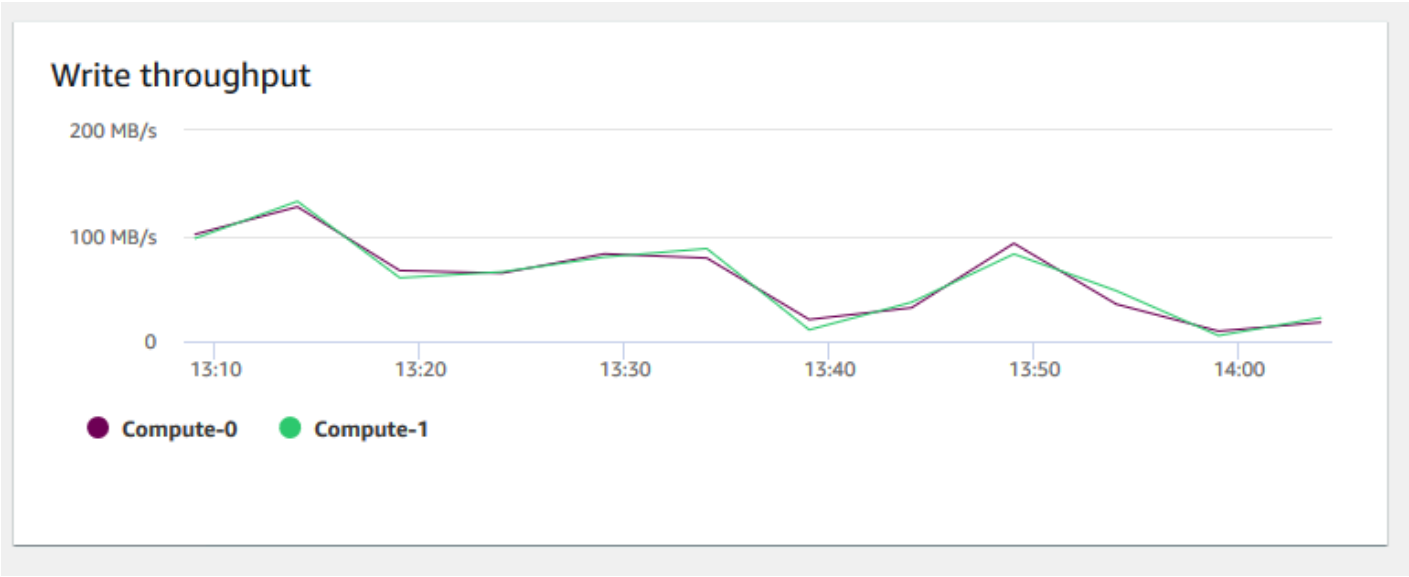
- Débit de lecture – Indique le nombre moyen de mégaoctets lus sur le disque par seconde. Vous pouvez évaluer ce graphique pour surveiller l'aspect physique correspondant du cluster. Ce débit n'inclut pas le trafic réseau entre les instances du cluster et le volume de cluster.



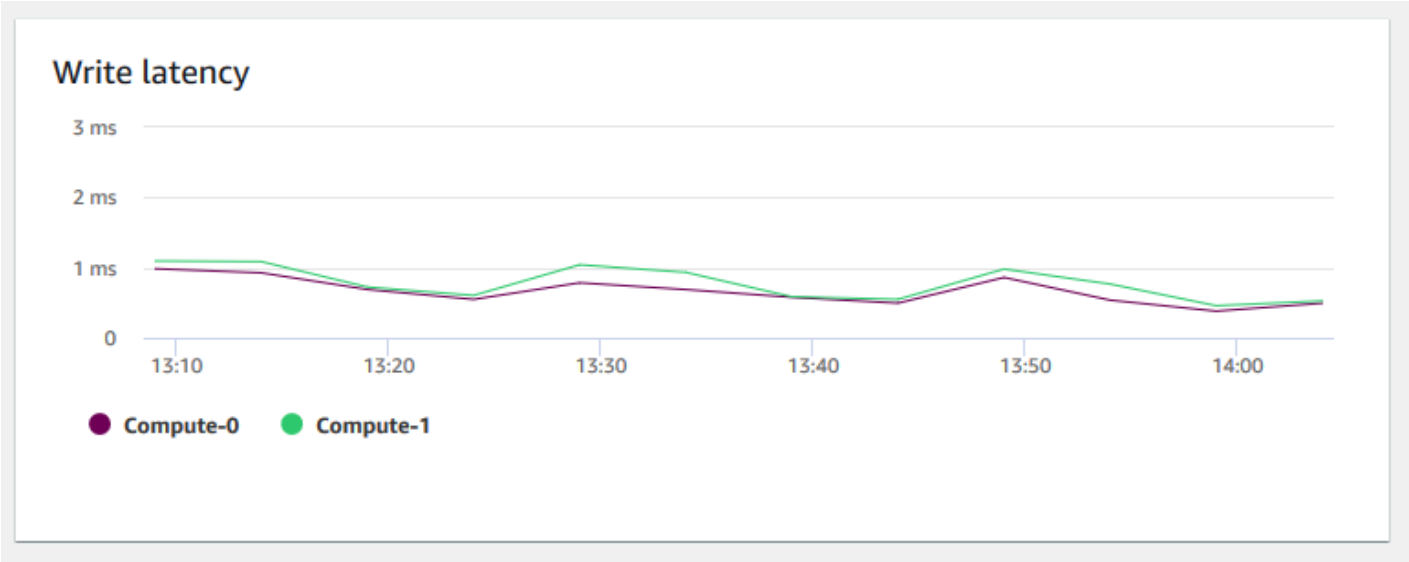
- Latence de lecture : indique le temps moyen nécessaire aux I/O opérations de lecture sur disque par milliseconde. Vous pouvez afficher les temps de réponse pour que les données reviennent. Lorsque la latence est élevée, cela signifie que l'expéditeur passe plus de temps inactif (sans envoyer de nouveaux paquets), ce qui réduit la vitesse de croissance du débit.



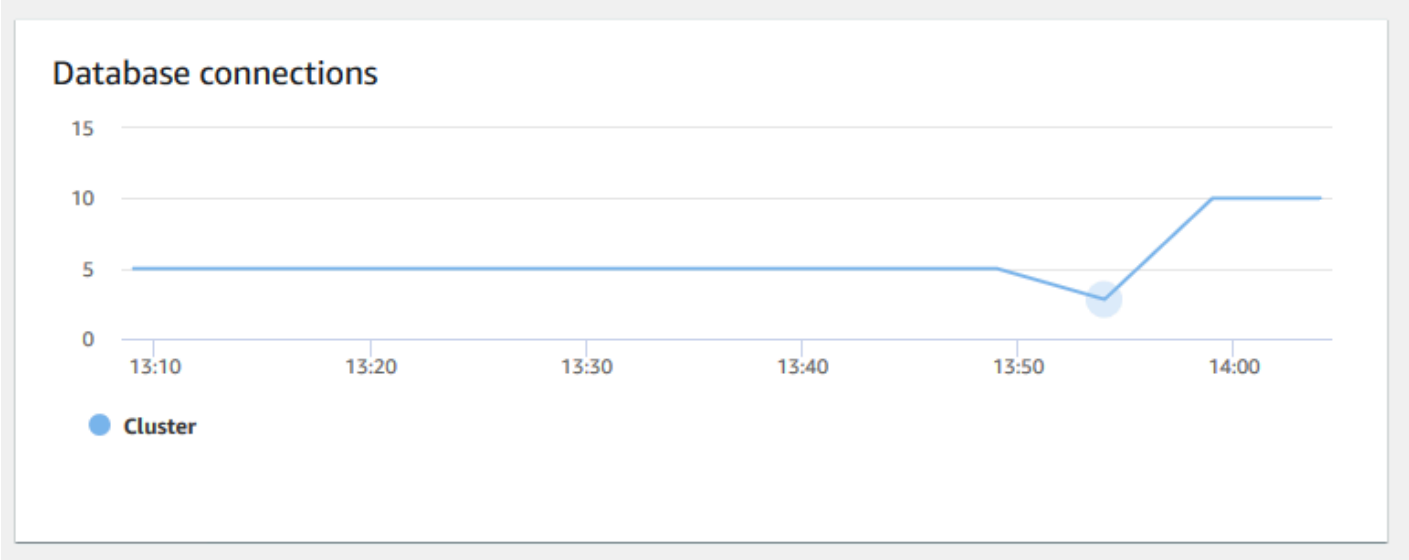
- Débit d’écriture – Indique le nombre moyen de mégaoctets écrits sur le disque par seconde. Vous pouvez évaluer cette métrique pour surveiller l’aspect physique correspondant du cluster. Ce débit n’inclut pas le trafic réseau entre les instances du cluster et le volume de cluster.



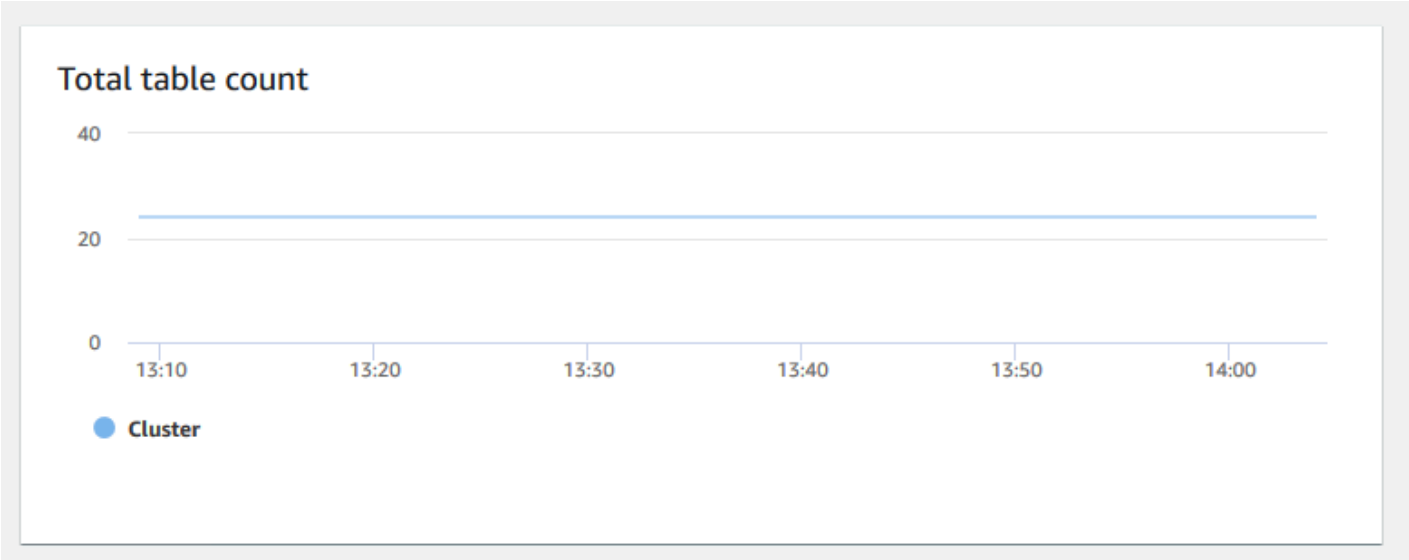
- Latence d'écriture : indique la durée moyenne en millisecondes nécessaires aux opérations d'écriture I/O sur disque. Vous pouvez évaluer le temps de retour de l’accusé de réception d’écriture. Lorsque la latence est élevée, cela signifie que l’expéditeur passe plus de temps inactif (sans envoyer de nouveaux paquets), ce qui réduit la vitesse de croissance du débit.



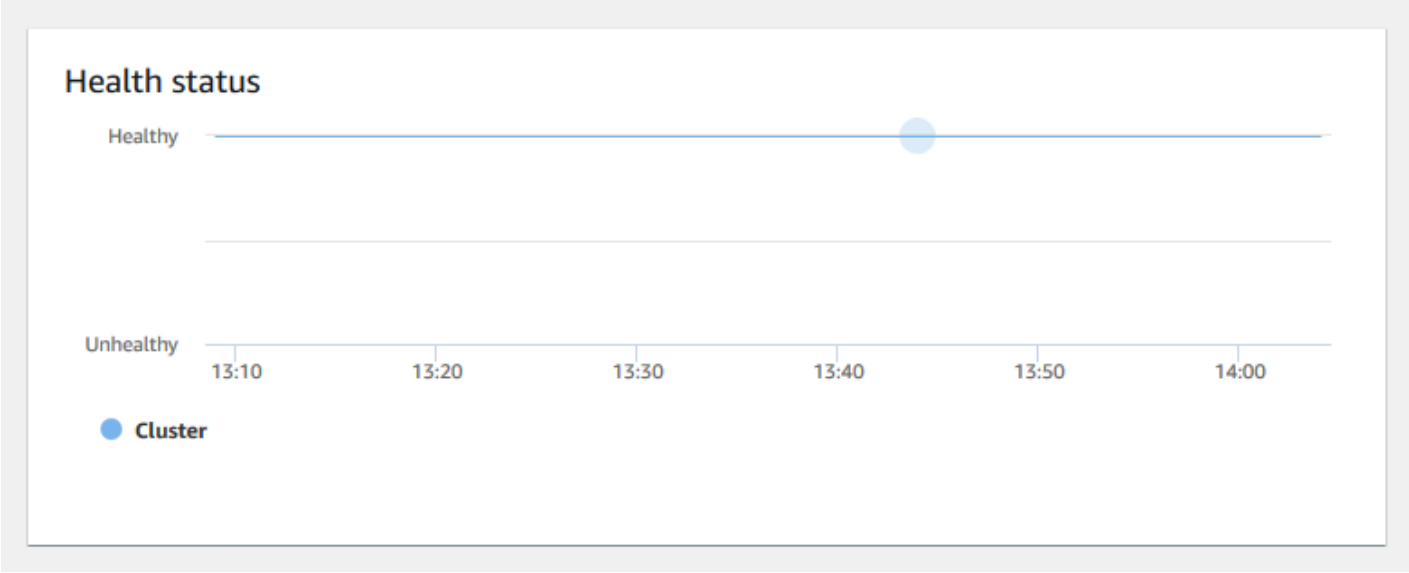
- Connexions à la base de données – Indique le nombre de connexions à la base de données d'un cluster. Vous pouvez utiliser ce graphique pour voir le nombre de connexions établies à la base de données et trouver une heure où l'utilisation du cluster est la plus faible.



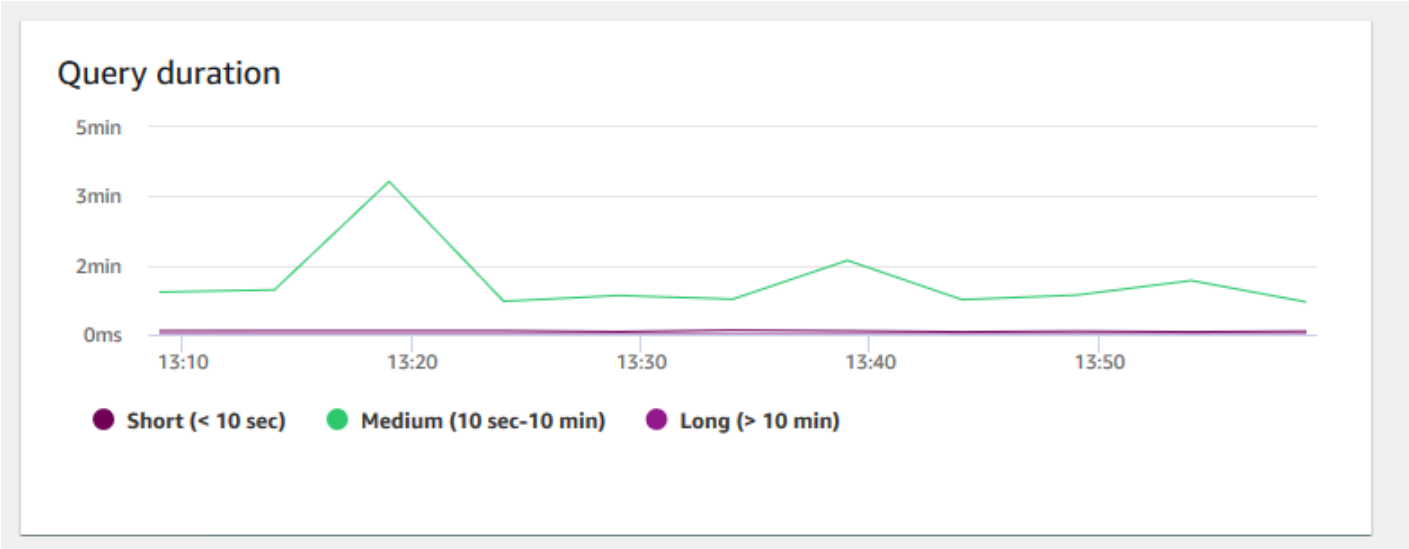
- Nombre total de tables – Indique le nombre de tables utilisateur ouvertes à un moment donné dans un cluster. Vous pouvez surveiller les performances du cluster lorsque le nombre de tables ouvertes est élevé.



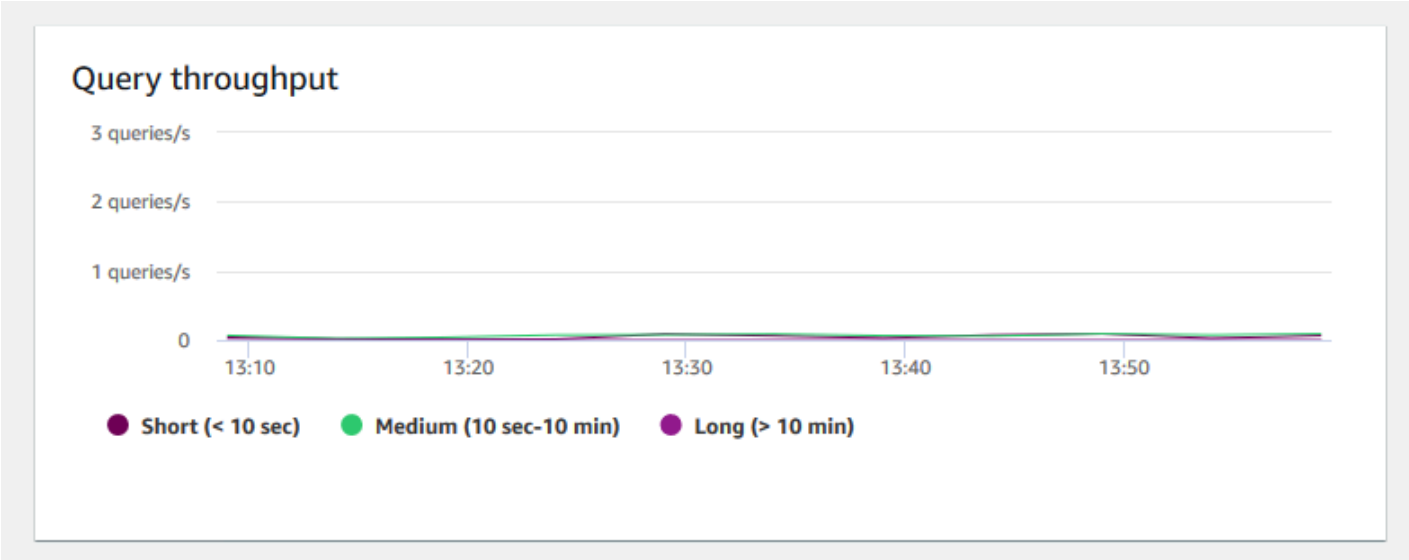
- État d'intégrité – Indique l'état d'intégrité du cluster comme `Healthy` ou `Unhealthy`. Si le cluster peut se connecter à sa base de données et exécuter une requête simple avec succès, le cluster est considéré comme sain. Sinon, le cluster est défectueux. Un état défectueux peut se produire lorsque la base de données du cluster subit une très lourde charge ou s'il y a un problème de configuration avec une base de données du cluster.



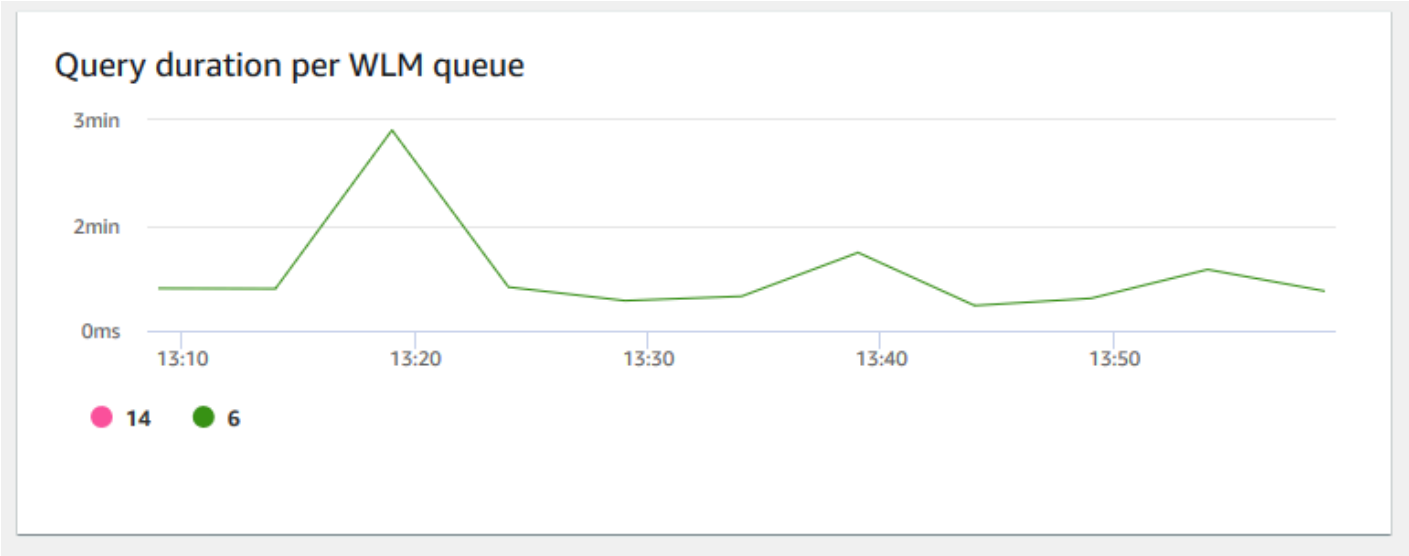
- Durée de la requête – Indique la durée moyenne d'exécution d'une requête en microsecondes. Vous pouvez comparer les données de ce graphique pour mesurer les I/O performances au sein du cluster et ajuster ses requêtes les plus chronophages si nécessaire.



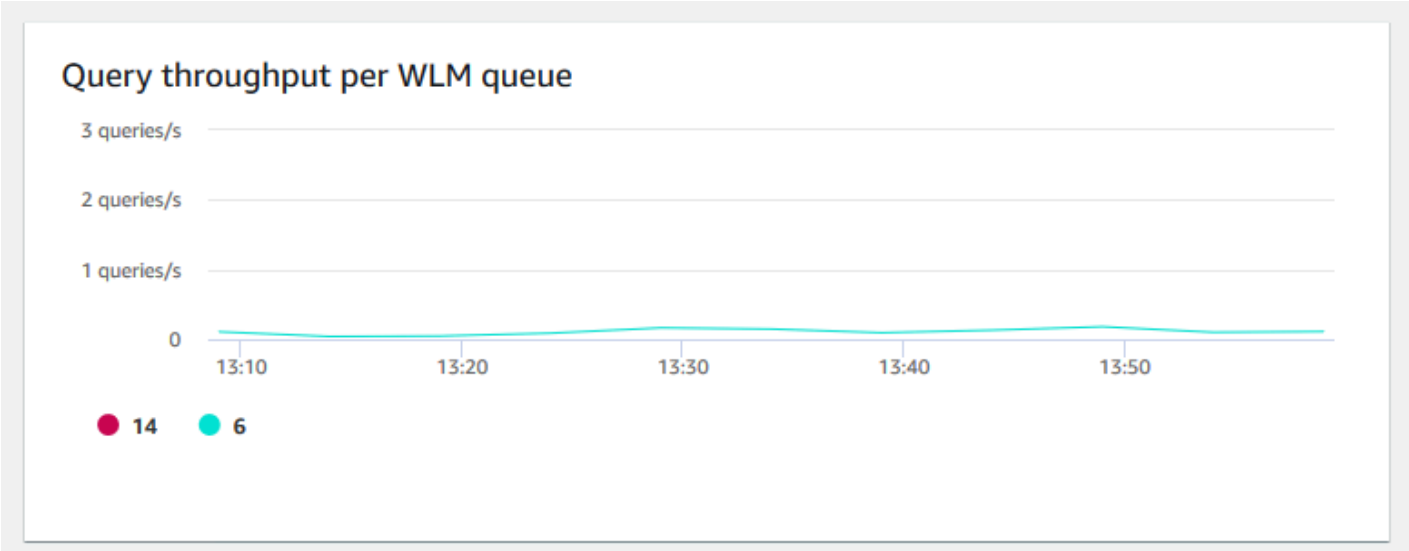
- Débit des requêtes – Indique le nombre moyen de requêtes terminées par seconde. Vous pouvez analyser les données de ce graphique pour mesurer les performances de la base de données et caractériser la capacité du système à traiter une charge de travail multiutilisateur de manière équilibrée.



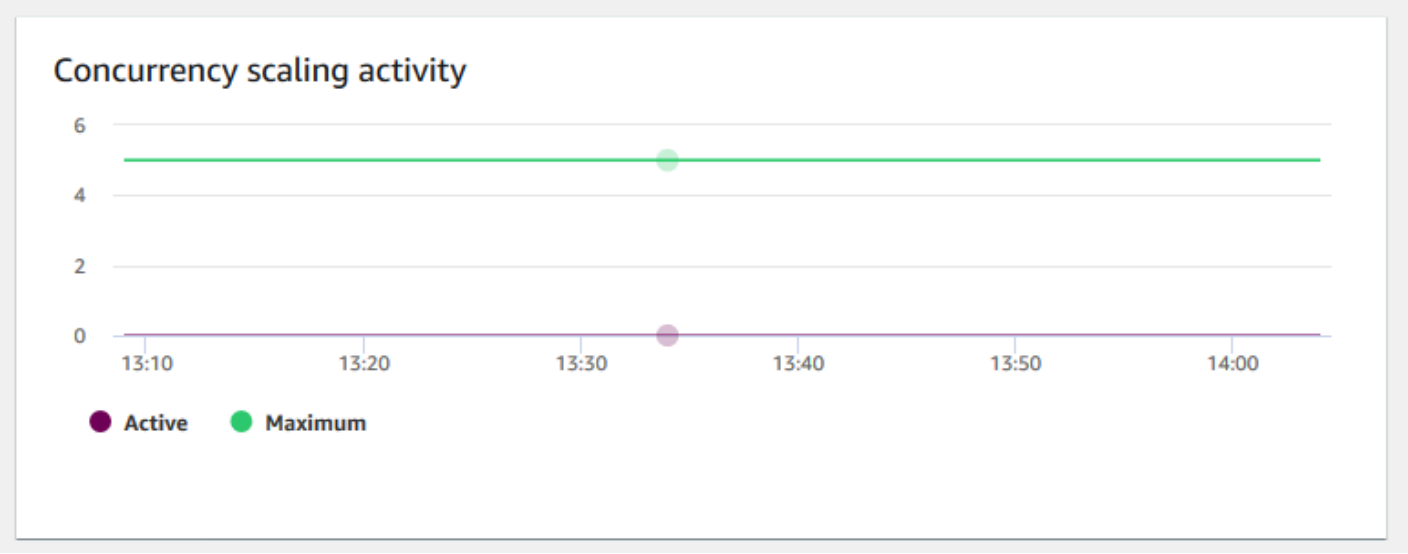
- Durée de la requête par file d'attente WLM – Indique la durée moyenne d'exécution d'une requête en microsecondes. Vous pouvez comparer les données de ce graphique pour mesurer les I/O performances par file d'attente WLM et ajuster ses requêtes les plus chronophages si nécessaire.



- Débit de requêtes par file d'attente WLM – Indique le nombre moyen de requêtes terminées par seconde. Vous pouvez analyser les données de ce graphique pour mesurer les performances de base de données par file d'attente WLM.



- Activité de mise à l'échelle de la simultanéité – Indique le nombre de clusters de mise à l'échelle de la simultanéité. Lorsque la mise à l'échelle de la simultanéité est activée, Amazon Redshift ajoute automatiquement de la capacité de cluster supplémentaire lorsque vous en avez besoin pour traiter une augmentation des requêtes de lecture simultanées.



Affichage de l'historique des requêtes

Vous pouvez utiliser les métriques de l'historique des requêtes dans Amazon Redshift pour faire ce qui suit :

- Isoler et diagnostiquer les problèmes de performances des requêtes.
- Comparer les métriques d'exécution des requêtes et les métriques de performance du cluster sur la même chronologie pour voir comment les deux peuvent être liées. Cela aide à identifier les requêtes qui ne s'exécutent pas correctement, à rechercher les goulets d'étranglement et à déterminer si vous devez redimensionner votre cluster pour votre charge de travail.
- Exploration vers le bas jusqu'aux détails d'une requête spécifique en la sélectionnant dans la chronologie. Lorsque l'ID de requête et d'autres propriétés sont affichés dans une ligne sous le graphique, vous pouvez choisir la requête pour afficher les détails de la requête. Les détails incluent, par exemple, l'instruction SQL de la requête, les détails d'exécution et le plan de requête. Pour plus d'informations, consultez Affichage et analyse des détails des requêtes.
- Déterminez si vos travaux de chargement se terminent correctement et respectent vos contrats de niveau de service (SLA).

Pour afficher les données de l'historique des requêtes

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.

2. Dans le menu de navigation, choisissez Clusters, puis choisissez le nom du cluster dans la liste pour ouvrir ses détails. Les détails du cluster sont affichés, ce qui peut inclure les onglets Performance du cluster, Surveillance des requêtes, Bases de données, Unités de partage des données, Planifications, Maintenance et Propriétés.
3. Choisissez l'onglet Surveillance des requêtes pour connaître les métriques relatives à vos requêtes.
4. Dans la section Surveillance des requêtes choisissez l'onglet Historique des requêtes.

   À l'aide des contrôles de la fenêtre, vous pouvez basculer entre la liste de requêtes et les métriques de cluster.

   Lorsque vous choisissez la liste de requêtes, l'onglet inclut les graphiques suivants :

   - Exécution de la requête – L'activité de la requête sur une ligne de temps. Utilisez ce graphique pour voir quelles requêtes sont en cours d'exécution pendant la même période. Choisissez une requête pour afficher plus de détails sur l'exécution de la requête. L'axe des x affiche la période sélectionnée. Vous pouvez filtrer les requêtes graphiques selon les critères En cours d'exécution, Terminées, Charges, etc. Chaque barre représente une requête, et la longueur de la barre représente son exécution depuis le début de la barre jusqu'à la fin. Les requêtes peuvent inclure des instructions de manipulation de données SQL (telles que SELECT, INSERT, DELETE) et des charges (telles que COPY). Par défaut, les 100 requêtes les plus longues en cours d'exécution sont affichées pour la période sélectionnée.
   - Requêtes et charges – Liste des requêtes et des charges qui ont été exécutées sur le cluster. La fenêtre inclut une option de Terminer la requête si une requête est en cours d'exécution.

   Lorsque vous choisissez Métriques de cluster, l'onglet inclut les graphiques suivants :

   - Exécution de la requête – L'activité de la requête sur une ligne de temps. Utilisez ce graphique pour voir quelles requêtes sont en cours d'exécution pendant la même période. Choisissez une requête pour afficher plus de détails sur l'exécution de la requête.
   - Utilisation du CPU – L'utilisation du CPU du cluster par le nœud principal et la moyenne des nœuds de calcul.
   - Capacité de stockage utilisée – Le pourcentage de la capacité de stockage utilisée.
   - Connexions de base de données actives – Le nombre de connexions de base de données actives au cluster.

Tenez compte des éléments suivants lorsque vous utilisez les graphiques d'historique des requêtes :

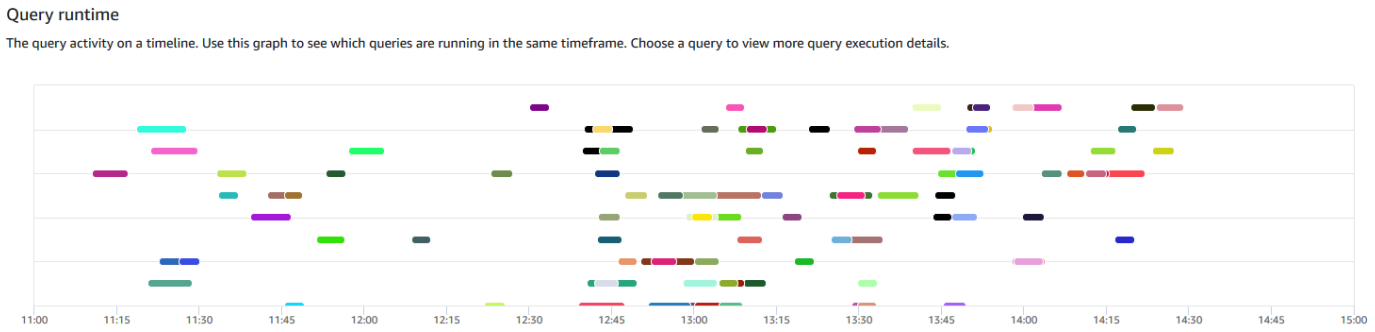
- Choisissez une barre qui représente une requête spécifique dans le graphique Exécution de la requête pour afficher les détails de cette requête. Vous pouvez également choisir un ID de requête dans la liste Requêtes et charges pour voir ses détails.
- Vous pouvez effectuer un balayage pour sélectionner une section du graphique Exécution de requête pour effectuer un zoom afin d'afficher une période spécifique.
- Dans le graphique Exécution de la requête, pour que toutes les données soient prises en compte par le filtre choisi, faites défiler toutes les pages répertoriées dans la liste Requêtes et charges.
- Vous pouvez modifier les colonnes et le nombre de lignes affichées dans la liste Requêtes et charges à l'aide de la fenêtre de préférences affichée par l'icône des paramètres (engrenage).
- La liste Requêtes et charges peut également être affichée en naviguant à partir de l'icône Requêtes du navigateur gauche, Requêtes et charges. Pour plus d'informations, consultez Affichage des requêtes et des charges.

Graphiques de l'historique des requêtes

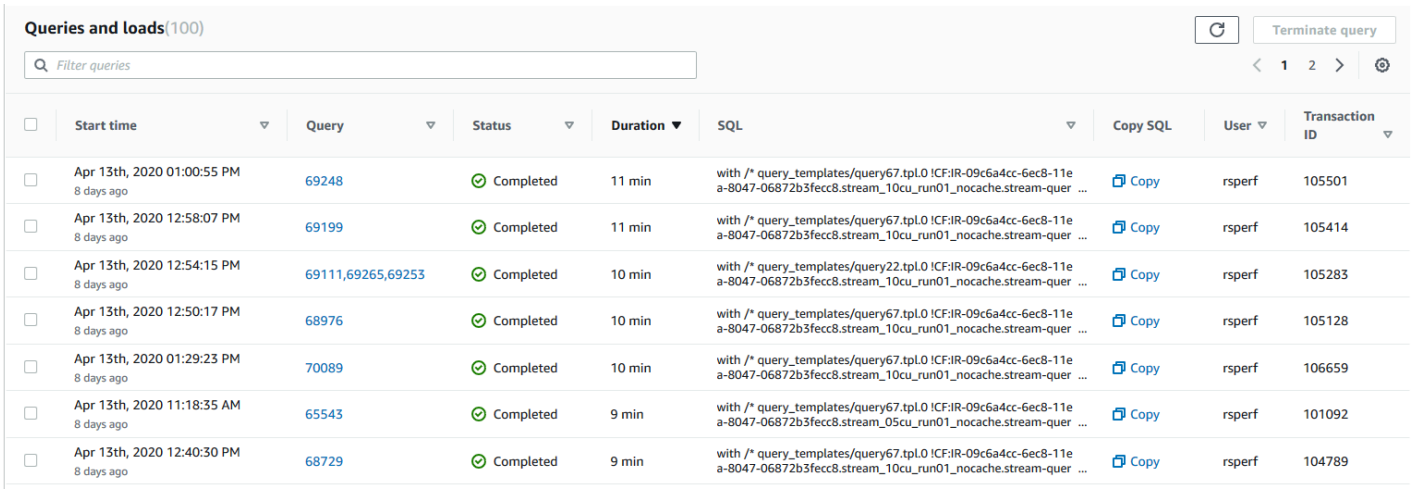
Les exemples suivants illustrent les graphiques qui s'affichent dans la nouvelle console Amazon Redshift.

> **Note**
>
> Les graphiques de la console Amazon Redshift ne contiennent que les données des 100 000 requêtes les plus récentes.

- Exécution de requête



- Requêtes et charges



Queries and loads(100)

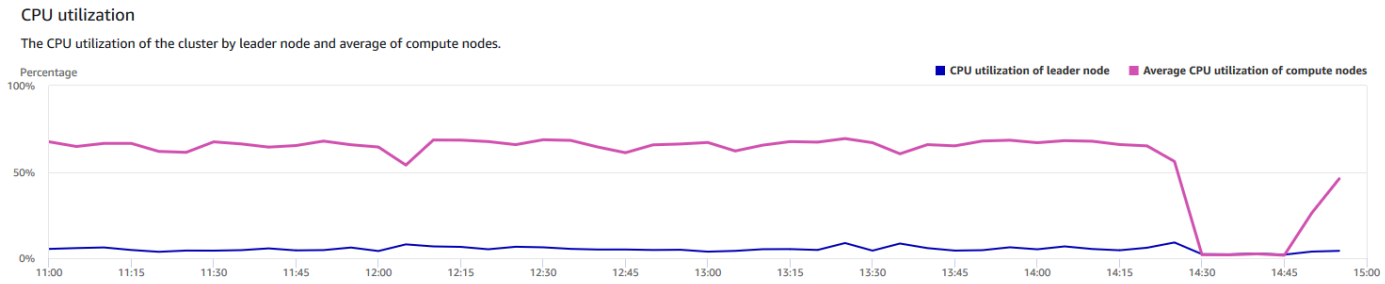
Filter queries

Terminate query

1 2

Start time	Query	Status	Duration	SQL	Copy SQL	User	Transaction ID
Apr 13th, 2020 01:00:55 PM 8 days ago	69248	Completed	11 min	with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105501
Apr 13th, 2020 12:58:07 PM 8 days ago	69199	Completed	11 min	with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105414
Apr 13th, 2020 12:54:15 PM 8 days ago	69111,69265,69253	Completed	10 min	with /* query_templates/query22.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105283
Apr 13th, 2020 12:50:17 PM 8 days ago	68976	Completed	10 min	with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105128
Apr 13th, 2020 01:29:23 PM 8 days ago	70089	Completed	10 min	with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	106659
Apr 13th, 2020 11:18:35 AM 8 days ago	65543	Completed	9 min	with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_05cu_run01_nocache.stream-quer ...	Copy	rsperf	101092
Apr 13th, 2020 12:40:30 PM 8 days ago	68729	Completed	9 min	with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	104789

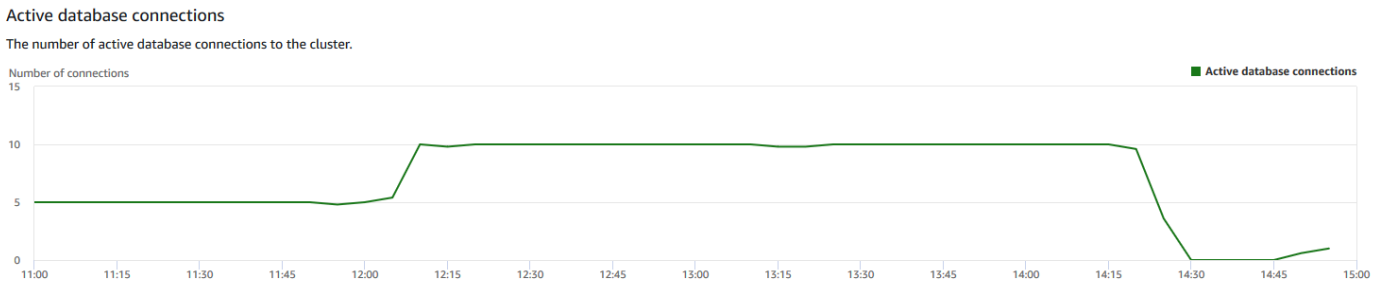
- Utilisation de l'UC



- Capacité de stockage utilisée



- Connexions actives à la base de données



Affichage des données de performances de base de données

Vous pouvez utiliser les mesures de performances de base de données dans Amazon Redshift pour effectuer les opérations suivantes :

- Analyser le temps passé par les requêtes par étapes de traitement. Vous pouvez rechercher des tendances inhabituelles dans le temps passé dans une étape.
- Analyser le nombre de requêtes, la durée et le débit des requêtes par plages de durée (courte, moyenne, longue).
- Rechercher les tendances concernant le temps d'attente de requête par priorité de requête (la plus faible, faible, normale, élevée, la plus élevée, critique).
- Rechercher les tendances de la durée de la requête, du débit ou du temps d'attente par file d'attente WLM.

Pour afficher les données de performances de base de données

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters, puis choisissez le nom du cluster dans la liste pour ouvrir ses détails. Les détails du cluster sont affichés, notamment les onglets Performance du cluster, Surveillance des requêtes, Bases de données, Unités de partage des données, Planifications, Maintenance et Propriétés.
3. Choisissez l'onglet Surveillance des requêtes pour connaître les métriques relatives à vos requêtes.
4. Dans la section Surveillance des requêtes, choisissez l'onglet Performances de la base de données.

   À l'aide des contrôles de la fenêtre, vous pouvez basculer entre les métriques de cluster et les métriques de file d'attente WLM.

   Lorsque vous choisissez Métriques de cluster, l'onglet inclut les graphiques suivants :

   - Répartition de l'exécution de la charge de travail – Le temps utilisé dans les étapes de traitement des requêtes.
   - Requêtes par plage de durée – Le nombre de requêtes courtes, moyennes et longues.
   - Débit de requête – Le nombre moyen de requêtes effectuées par seconde.

- Durée de la requête – Le temps moyen nécessaire pour exécuter une requête.
- Temps d'attente moyen par priorité –Le temps total d'attente des requêtes dans la file d'attente WLM par priorité de requête.

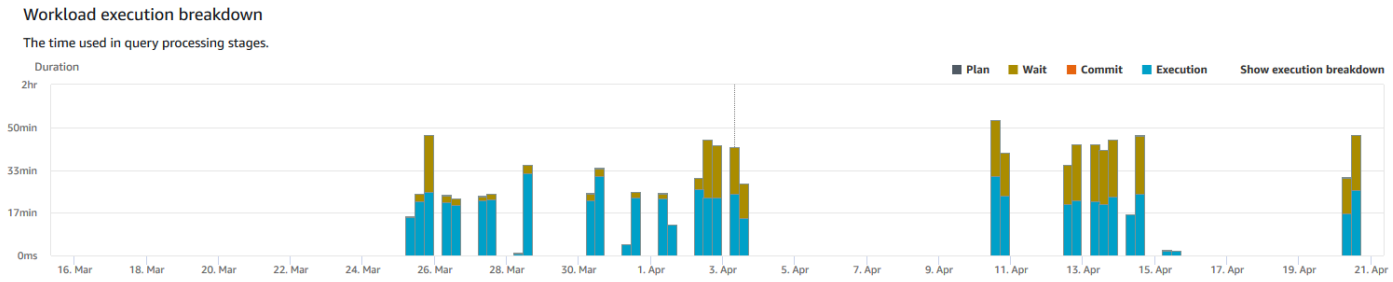
Lorsque vous choisissez des métriques de file d'attente WLM, l'onglet inclut les graphiques suivants :

- Durée de la requête par file d'attente –La durée moyenne de la requête par file d'attente WLM.
- Débit des requêtes par file d'attente –Le nombre moyen de requêtes effectuées par seconde par file d'attente WLM.
- Temps d'attente des requêtes par file d'attente –La durée moyenne d'attente des requêtes par file d'attente WLM.

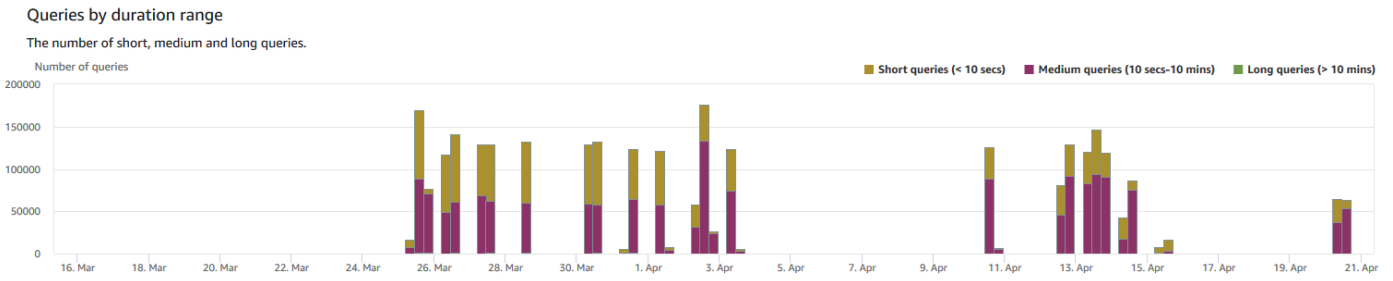
Graphiques de performances de base de données

Les exemples suivants illustrent les graphiques qui s'affichent dans la nouvelle console Amazon Redshift.

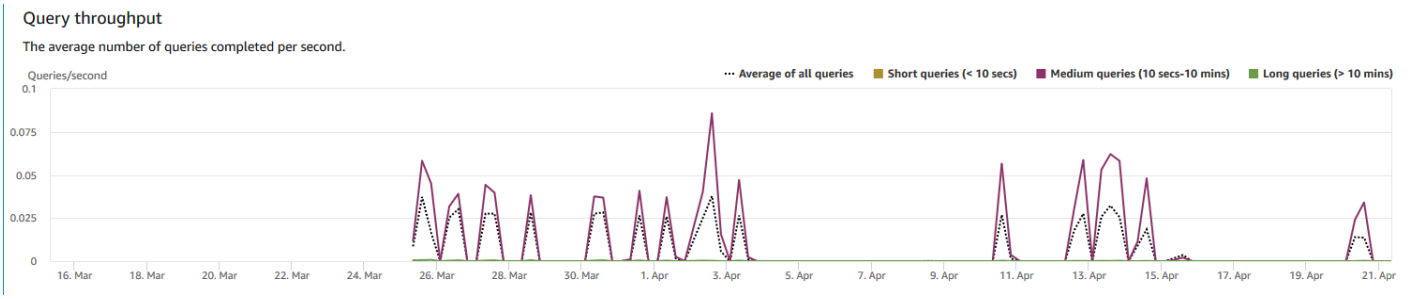
- Répartition de l'exécution de la charge de travail



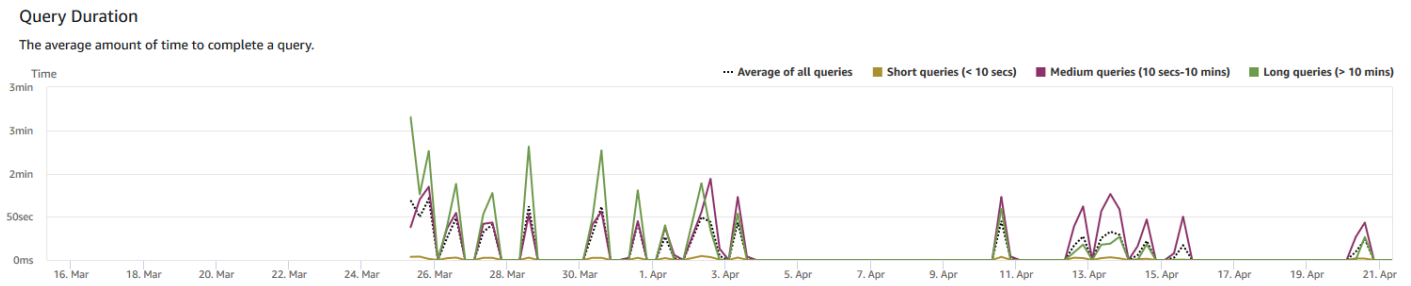
- Requêtes par plage de durée



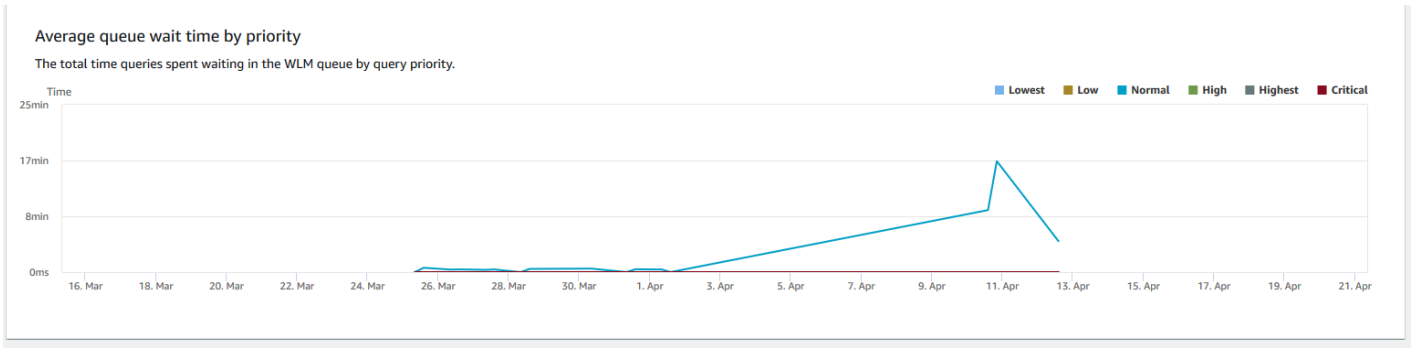
- Débit de requête



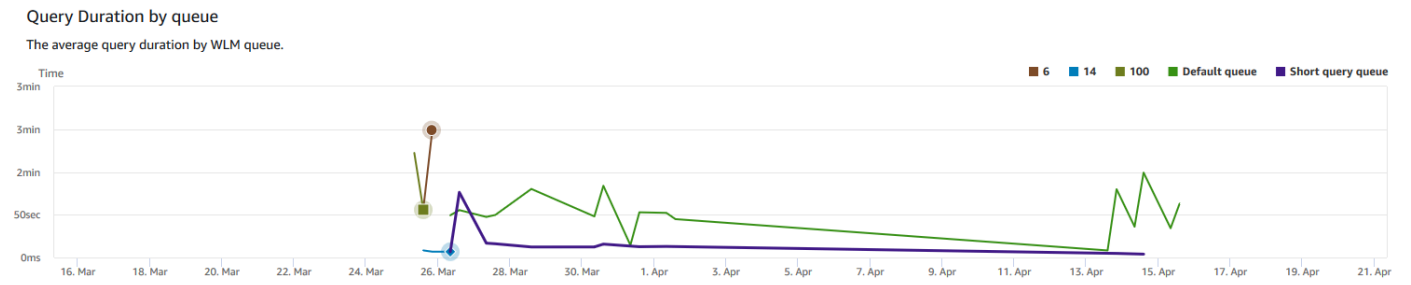
- Durée de requête



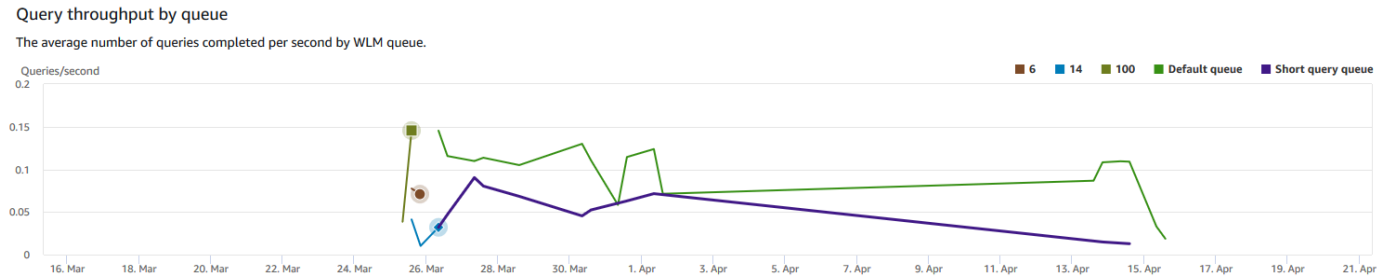
- Temps d’attente moyen par priorité



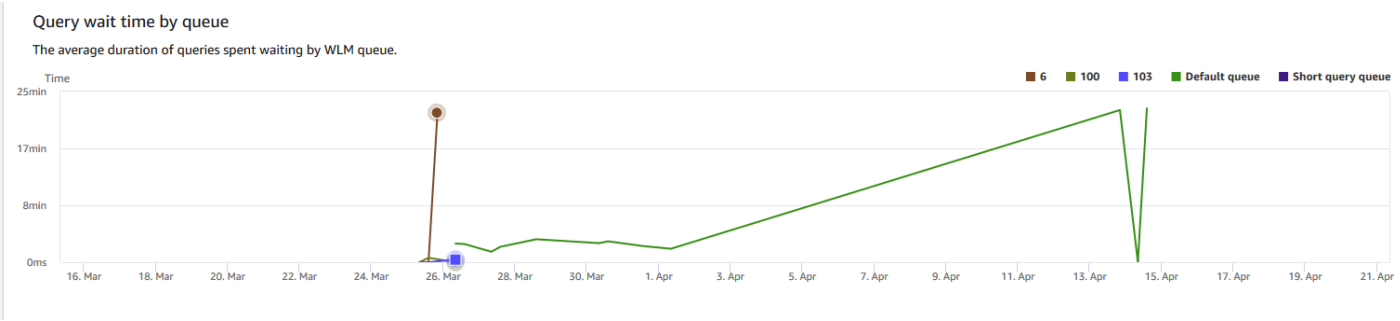
- Durée de la requête par file d’attente



- Débit de requête par file d’attente



- Interroger le temps d'attente par file d'attente



Affichage de la simultanéité des charges de travail et données de mise à l'échelle de la simultanéité

En utilisant des métriques de mise à l'échelle de simultanéité dans Amazon Redshift, vous pouvez effectuer les actions suivantes :

- Analyser si vous pouvez réduire le nombre de requêtes en file d'attente en activant la mise à l'échelle de la simultanéité. Vous pouvez comparer par file d'attente WLM ou pour toutes les files d'attente WLM.
- Affichage de l'activité de mise à l'échelle de la simultanéité dans les clusters de mise à l'échelle de la simultanéité. Cela peut vous indiquer si la de mise à l'échelle de la simultanéité est limitée par `max_concurrency_scaling_clusters`. Si c'est le cas, vous pouvez choisir d'augmenter la valeur de `max_concurrency_scaling_clusters` dans le paramètre de base de données.
- Affichage de l'utilisation totale de la mise à l'échelle de la simultanéité cumulée sur tous les clusters de mise à l'échelle de la simultanéité.

Pour afficher les données de mise à l'échelle de la simultanéité

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.

2. Dans le menu de navigation, choisissez Clusters, puis choisissez le nom du cluster dans la liste pour ouvrir ses détails. Les détails du cluster sont affichés, ce qui peut inclure les onglets Performance du cluster, Surveillance des requêtes, Bases de données, Unités de partage des données, Planifications, Maintenance et Propriétés.
3. Choisissez l'onglet Surveillance des requêtes pour connaître les métriques relatives à vos requêtes.
4. Dans la section Surveillance des requêtes, choisissez l'onglet Simultanéité des charges de travail.

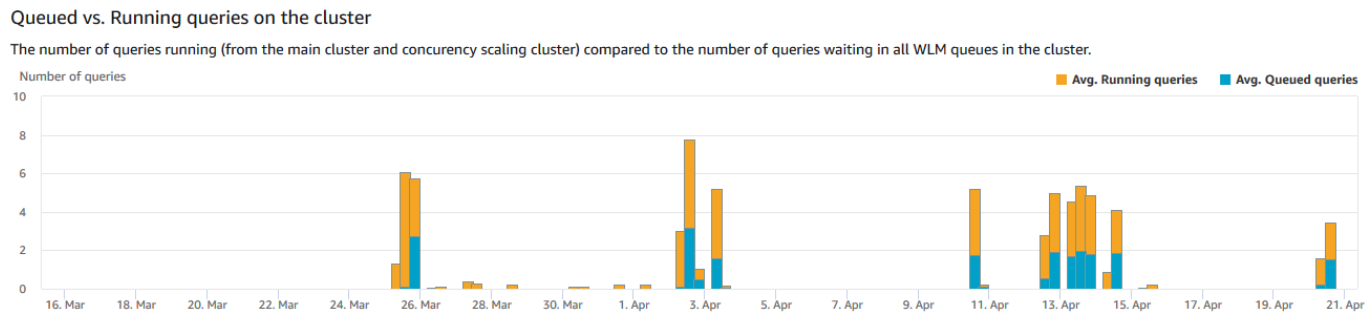
   L'onglet comprend les graphiques suivants :

   - Exécution de requêtes sur le cluster – Le nombre de requêtes en cours d'exécution (du cluster principal et du cluster de mise à l'échelle de la simultanéité) comparé au nombre de requêtes en attente dans toutes les files d'attente WLM du cluster.
   - Requêtes en cours d'exécution par file d'attente – Le nombre de requêtes en cours d'exécution (du cluster principal et du cluster de mise à l'échelle de la simultanéité) comparé au nombre de requêtes en attente dans chaque file d'attente WLM.
   - Activité de mise à l'échelle de la simultanéité – Le nombre de clusters de mise à l'échelle de la simultanéité qui traitent activement les requêtes.
   - Utilisation de la mise à l'échelle de la simultanéité – L'utilisation des clusters de mise à l'échelle de la simultanéité qui ont une activité de traitement des requêtes active.

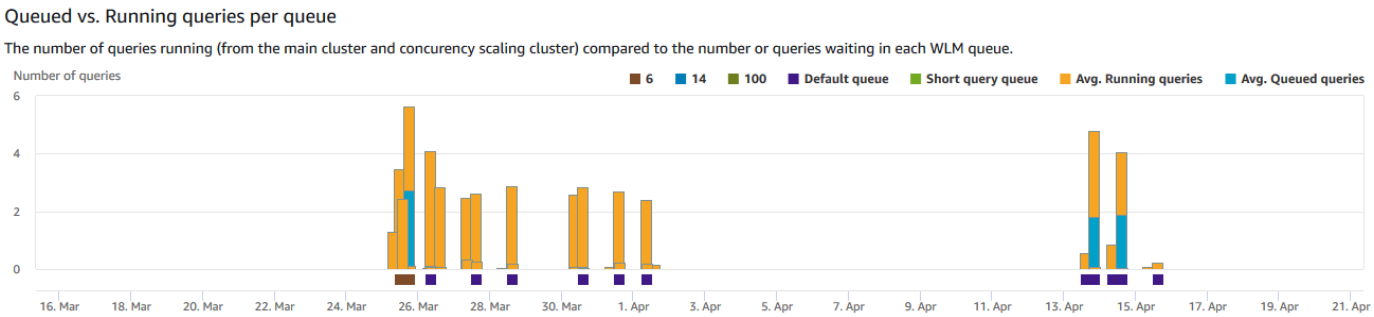
Graphiques de simultanéité des charges de travail

Les exemples suivants illustrent les graphiques qui s'affichent dans la nouvelle console Amazon Redshift. Pour créer des graphiques similaires dans Amazon CloudWatch, vous pouvez utiliser la mise à l'échelle de concurrence et les métriques WLM CloudWatch . Pour plus d'informations sur CloudWatch les statistiques d'Amazon Redshift, consultezDonnées de performances dans Amazon Redshift.

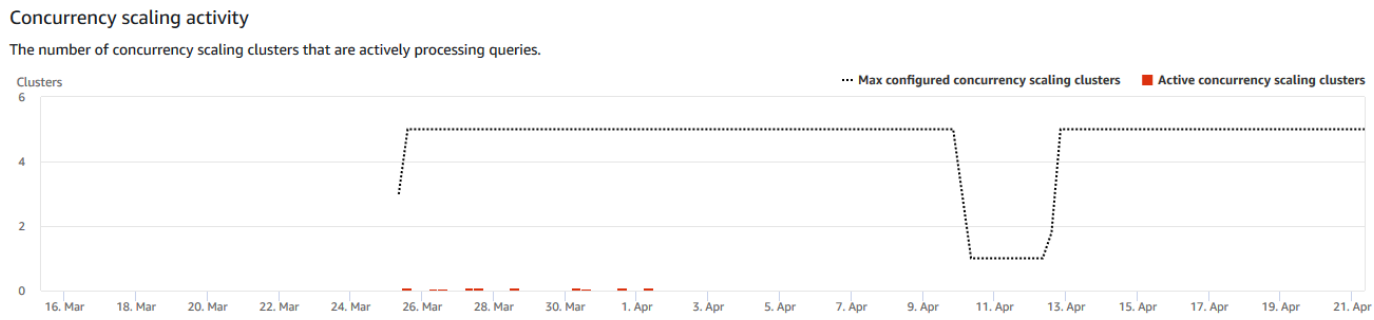
- Requêtes en attente ou en cours d'exécution sur le cluster



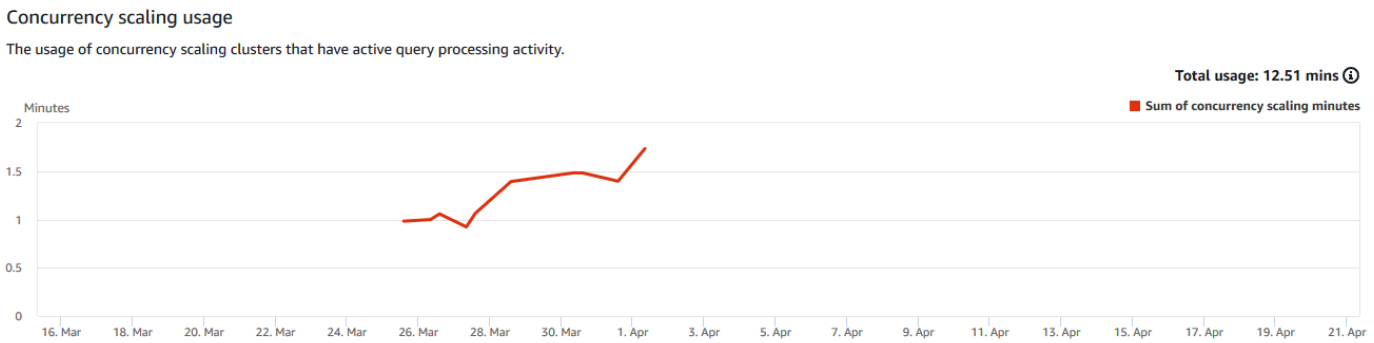
- Mise en file d'attente ou exécution de requêtes par file d'attente



- Activité de mise à l'échelle de simultanéité



- Utilisation de la mise à l'échelle de la simultanéité



Affichage des données d'optimisation automatique

La console Amazon Redshift fournit des informations sur les optimisations automatiques, ou autonomies, exécutées à l'aide de ressources de calcul supplémentaires. Vous pouvez utiliser ces informations pour suivre l'utilisation et vérifier si les limites d'utilisation ont été atteintes. Bien qu'Amazon Redshift ne vous facture pas les fonctionnalités autonomes exécutées sur le cluster provisionné lui-même, il vous facture les fonctionnalités autonomes exécutées à l'aide de ressources de calcul supplémentaires. Pour plus d'informations, consultez la section Allocation de ressources de calcul supplémentaires pour l'optimisation automatique des bases de données dans le manuel Amazon Redshift Database Developer Guide.

Pour afficher des données supplémentaires sur l'autonomie de calcul

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters, puis choisissez le nom d’un cluster dans la liste pour ouvrir ses détails.
3. Sur la page de détails du cluster, sélectionnez Gérer la limite d'utilisation dans le menu déroulant Actions. Vous pouvez également sélectionner l'onglet Maintenance pour un cluster, puis faire défiler la page vers le bas et sélectionner Créer des limites d'utilisation.
4. Le graphique présentant les données d'autonomie de calcul supplémentaires apparaît dans la section intitulée Limite d'utilisation pour le calcul supplémentaire à des fins d'optimisation automatique. Le graphique affiche la durée pendant laquelle Amazon Redshift exécute des fonctions autonomes en utilisant des ressources de calcul supplémentaires au cours d'une période donnée.

Affichage des requêtes et des charges

La console Amazon Redshift fournit des informations sur les requêtes et les chargements qui s’exécutent dans la base de données. Vous pouvez utiliser ces informations pour identifier et résoudre les requêtes qui nécessitent un temps de traitement long et créent des goulets d’étranglement, ce qui empêche que les autres requêtes soient traitées efficacement. Vous pouvez utiliser les informations sur les requêtes dans la console Amazon Redshift pour surveiller le traitement des requêtes.

Pour afficher les données de performance des requêtes

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Requêtes et charges pour afficher la liste des requêtes pour votre compte.

   Par défaut, la liste affiche les requêtes de tous vos clusters au cours des dernières 24 heures. Vous pouvez modifier la portée de la date affichée dans la console.

   > **Important**
   >
   > La liste Requêtes et chargements affiche les requêtes en cours d'exécution les plus longues du système et ce, jusqu'à 100 requêtes.

Affichage et analyse des détails des requêtes

Avec un identificateur de requête, vous pouvez afficher les détails d'une requête. Les détails peuvent inclure, par exemple, l'état d'achèvement de la requête, sa durée, l'instruction SQL et s'il s'agit d'une requête utilisateur ou d'une requête réécrite par Amazon Redshift. Une requête utilisateur est une requête qui est soumise à Amazon Redshift, à partir d'un client SQL ou générée par un outil de Business Intelligence. Amazon Redshift peut réécrire la requête pour l'optimiser, ce qui peut entraîner plusieurs requêtes réécrites. Bien que le processus soit effectué par Amazon Redshift, vous voyez les requêtes réécrites sur la page des détails de la requête avec la requête de l'utilisateur.

Pour afficher une requête

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Requêtes et charges pour afficher la liste des requêtes pour votre compte. Vous devrez peut-être modifier les paramètres de cette page pour rechercher votre requête.
3. Choisissez l'identifiant de Requête dans la liste pour afficher les Détails de la requête.

   La page Détails de requête inclut les onglets Détails de requête et Plan de requête avec des métriques sur la requête.

Les mesures incluent des détails sur une requête tels que l'heure de début, l'ID de requête, l'état et la durée. D'autres détails incluent si une requête s'est exécutée sur un cluster principal ou un cluster de mise à l'échelle concurrent, et s'il s'agit d'une requête parent ou réécrite.

Afficher les performances de cluster pendant l'exécution des requêtes

Vous pouvez surveiller les performances de vos clusters lors de l'exécution des requêtes afin d'identifier les goulots d'étranglement potentiels et d'optimiser l'exécution des requêtes. L'affichage des performances du cluster au fur et à mesure de l'exécution des requêtes fournit une vue en temps réel des indicateurs au niveau du système, tels que l'utilisation du processeur, le trafic disque I/O et réseau, ainsi que des détails au niveau des requêtes tels que le temps d'exécution, les données traitées et les étapes de la requête. Les procédures suivantes vous aident à accéder aux indicateurs de performance et à les interpréter afin de gérer et d'optimiser efficacement vos clusters alloués.

Pour afficher les performances de cluster pendant l'exécution des requêtes

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters, puis choisissez le nom du cluster dans la liste pour ouvrir ses détails. Les détails du cluster sont affichés, ce qui peut inclure les onglets Performance du cluster, Surveillance des requêtes, Bases de données, Unités de partage des données, Planifications, Maintenance et Propriétés.
3. Choisissez l'onglet Surveillance des requêtes pour plus de détails.

   Pour plus d'informations, consultez Affichage de l'historique des requêtes.

Affichage des métriques du cluster pendant les opérations de chargement

Lorsque vous affichez les performances du cluster pendant les opérations de chargement, vous pouvez identifier les requêtes qui consomment des ressources et prendre des mesures pour atténuer leur effet. Vous pouvez mettre fin à une charge si vous ne voulez pas qu'elle s'exécute jusqu'à la fin.

> **Note**
>
> La possibilité de mettre fin aux requêtes et aux charges dans Amazon Redshift requiert une autorisation spécifique. Si vous souhaitez que les utilisateurs puissent mettre fin aux requêtes et aux chargements, veillez à ajouter l'`redshift:CancelQuerySession`action à votre

politique Gestion des identités et des accès AWS (IAM). Cette exigence s'applique que vous sélectionniez la politique AWS gérée en lecture seule par Amazon Redshift ou que vous créiez une politique personnalisée dans IAM. Les utilisateurs qui ont la stratégie Amazon Redshift Full Access (Accès complet à Amazon Redshift) disposent déjà des autorisations nécessaires pour mettre fin aux requêtes et aux charges. Pour en savoir plus sur les actions dans les stratégies IAM pour Amazon Redshift, consultez Gestion de l'accès aux ressources.

Pour afficher les performances de cluster pendant les opérations de chargement

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters, puis choisissez le nom du cluster dans la liste pour ouvrir ses détails. Les détails du cluster sont affichés, ce qui peut inclure les onglets Performance du cluster, Surveillance des requêtes, Bases de données, Unités de partage des données, Planifications, Maintenance et Propriétés.
3. Choisissez l'onglet Surveillance des requêtes pour plus de détails.
4. Dans la section Requêtes et chargements, choisissez Chargements pour afficher les opérations de chargement d'un cluster. Si un chargement est en cours d'exécution, vous pouvez l'arrêter en choisissant Arrêter une requête.

Affichage du graphe de répartition de l'exécution de la charge de travail sur le cluster

Vous pouvez obtenir une vue détaillée des performances de votre charge de travail en consultant le graphique de répartition de l'exécution de la charge de travail dans la console. Nous construisons le graphique à partir des données fournies par la QueryRuntimeBreakdown métrique. Avec ce graphique, vous pouvez voir combien de temps vos requêtes ont consacré aux différentes étapes du traitement, comme l'attente et la planification.

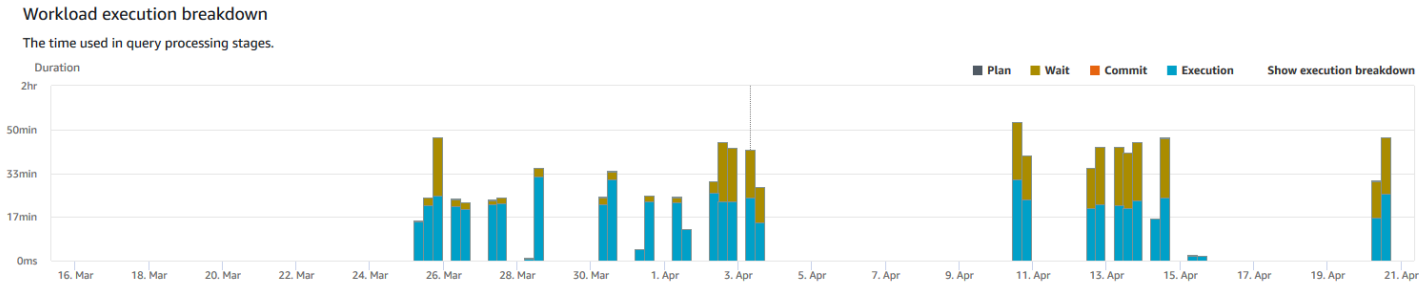
> **Note**
>
> Le graphique de répartition de l'exécution de la charge de travail n'est pas affiché pour les clusters à nœud unique.

La liste de métriques suivante décrit les caractéristiques les différentes étapes du traitement :

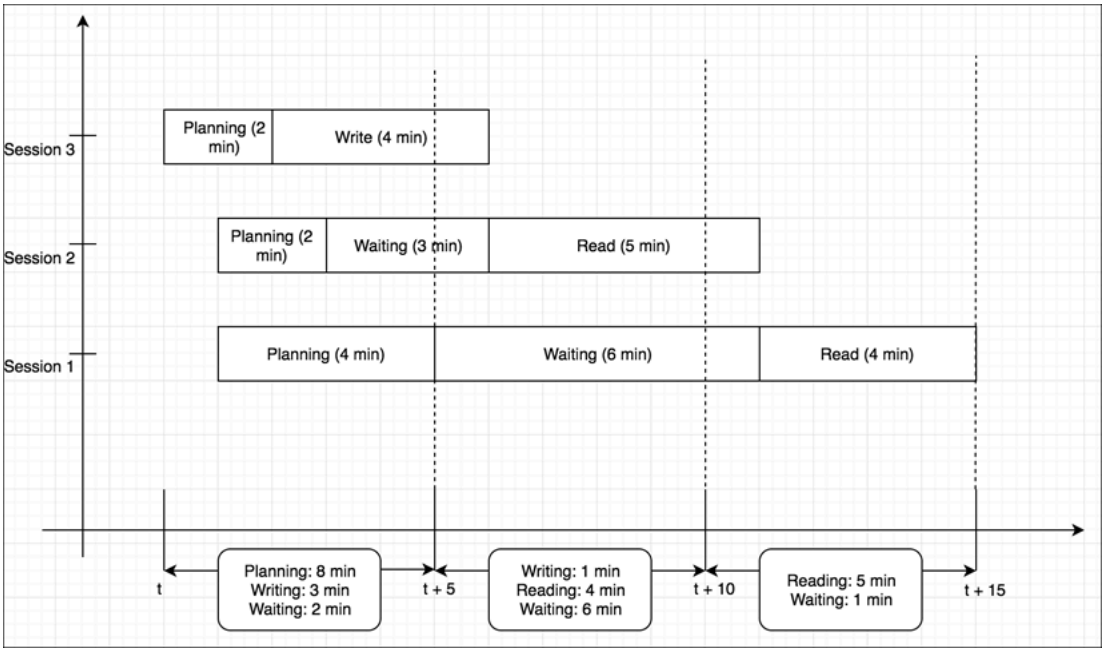
- `QueryPlanning` : Temps passé à analyser et à optimiser les instructions SQL.
- `QueryWaiting` : Temps passé dans la file d'attente de gestion de la charge de travail (WLM).
- `QueryExecutingRead` : Temps passé à exécuter des requêtes en lecture.
- `QueryExecutingInsert` : Temps passé à exécuter des requêtes d'insertion.
- `QueryExecutingDelete` : Temps passé à exécuter des requêtes de suppression.
- `QueryExecutingUpdate` : Temps passé à exécuter des requêtes de mise à jour.
- `QueryExecutingCtas` : Temps passé à exécuter des requêtes CREATE TABLE AS.
- `QueryExecutingUnload` : Temps passé à exécuter des requêtes en de déchargement.
- `QueryExecutingCopy` : Temps passé à exécuter des requêtes de copie.

Par exemple, le graphique suivant dans la console Amazon Redshift présente le temps que les requêtes ont passé dans les étapes de planification, d'attente, de lecture et d'écriture. Vous pouvez combiner les résultats de ce graphique avec d'autres métriques pour une analyse plus approfondie. Dans certains cas, votre graphique peut montrer que les requêtes de courte durée (comme mesuré par la métrique `QueryDuration`) passent beaucoup de temps à l'état d'attente. Vous pouvez alors augmenter le taux de simultanéité WLM d'une file d'attente particulière pour accroître le débit.

Voici un exemple du graphique de répartition de l'exécution de la charge de travail. Dans le graphique, la valeur de l'axe des y correspond à la durée moyenne de chaque étape à l'heure spécifiée affichée sous la forme d'un graphique à barres empilées.



Le diagramme suivant montre comment Amazon Redshift regroupe le traitement des requêtes pour les sessions simultanées.



Pour afficher du graphe de répartition de l'exécution de la charge de travail sur le cluster

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters, puis choisissez le nom du cluster dans la liste pour ouvrir ses détails. Les détails du cluster sont affichés, ce qui peut inclure les onglets Performance du cluster, Surveillance des requêtes, Bases de données, Unités de partage des données, Planifications, Maintenance et Propriétés.
3. Choisissez l'onglet Surveillance des requêtes pour connaître les métriques relatives à vos requêtes.
4. Dans la section Surveillance des requêtes, choisissez Performances de base de données, puis Métriques de cluster.

   Les métriques suivantes sont indiquées sur le graphique pour une période de temps sous forme de diagramme à barres :

   - Durée de Plan
   - Durée d'Attente
   - Heure de validation
   - Durée d'exécution

Analyse de l’exécution des requêtes

Vous pouvez analyser les détails d’exécution d’une requête pour comprendre ses performances et identifier les domaines potentiels d’optimisation. L’analyse d’une requête fournit un aperçu du plan de requête, notamment des étapes impliquées, du temps nécessaire à chaque étape et de la quantité de données traitées. Les cas d’utilisation courants incluent le dépannage des requêtes lentes, l’optimisation des stratégies de distribution des données et l’identification des opportunités de réécriture ou d’indexation des requêtes.

Pour analyser une requête

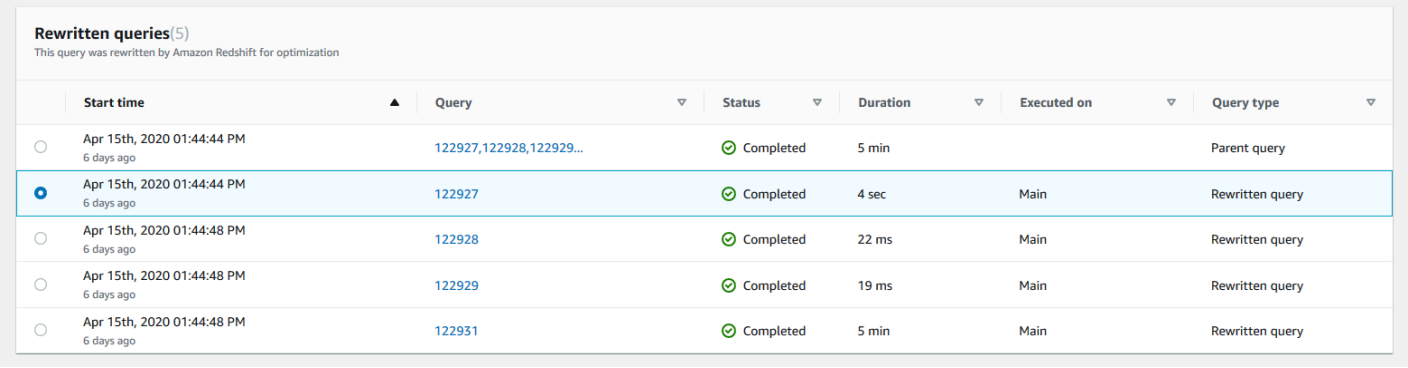
1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Requêtes et charges pour afficher la liste des requêtes pour votre compte. Vous devrez peut-être modifier les paramètres de cette page pour rechercher votre requête.
3. Choisissez l’identifiant de Requête dans la liste pour afficher les Détails de la requête.

   La page Détails de requête inclut les onglets Détails de requête et Plan de requête avec des métriques sur la requête.

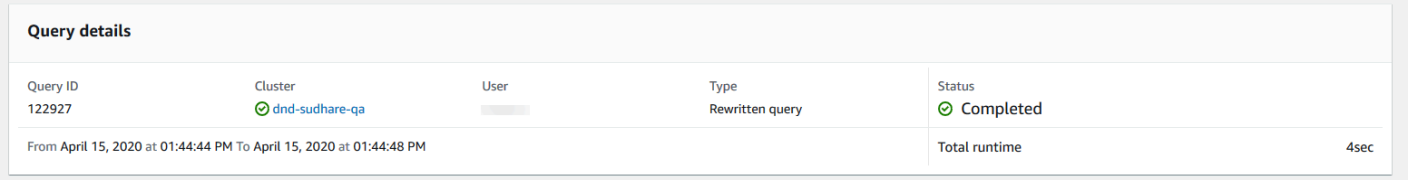
   > **Note**
   >
   > Vous pouvez également accéder à la page de Détails d’une requête à partir de la page de Détails d’un cluster, onglet Historique des requêtes, lorsque vous effectuez une analyse descendante d’une requête dans un graphique de Temps d’exécution des requêtes.

La page Détails de la requête contient les sections suivantes :

- Une liste de requêtes réécrites, comme illustré dans la capture d’écran suivante.



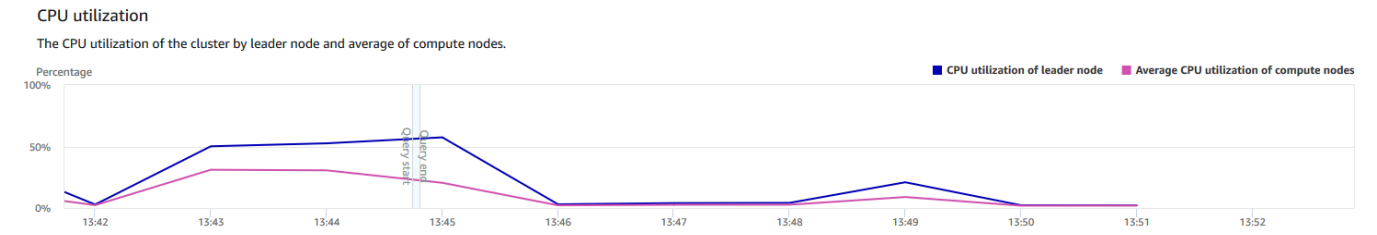
- Une section Détails de la requête comme illustré dans la capture d'écran suivante.



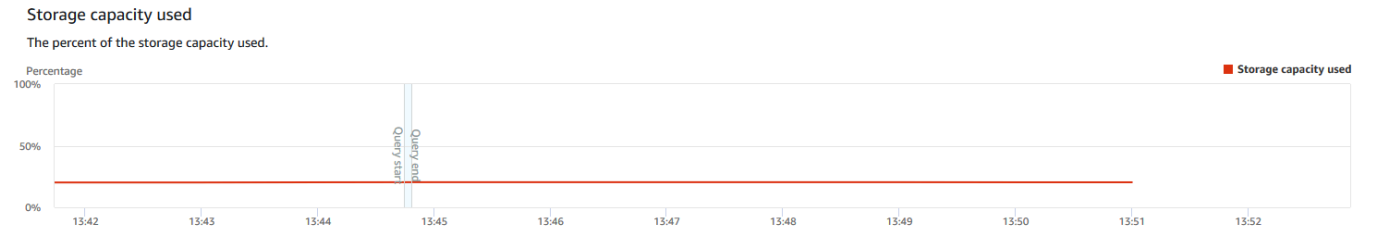
- Un onglet Détails de la requête qui contient le SQL exécuté et les détails d'exécution.
- Un onglet Plan de requête qui contient les étapes du Plan de requête et d'autres informations sur le plan de requête. Ce tableau contient également des graphiques sur le cluster lors de l'exécution de la requête.
  - État d'intégrité du cluster



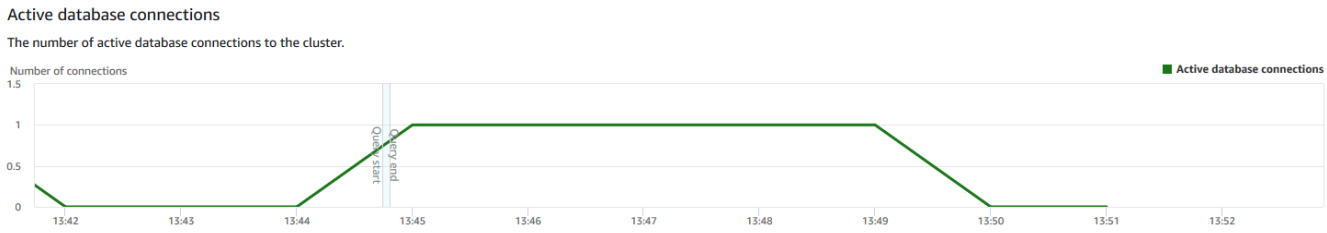
  - Utilisation de l'UC



  - Capacité de stockage utilisée



- Connexions actives à la base de données



Création d'une alarme

Les alarmes que vous créez dans la console Amazon Redshift sont des CloudWatch alarmes. Elles sont utiles, car elles vous aident à prendre des décisions proactives sur votre cluster et une instance sans serveur. Vous pouvez définir une ou plusieurs alarmes sur les métriques répertoriées dans Données de performances dans Amazon Redshift. Par exemple, définir une alarme pour une valeur élevée de `CPUUtilization` sur un nœud de cluster aide à indiquer quand le nœud est surutilisé. Une alarme indiquant un `DataStorage` élevé permet de suivre l'espace de stockage que votre espace de noms sans serveur utilise pour vos données.

Depuis Actions, vous pouvez modifier ou supprimer des alarmes. Vous pouvez également créer une alerte Chime ou Slack pour envoyer une alerte à Slack ou Amazon Chime en spécifiant une URL de webhook Slack ou Amazon Chime. CloudWatch

Dans cette section, vous trouverez comment créer une alarme à l'aide de la console Amazon Redshift. Vous pouvez créer une alarme à l'aide de la CloudWatch console ou de toute autre manière de travailler avec les métriques, par exemple à l'aide du SDK AWS CLI ou d'un AWS SDK.

Pour créer une CloudWatch alarme à l'aide de la console Amazon Redshift

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.

   Si vous utilisez Amazon Redshift sans serveur, choisissez Go to Serverless (Accéder à sans serveur) en haut à droite du tableau de bord.
2. Dans le menu de navigation, choisissez Alarmes, puis choisissez Créer une alarme.
3. Sur la page Créer une alarme, entrez les propriétés pour créer une CloudWatch alarme.
4. Sélectionnez Créer une alerte.

Arrêt d’une requête en cours d’exécution

Vous pouvez également utiliser l’onglet Requêtes pour mettre fin à une requête en cours.

> **Note**
>
> La possibilité de mettre fin aux requêtes et aux charges dans Amazon Redshift requiert une autorisation spécifique. Si vous souhaitez que les utilisateurs puissent mettre fin aux requêtes et aux chargements, veillez à ajouter l'`redshift:CancelQuerySession`action à votre politique Gestion des identités et des accès AWS (IAM). Cette exigence s'applique que vous sélectionniez la politique AWS gérée Amazon Redshift en lecture seule ou que vous créiez une politique personnalisée dans IAM. Les utilisateurs qui ont la stratégie Amazon Redshift Full Access (Accès complet à Amazon Redshift) disposent déjà des autorisations nécessaires pour mettre fin aux requêtes et aux charges. Pour en savoir plus sur les actions dans les stratégies IAM pour Amazon Redshift, consultez Gestion de l’accès aux ressources.

Pour arrêter une requête en cours d’exécution

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez REQUÊTES, puis choisissez Requêtes et chargements pour afficher la liste des requêtes pour votre compte.
3. Choisissez dans la liste la requête en cours d’exécution qui doit être arrêtée, puis choisissez Arrêter la requête.

Statistiques de performance dans la CloudWatch console

Lorsque vous utilisez les métriques Amazon Redshift dans la CloudWatch console, gardez quelques points à l'esprit :

- Les données relatives aux performances des requêtes et des chargements sont uniquement disponibles dans la console Amazon Redshift.
- Certaines métriques du CloudWatch ont des unités différentes de celles utilisées dans la console Amazon Redshift. Par exemple, `WriteThroughput` est affiché dans GB/s (par rapport à Bytes/s dans CloudWatch), qui est une unité plus pertinente pour l'espace de stockage typique d'un nœud.

Lorsque vous utilisez des métriques Amazon Redshift dans la CloudWatch console, dans les outils de ligne de commande ou dans un SDK Amazon, gardez ces concepts à l'esprit :

1. Tout d'abord, spécifiez la dimension de métrique à utiliser. Une dimension est une paire nom-valeur qui vous aide à identifier une métrique de façon unique. Les dimensions d'Amazon Redshift sont `ClusterIdentifier` et `NodeID`. Dans la CloudWatch console, les `Redshift Node` vues `Redshift Cluster` et sont fournies pour sélectionner facilement les dimensions spécifiques au cluster et au nœud. Pour en savoir plus sur les dimensions, consultez Dimensions dans le Guide du développeur CloudWatch .
2. Ensuite, spécifiez le nom de la métrique, par exemple `ReadIOPS`.

Le tableau suivant résume les types de dimensions métriques Amazon Redshift qui sont à votre disposition. Selon la métrique, les données sont disponibles gratuitement par intervalles d'1 minute ou de 5 minutes. Pour de plus amples informations, veuillez consulter Métriques Amazon Redshift.

CloudWatch espace de noms	Dimension	Description
`AWS/Redshift`	`NodeID`	Filtre les données demandées qui sont spécifiques aux nœuds d'un cluster. `NodeID`Dest soit « Leader », soit « Shared », soit Compute-N « » où N est égal à 0, 1,... pour le nombre de nœuds du cluster. « Shared » signifie que le cluster a un seul nœud, c'est-à-dire le nœud principal, et que les nœuds de calcul sont associés.
`AWS/Redshift`	`ClusterIdentifier`	Les filtres ont demandé des données spécifiques au cluster. Les métriques spécifiques aux clusters incluent `HealthStatus` , `MaintenanceMode` et `DatabaseConnections` . Les métriques générales de cette dimension (par exemple `ReadIOPS`) qui sont également des métriques de nœuds représentent une agrégation des données des métriques de nœud. Veillez à interpréter ces métriques parce qu'elles regroupent un comportement de nœud principal et de nœuds de calcul.

L'utilisation des métriques de passerelle et de volume est similaire à l'utilisation des autres métriques de service. La plupart des tâches courantes sont décrites dans la CloudWatch documentation, notamment les suivantes :

- Affichage des métriques disponibles
- Obtention des statistiques d'une métrique
- Création d'alarmes CloudWatch

Profileur de requêtes

Ce document décrit le profileur de requêtes, un outil graphique permettant d'analyser les composants et les performances d'une requête.

Le profileur de requêtes est une fonctionnalité de surveillance et de dépannage des requêtes que vous pouvez afficher via la console Amazon Redshift. Il est utile pour analyser les performances des requêtes. Son objectif principal est d'afficher un ordre d'exécution visuel et graphique, un plan d'exécution et des statistiques concernant une requête, afin de faciliter sa compréhension et son dépannage. Le profileur de requêtes vous aide à analyser les types de composants de requête suivants :

- Requêtes enfants : une requête enfant est une partie du travail qui découle d'une requête. Amazon Redshift peut diviser une requête en plusieurs requêtes enfants si le traitement de plusieurs petites requêtes est plus efficace que celui d'une seule grande requête. Dans le profileur, vous pouvez voir les propriétés de chaque requête enfant. Une requête enfant est composée de flux et de sous-composants supplémentaires.

  Les types de requêtes enfants affichés par le profileur de requêtes sont généralement les suivants :

  - Requête de table temporaire : le texte de cette requête enfant commence par la commande `CREATE TEMP TABLE`. Cette requête enfant crée des tables temporaires que d'autres requêtes enfants peuvent traiter.
  - Requête de statistiques : le profileur de requêtes ajoute le commentaire suivant au début de cette requête enfant pour aider à l'identifier :

    ```
    -- collect statistics of child query queryID
    ```

    Cette requête enfant collecte des informations que le moteur de requêtes Amazon Redshift utilise pour optimiser les performances.

> **Note**
>
> Le profileur de requêtes affiche la requête fournie par l'utilisateur comme dernière requête enfant exécutée par Amazon Redshift.

- Flux : un flux est un ensemble de segments répartis sur une tranche de nœuds de calcul disponible Chaque requête enfant est composée d'un ou de plusieurs segments. Dans le profileur de requêtes, vous pouvez voir les propriétés de chaque flux, telles que son temps d'exécution. En parcourant la liste des flux, il est probable que vous puissiez rapidement détecter les problèmes de performance.
- Segments : un segment est une combinaison de plusieurs étapes qu'un seul processus peut exécuter. Un segment est également la plus petite unité de compilation exécutable par une tranche de nœuds de calcul. Une tranche est l'unité de traitement parallèle dans Amazon Redshift. Les segments d'un flux s'exécutent en parallèle. Le profileur de requêtes n'affiche pas les segments graphiquement, mais vous pouvez accéder aux informations des segments pour une étape dans le volet de détails de cette étape.
- Étapes : chaque segment est composé d'un ensemble d'étapes. Une étape est un élément d'une requête. Les étapes peuvent inclure une étape hashjoin, par exemple, ou un scan, qui consiste à lire les enregistrements d'une table.

Pour plus d'informations sur les flux, les segments et les étapes, consultez Flux de travail de planification et d'exécution des requêtes dans le Guide de développeur de base de données Amazon Redshift.

Le profileur de requêtes affiche les informations renvoyées par les vues `SYS_QUERY_HISTORY`, `SYS_QUERY_DETAIL`, `SYS_QUERY_EXPLAIN` et `SYS_CHILD_QUERY_TEXT`. Pour plus d'informations sur ces vues, consultez SYS_QUERY_HISTORY, SYS_QUERY_DETAIL, SYS_QUERY_EXPLAIN, and SYS_CHILD_QUERY_TEXT dans le Guide du développeur de base de données Amazon Redshift.

Le profileur de requêtes affiche uniquement les informations relatives aux requêtes récemment exécutées sur la base de données. Une requête qui se termine en utilisant des données de cache préremplies plutôt que d'être exécutée sur la base de données n'aura pas de profil de requête si aucune information n'était disponible auparavant pour cette requête. C'est parce qu'Amazon Redshift ne génère pas de plan de requête pour cette requête.

Prérequis pour l’utilisation du profileur de requêtes

Conçues pour être faciles à utiliser et réduire la complexité, les vues de surveillance SYS fournissent une gamme complète de métriques pour une surveillance et un dépannage efficaces. Les vues de surveillance SYS garantissent également l’historique des requêtes des sept derniers jours, quelle que soit la taille ou l’activité du cluster. Les utilisateurs n’ont de visibilité que pour les requêtes qu’ils ont exécutées, tandis que les super-utilisateurs ont une visibilité sur les requêtes de tous les utilisateurs.

Votre compte ou rôle d’utilisateur IAM a besoin d’autorisations pour accéder à la section Surveillance des requêtes et des bases de données de la console. Cette section décrit comment accorder des autorisations à un compte ou un rôle utilisateur

Utilisez la politique suivante pour ajouter des autorisations minimales à votre compte ou rôle d’utilisateur IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "redshift:DescribeClusters",
                "redshift-serverless:ListNamespaces",
                "redshift-serverless:ListWorkgroups",
                "redshift-data:ExecuteStatement",
                "redshift-data:DescribeStatement",
                "redshift-data:GetStatementResult"
            ],
            "Resource": [
                "arn:aws:redshift-serverless:us-east-1:111122223333:*",
                "arn:aws:redshift:us-east-1:111122223333:*"
            ]
        }
    ]
}
```

Rubriques

- Octroi d’autorisations de surveillance des requêtes à un rôle
- Octroi d’autorisations de surveillance des requêtes à un utilisateur
- Informations d’identification temporaires utilisant votre identité IAM

Octroi d’autorisations de surveillance des requêtes à un rôle

Les utilisateurs dotés d’un rôle avec l’autorisation `sys:monitor` peuvent consulter toutes les requêtes. Les utilisateurs dotés d’un rôle avec l’autorisation `sys:operator` peuvent annuler des requêtes, analyser l’historique des requêtes et effectuer des opérations de nettoyage.

Pour accorder une autorisation de surveillance des requêtes à un rôle

1. Utilisez la commande suivante pour fournir un accès au moniteur système, où *role-name* est le nom du rôle pour lequel vous souhaitez fournir l'accès.

```
grant role sys:monitor to "IAMR:role-name";
```

2. (Facultatif) Utilisez la commande suivante pour fournir l'accès à l'opérateur système, où *role-name* est le nom du rôle pour lequel vous souhaitez fournir l'accès.

```
grant role sys:operator to "IAMR:role-name";
```

Octroi d’autorisations de surveillance des requêtes à un utilisateur

Les utilisateurs avec l’autorisation `sys:monitor` peuvent afficher toutes les requêtes. Les utilisateurs avec l’autorisation `sys:operator` peuvent annuler des requêtes, analyser l’historique des requêtes et effectuer des opérations de vide.

Pour accorder une autorisation de surveillance des requêtes à un utilisateur

1. Utilisez la commande suivante pour fournir un accès au moniteur système, où *user-name* est le nom de l'utilisateur auquel vous souhaitez fournir l'accès.

```
grant role sys:monitor to "IAMR:user-name";
```

2. (Facultatif) Utilisez la commande suivante pour fournir l'accès à l'opérateur système, où *-name* est le nom de l'utilisateur auquel vous souhaitez fournir l'accès.

```
grant role sys:operator to "IAMR:user-name";
```

Informations d'identification temporaires utilisant votre identité IAM

Cette option est disponible uniquement lors de la connexion à un cluster. Avec cette méthode, le profileur de requêtes mappe un nom d'utilisateur à votre identité IAM et génère un mot de passe temporaire pour se connecter à la base de données sous votre identité IAM. Un utilisateur utilisant cette méthode pour se connecter doit disposer de l'autorisation IAM pour `redshift:GetClusterCredentialsWithIAM`. Pour empêcher les utilisateurs d'utiliser cette méthode, modifiez leur rôle ou utilisateur IAM afin de refuser cette autorisation.

Accès au profileur de requêtes dans la console Amazon Redshift pour l'analyse d'une requête

Vous pouvez accéder au profileur de requêtes pour Amazon Redshift sans serveur ou Amazon Redshift alloué. Consultez les sections suivantes pour obtenir des détails :

Rubriques

- Accès au profileur de requêtes dans la console Amazon Redshift pour Amazon Redshift sans serveur
- Accès au profileur de requêtes dans la console Amazon Redshift pour Amazon Redshift alloué

Accès au profileur de requêtes dans la console Amazon Redshift pour Amazon Redshift sans serveur

Pour accéder au profileur de requêtes pour Amazon Redshift sans serveur, procédez comme suit :

- Ouvrez la console Amazon Redshift sans serveur.
- Dans le volet de navigation, sous Surveillance, sélectionnez Surveillance des requêtes et des bases de données.
- Choisissez un groupe de travail.
- Choisissez Requêtes et surveillance des bases de données.
- Choisissez une requête.
- Choisissez l'onglet Plan de requête sur la page Détails de la requête.

Si un plan de requêtes est disponible, vous verrez une liste de requêtes secondaires. Choisissez une requête pour l'afficher dans le profileur de requêtes.

Accès au profileur de requêtes dans la console Amazon Redshift pour Amazon Redshift alloué

Pour accéder au profileur de requêtes pour Amazon Redshift alloué, procédez comme suit :

- Ouvrez le Tableau de bord des clusters alloués. Amazon Redshift
- Choisissez un cluster.
- Choisissez Query monitoring (Surveillance des requêtes).
- Connectez-vous à une base de données.
- Choisissez Requêtes et surveillance des bases de données.
- Choisissez une requête.

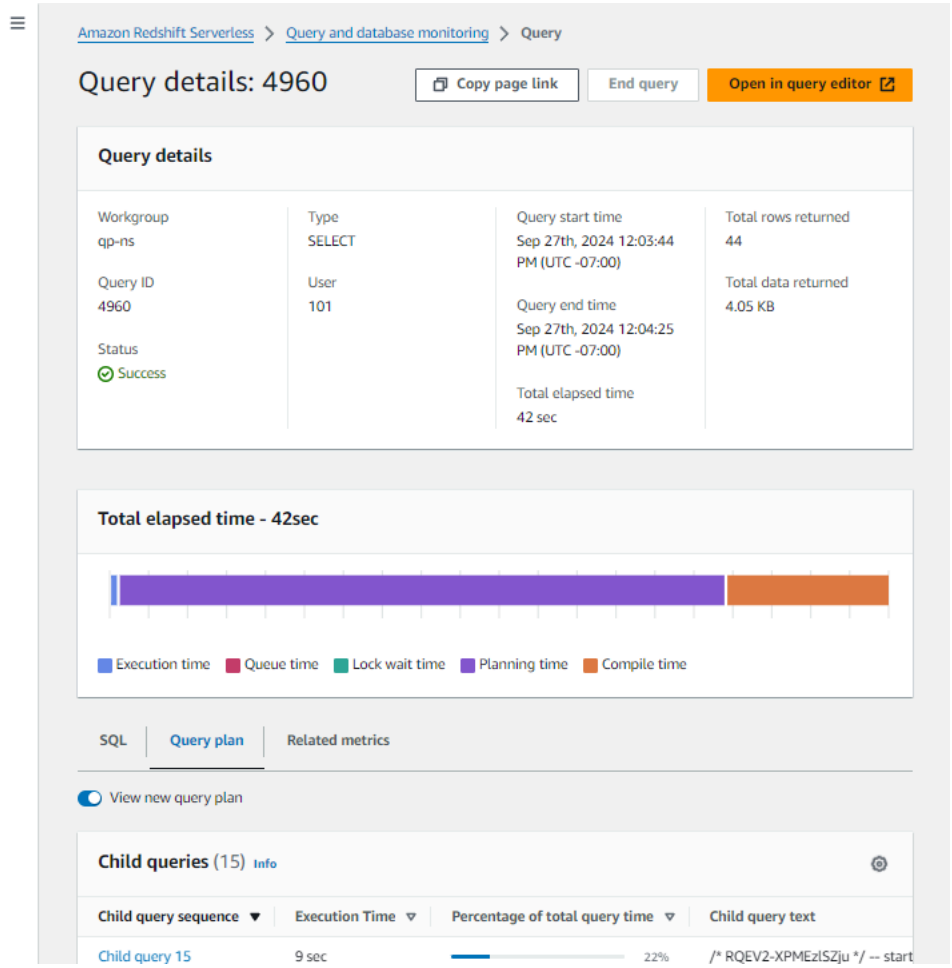
Si un plan de requêtes est disponible, vous verrez une liste de requêtes secondaires. Choisissez une requête pour l'afficher dans le profileur de requêtes.

Interface utilisateur du profileur de requêtes

Le profileur de requêtes utilise les pages suivantes pour afficher les informations relatives à votre requête :

- Page des détails de la requête : cette page affiche les statistiques et les requêtes secondaires relatives à votre requête.
- Page de requête enfant : cette page affiche les statistiques, les flux et une représentation visuelle du plan d'exécution d'une requête enfant. La console affiche cette page lorsque vous choisissez une requête enfant dans la liste des Requêtes enfants de la page Surveillance des requêtes et des bases de données.

Page des détails de la requête



La page Détails de la requête comprend les éléments suivants :

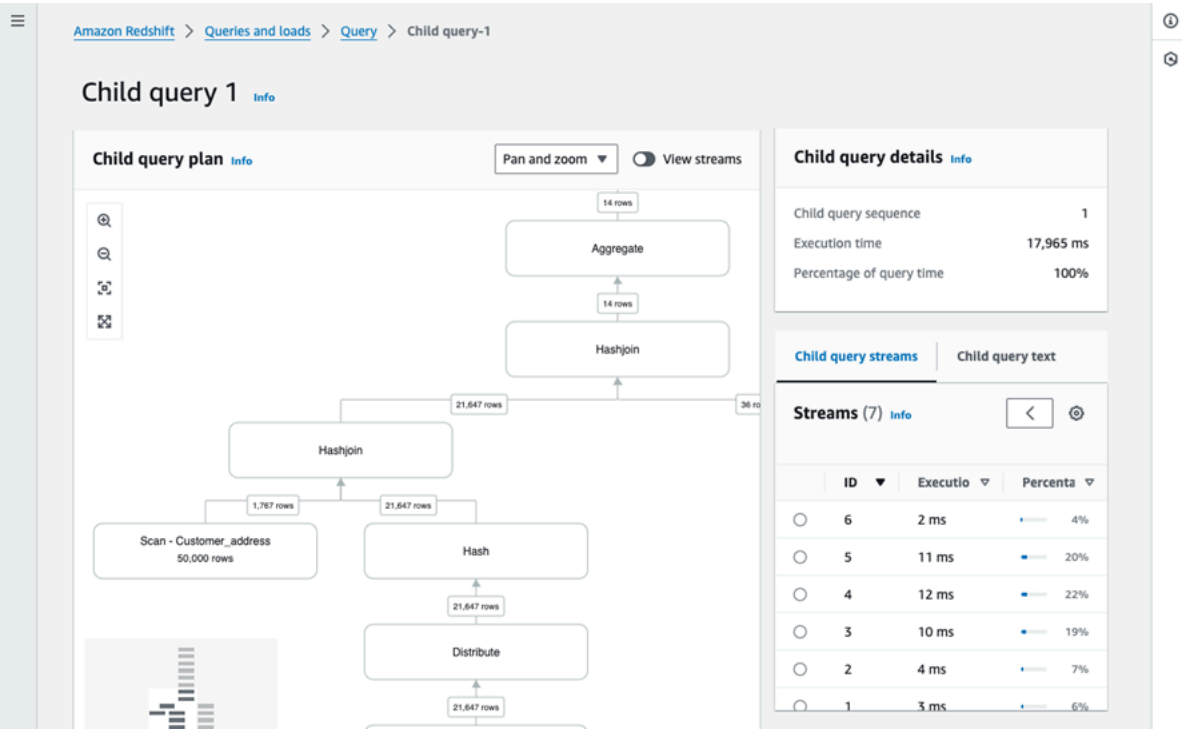
- Volet supérieur : le volet situé en haut de la page affiche les détails de la requête, tels que son statut et son type. Pour plus d'informations sur la source des informations affichées dans le volet supérieur, consultez SYS_QUERY_HISTORY dans le Guide du développeur de base de données Amazon Redshift.
- Onglet SQL : cet onglet du panneau inférieur affiche le texte SQL de la requête utilisateur d'origine.
- Onglet Plan de la requête : cet onglet du panneau inférieur affiche la liste des requêtes enfants qu'Amazon Redshift utilise pour préparer les données et les statistiques pour la requête de l'utilisateur. Par défaut, la liste Requêtes enfants affiche des informations et des statistiques agrégées sur chaque requête enfant. Pour plus d'informations sur la source des informations affichées sur cette page, consultez SYS_QUERY_DETAIL dans le Guide du développeur de base de données Amazon Redshift.

Vous pouvez ajouter ou supprimer des colonnes de la liste Requêtes enfants à l'aide du menu Préférences.

- Mesures associées — Cet onglet du panneau inférieur affiche les CloudWatch mesures suivantes pour la requête :
  - Capacité RPU utilisée (pour les groupes de travail sans serveur) : capacité de calcul utilisée par la requête, mesurée en unités de traitement Redshift (RPU). Pour plus d'informations, consultez Capacité de calcul pour Amazon Redshift sans serveur.
  - État de santé du cluster, utilisation du processeur, capacité de stockage utilisée (pour les clusters alloués) : état et ressources système utilisées par la requête.
  - Connexions de base de données actives : métrique `DatabaseConnections` de la requête.

  Pour plus d'informations sur CloudWatch les métriques, consultezDonnées de performances dans Amazon Redshift.

Page de requête enfant



La page Requête enfant comprend les éléments suivants :

- Liste déroulante des requêtes enfants : ce contrôle indique le nom de la séquence et le temps d'exécution de chaque requête enfant. Vous pouvez accéder à d'autres requêtes enfants en les sélectionnant dans ce contrôle.
- Panneau latéral : ce panneau contient des onglets permettant d'afficher les flux de requêtes enfants et le texte de la requête enfant.
- Onglet Flux de la requête enfant : cet onglet du panneau supérieur affiche les éléments suivants :
  - Flux : ce volet affiche la liste des flux contenus dans la requête enfant. Ce volet affiche des informations et des données agrégées sur les flux utilisés par Amazon Redshift pour optimiser la requête. Pour plus d'informations sur les détails de ce volet, consultez SYS_QUERY_DETAIL dans le Guide du développeur de base de données Amazon Redshift.

    Vous pouvez ajouter ou supprimer des colonnes dans le volet Flux à l'aide du menu Préférences. Vous accédez au menu Préférences à l'aide de l'icône en forme de roue dentée dans le volet Flux.
  - Volet de requête enfant : représentation graphique des étapes de la requête enfant. Pour plus d'informations sur le volet de Requête enfant, consultez Volet de requête enfant ci-après.
- Onglet de texte de la requête enfant : cet onglet du panneau supérieur affiche le code SQL de la requête enfant.
- Volet des détails de la requête enfant : ce volet situé dans le panneau de droite affiche les détails de la requête enfant. Pour plus d'informations sur les détails de ce volet, consultez SYS_QUERY_DETAIL dans le Guide du développeur de base de données Amazon Redshift.
- Volet des détails du flux : lorsque vous choisissez un flux dans le volet Flux, le volet Détails du flux affiche des informations sur le flux. Pour plus d'informations sur les détails de ce volet, consultez SYS_QUERY_DETAIL dans le Guide du développeur de base de données Amazon Redshift.
- Volet des détails de l'étape : lorsque vous choisissez une étape dans le volet Flux ou dans le graphe du Plan de Requête enfant, le volet Détails de l'étape affiche des informations sur l'étape. Pour plus d'informations sur les détails de ce volet, consultez SYS_QUERY_DETAIL dans le Guide du développeur de base de données Amazon Redshift.

Volet de requête enfant

Le profileur de requêtes affiche la requête enfant dans le volet Requête enfant sous forme de représentation graphique des étapes de la requête enfant sélectionnée.

Le volet Requête enfant affiche l'ordre d'exécution et les relations entre les étapes. Par exemple, si une étape joint le résultat de deux autres étapes, le volet Requête enfant affiche l'étape sous la forme d'un nœud arborescent alimenté par deux nœuds :



Le volet Requête enfant n'affiche pas les flux contenant les étapes par défaut. Pour afficher les flux utilisés par Amazon Redshift pour partitionner logiquement les étapes de la requête enfant, choisissez Afficher les flux. Lorsque vous choisissez Afficher les flux, le volet de Requête enfant affiche les étapes contenues dans les flux de la requête.

Le volet Requête enfant n'affiche pas d'informations sur les segments. Pour voir le segment correspondant à une étape, sélectionnez l'étape. Le volet Détails de l'étape affiche ensuite le segment correspondant à l'étape.

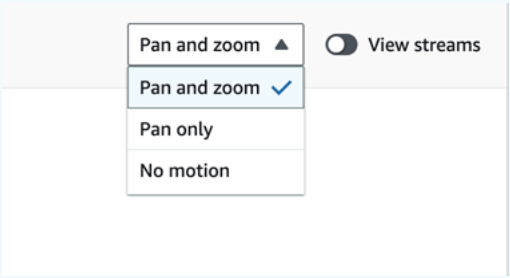
Navigation dans le volet Requête enfant

Dans le volet Requête enfant, vous pouvez choisir les étapes à suivre pour obtenir des informations détaillées les concernant. Vous pouvez également déplacer et zoomer sur l'espace de travail pour mieux visualiser les étapes de votre plan de requête.

Vous pouvez choisir des nœuds, déplacer et zoomer dans le volet Requête enfant en utilisant les méthodes suivantes :

- À l'aide de la souris : vous pouvez choisir des nœuds, cliquer et faire glisser l'espace de travail pour le déplacer, et maintenir **`Ctrl`** (Windows) ou **`CMD`** (Mac) et appuyer sur la molette de la souris pour zoomer. Le choix d'un nœud entraîne le zoom et le panoramique de l'espace de travail pour mettre en évidence ce nœud. Si vous choisissez un flux dans l'espace de travail, ce flux est surligné dans la liste des Flux. Si vous choisissez une étape dans l'espace de travail, le volet Détails de l'étape affiche les informations relatives à cette étape.
- Utilisation des commandes de zoom et d'ajustement situées dans le coin supérieur gauche de l'espace de travail : ces commandes vous permettent de zoomer en avant, de dézoomer, de zoomer sur l'ensemble de l'espace de travail et de passer en mode plein écran. Lorsque vous zoomez pour l'adapter à l'ensemble du plan de requête, l'espace de travail centre le plan de requête à la fois horizontalement et verticalement.

- Utilisation de la mini-carte dans le coin inférieur droit de l'espace de travail : vous pouvez déplacer ou zoomer sur l'espace de travail à l'aide de la commande de minicarte située dans le coin inférieur gauche de l'espace de travail.
- Choix d'un flux dans le volet Flux : si vous choisissez un flux dans le volet Flux, l'espace de travail se déplace et zoome pour afficher le flux sélectionné, et affiche des informations sur le flux dans le volet Détails du flux.
- Choix d'une étape dans le volet Détails du flux : si vous choisissez une étape dans le volet Détails du flux, l'espace de travail se déplace et zoome pour afficher l'étape sélectionnée, et affiche des informations sur l'étape dans le volet Détails de l'étape.

> **Note**
>
> Lorsque vous choisissez une étape, que ce soit dans l'espace de travail ou dans un autre volet, l'espace de travail tente de zoomer et de se déplacer de manière à ce que l'étape sélectionnée soit mieux visible.
> Lorsque vous choisissez un flux ou une étape dans l'espace de travail ou dans un autre volet, l'espace de travail ne zoome et se déplace sur ce flux ou cette étape que si vous avez sélectionné Panoramique et zoom dans le contrôle supérieur droit de l'espace de travail. Vous pouvez limiter ce comportement au panoramique et au zoom, au panoramique uniquement ou à l'absence de mouvement en choisissant le réglage approprié dans le menu déroulant.
>
> 
>

Résolution des problèmes de requêtes avec le profileur de requêtes

Si vous résolvez les problèmes liés à une requête, vous pouvez choisir une requête enfant afin de déterminer quel flux utilise le Pourcentage le plus élevé du temps total de requête. Il s'agit d'un moyen rapide de déterminer quelle partie de votre requête doit être analysée plus en détail.

Une fois que vous avez déterminé quelle requête enfant prend le plus de temps, consultez ses étapes pour déterminer quelle jointure ou quel scan est susceptible de ralentir les performances.

Surveillance des requêtes et des bases de données

Ce document décrit la page de surveillance des requêtes et des bases de données, une Console de gestion AWS fonctionnalité permettant d'analyser les performances d'un cluster provisionné par Amazon Redshift ou d'un groupe de travail sans serveur, ainsi que les requêtes exécutées à leur encontre.

Vous pouvez étudier les scénarios suivants à l'aide de la page Surveillance des requêtes et des bases de données :

- Surveiller les métriques de l'entrepôt de données pendant une période spécifiée
- Comment une requête contribue aux performances globales d'un entrepôt de données
- Afficher la répartition du temps d'exécution d'une requête en événements du cycle de vie tels que le temps d'attente du verrouillage, le temps de compilation et le temps d'exécution
- Quels utilisateurs exécutent les requêtes les plus gourmandes en ressources au cours d'une période donnée
- Surveiller l'impact des événements liés aux correctifs sur les performances des requêtes

Rubriques

- Permissions
- Console de surveillance des requêtes et des bases de données

Permissions

Les privilèges Compte AWS que vous utilisez pour accéder à la console affectent les requêtes affichées sur la page Surveillance des requêtes et des bases de données. Par défaut, vous ne pouvez consulter que vos propres requêtes. Pour consulter les requêtes appartenant à d'autres utilisateurs, accordez le rôle `SYS:MONITOR` à votre compte. Pour permettre à un utilisateur de mettre fin à l'exécution de requêtes depuis la page Surveillance des requêtes et des bases de données, accordez-lui le privilège `SYS:OPERATOR`.

Pour attribuer automatiquement le rôle `sys:monitor` à un utilisateur IAM ou un rôle pour Amazon Redshift sans serveur ou alloué, exécutez les commandes suivantes :

```
create role monitor;
grant role sys:monitor to role monitor;
```

Pour mettre à jour le rôle IAM utilisé pour le suivi des requêtes, procédez comme suit :

1. Sélectionnez l'onglet Tags (Identifications).
2. Choisissez Gérer les balises.
3. Ajouter une balise avec la clé **`RedshiftDbRoles`** et la valeur **`monitor`**.
4. Enregistrer les modifications.

Exécutez la commande suivante pour ajouter les informations d'identification de la base de données à un utilisateur :

```
grant role sys:monitor to <username>
```

Pour plus d'informations sur l'utilisation de la commande GRANT, consultez GRANT dans le Guide du développeur de base de données Amazon Redshift.

Pour utiliser la surveillance des requêtes, votre utilisateur IAM doit être autorisé à accéder au plan de données Amazon Redshift. Veillez à ce que votre utilisateur IAM dispose des autorisations suivantes dans sa politique d'autorisations :

```
{
    "Sid": "DataAPIPermissions",
    "Action": [
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:redshift-serverless:us-
west-2:123456789012:workgroup/01234567-89ab-cdef-0123-456789abcdef"
},
```

Informations d’identification temporaires utilisant votre identité IAM

Cette option est disponible uniquement lors de la connexion à un cluster. Avec cette méthode, la surveillance des requêtes et des bases de données mappe un nom d’utilisateur à votre identité IAM et génère un mot de passe temporaire pour se connecter à la base de données sous votre identité IAM. Un utilisateur utilisant cette méthode pour se connecter doit disposer de l’autorisation IAM pour `redshift:GetClusterCredentialsWithIAM`. Pour empêcher les utilisateurs d’utiliser cette méthode, modifiez leur rôle ou utilisateur IAM afin de refuser cette autorisation.

Console de surveillance des requêtes et des bases de données

Cette section décrit l’utilisation de la page de console de surveillance des requêtes et des bases de données.

Vous pouvez utiliser la console de surveillance des requêtes et des bases de données pour obtenir rapidement une vue d’ensemble des performances de votre entrepôt de données. Vous pouvez surveiller les performances de votre entrepôt de données au fil du temps et examiner les performances des clusters alloués ou des requêtes individuelles d’un entrepôt de données, afin d’identifier au mieux les goulots d’étranglement et les autres domaines à améliorer.

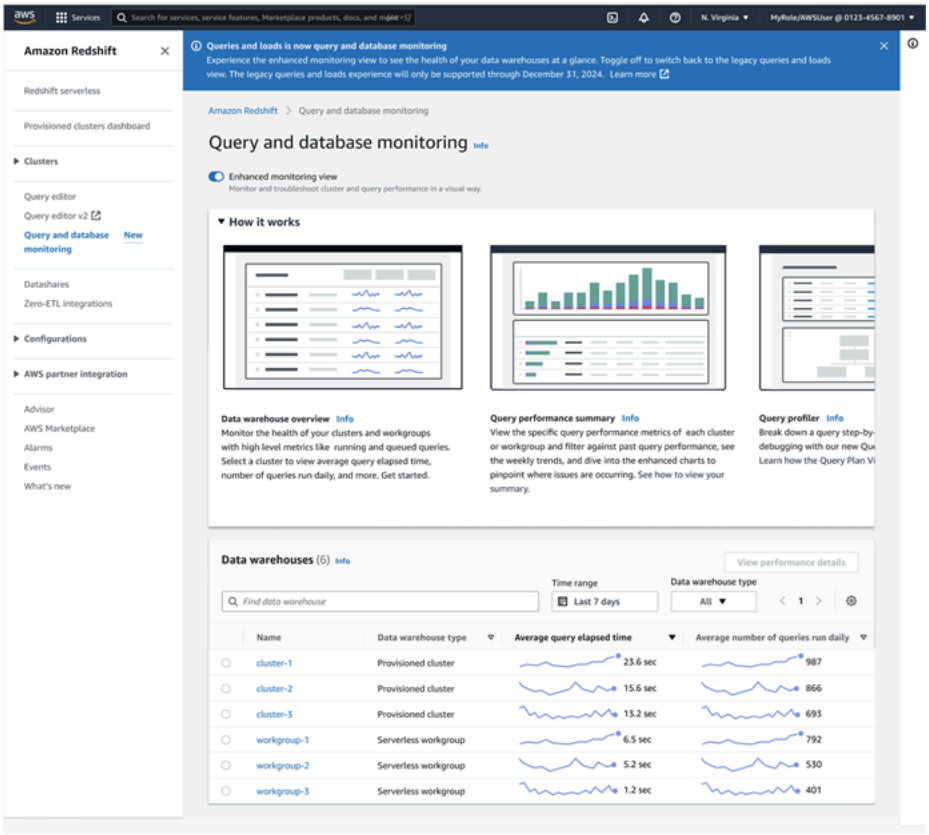
La page Surveillance des requêtes et des bases de données comprend les éléments suivants :

- Sécurité renforcée : vous avez besoin de privilèges élevés pour surveiller les requêtes des autres utilisateurs. Pour de plus amples informations, veuillez consulter Permissions.
- Seven-day historique des requêtes : accès garanti à sept jours d'historique des requêtes
- Surveillance des requêtes : vous pouvez surveiller les requêtes dans les clusters alloués et les groupes de travail sans serveur au niveau des requêtes des utilisateurs.
- Analyse des tendances des requêtes : vous pouvez comparer les performances de requêtes similaires répondant à des critères spécifiques.

Pour accéder à la page Surveillance des requêtes et des bases de données procédez comme suit :

1. Connectez-vous à la console Amazon Redshift à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Choisissez Surveillance des requêtes et des bases de données à partir du panneau de navigation.

La page de la console de surveillance des requêtes et des bases de données apparaît comme suit :



La page Surveillance des requêtes et des bases de données comprend les éléments suivants :

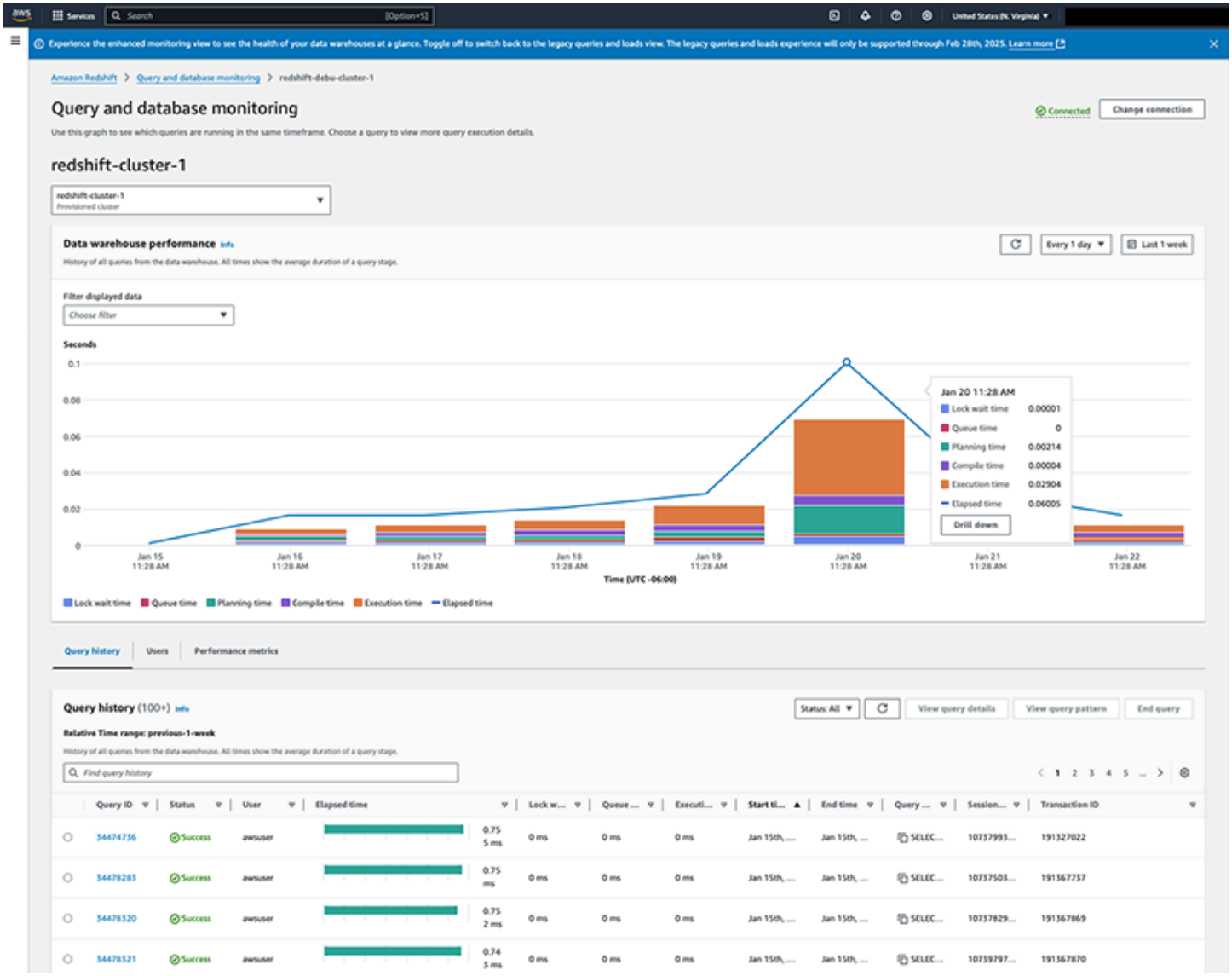
- Vue d'ensemble de l'entrepôt de données : surveillez les performances moyennes des requêtes pour vos clusters alloués et vos groupes de travail sans serveur. Vous pouvez rapidement identifier les problèmes de performances d'un cluster ou d'un groupe de travail spécifique en consultant les statistiques de cette page pour détecter les pics ou les périodes de forte activité.
- Résumé des performances des requêtes : surveillez les performances moyennes des requêtes pour un cluster alloué ou un groupe de travail sans serveur spécifique. Vous pouvez également accéder à la page Récapitulatif des performances des requêtes en cliquant sur l'un des clusters ou groupes de travail dans la liste Présentation de l'entrepôt de données.

Rubriques

- Récapitulatif des performances des requêtes
- Détails de la requête
- Modèle de requête

Récapitulatif des performances des requêtes

Lorsque vous sélectionnez Récapitulatif des performances des requêtes sur la page Surveillance des requêtes et des bases de données, ou un cluster ou un groupe de travail sur la page Présentation de l'entrepôt de données, la console affiche un récapitulatif des performances d'un cluster alloué individuel ou d'un groupe de travail sans serveur.



Cette page dispose des composants suivants :

- Liste déroulante du cluster ou du groupe de travail : choisissez le cluster ou le groupe de travail que vous souhaitez analyser.
- Performances de l'entrepôt de données : ce volet affiche l'historique du cluster ou du groupe de travail au cours de la période spécifiée, indiquant le temps consacré à chaque phase des requêtes.

Si vous constatez un pic au cours d'une certaine phase de requête, comme l'augmentation du temps de planification et d'exécution le 20 janvier dans le graphe précédent, vous pouvez utiliser ces informations pour identifier les problèmes liés aux performances de vos requêtes. La période par défaut affichée correspond aux sept derniers jours, mais vous pouvez ajuster la période en fonction de vos besoins d'analyse.

- Historique des requêtes : ce volet affiche l'historique des performances de chaque requête exécutée dans les filtres spécifiés. Vous pouvez utiliser ces informations pour résoudre les problèmes de performances d'une requête individuelle. Pour analyser plus en détail une requête spécifique, vous pouvez la sélectionner dans ce graphe ou dans le graphe des Performances de l'entrepôt de données.

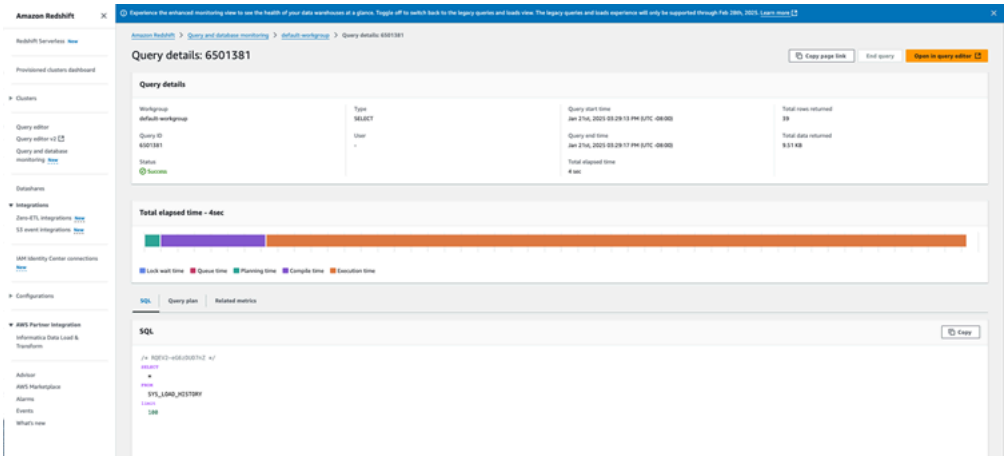
  Lorsque vous survolez un point de données du graphe, une fenêtre contextuelle apparaît. Cette fenêtre contextuelle affiche la répartition des métriques temporelles pour ce point de données. Si un point de données contient des données de requête, vous pouvez choisir Approfondir pour mettre à jour la plage de temps du graphe en fonction de l'unité de temps la plus petite du point de données. Ces unités de temps sont les suivantes :

  - jour
  - Heure
  - 15 minutes
  - 5 minutes
  - 1 minute

  Par exemple, si vous choisissez Approfondir sur un point de données, la plage du graphe passe à un jour. Si vous sélectionnez à nouveau Approfondir, la plage du graphe passe à une heure.
- Profileur de requêtes : outil graphique permettant de surveiller les performances des requêtes. Pour plus d'informations, consultez Profileur de requêtes.

Détails de la requête

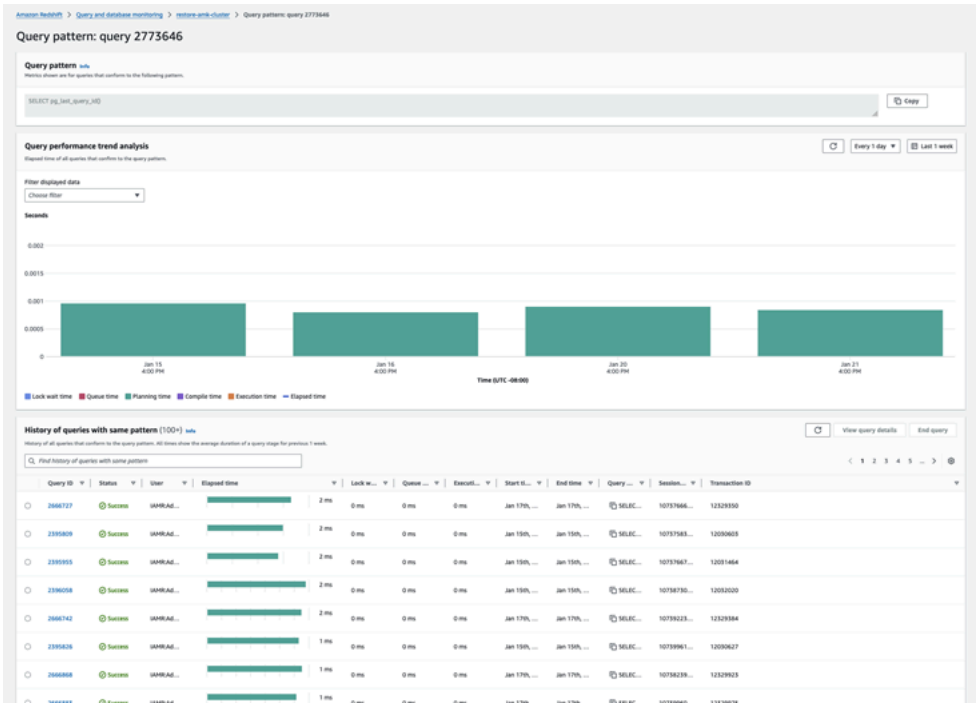
Lorsque vous choisissez une requête dans le volet Performances de l'entrepôt de données ou Historique des requêtes de la page détaillée du cluster ou du groupe de travail, la page Détails de la requête s'ouvre.



Pour obtenir des informations sur les Détails de la requête, consultez Page des détails de la requête.

Modèle de requête

Vous pouvez consulter l'historique des requêtes utilisant le même modèle en cliquant sur le bouton Afficher le modèle de requête dans le volet Historique des requêtes de la page Récapitulatif des performances des requêtes. La page Modèle de requête affiche toutes les requêtes de la semaine dernière qui sont extraites par une instruction SQL que vous spécifiez.



La page Modèle de requête comprend les éléments suivants :

- Modèle de requête : instruction SQL qui extrait les requêtes en cours d'analyse.

- Analyse des tendances des performances des requêtes : graphique à barres indiquant le temps écoulé pour toutes les requêtes sélectionnées par le modèle de requête. Les résultats sont regroupés par jour.
- Historique des requêtes utilisant le même modèle : temps nécessaire pour chaque phase des requêtes sélectionnée par le modèle de requête.

À l'aide de la page Modèle de requête, vous pouvez obtenir les informations suivantes :

- Tendances relatives aux requêtes exécutées à une heure précise chaque jour
- Augmentation du temps d'exécution pour les requêtes que vous exécutez régulièrement sur l'entrepôt de données.

View-based Requêtes système et surveillance des bases de données

Ce document décrit les vues SYS qui fournissent des données pour la page Surveillance des requêtes et des bases de données dans la console Amazon Redshift, un outil permettant d'analyser les composants et les performances d'une requête. Pour plus d'informations sur la page Surveillance des requêtes et des bases de données, consultez Surveillance des requêtes et des bases de données.

La page Surveillance des requêtes et des bases de données comporte une fonctionnalité qui affiche les informations fournies par les vues SYS. La vue de la console inclut le profileur de requêtes, qui affiche le plan d'exécution graphique d'une requête. Pour passer à la vue basée sur SYS, suivez les étapes ci-dessous pour accorder l'accès et les autorisations appropriés correspondant à la nouvelle page Surveillance des requêtes et des bases de données.

La vue basée sur SYS de la page Surveillance des requêtes et des bases de données comporte les fonctionnalités suivantes :

- Sécurité renforcée : vous avez besoin de privilèges élevés pour surveiller les requêtes des autres utilisateurs.
- Seven-day historique des requêtes : accès garanti à sept jours d'historique des requêtes
- Profileur de requêtes : outil graphique permettant de surveiller les performances des requêtes. Pour de plus amples informations, consultez Profileur de requêtes.

Par défaut, vous ne pouvez consulter que vos propres requêtes. Pour consulter les requêtes appartenant à d'autres utilisateurs, accordez le rôle `SYS:MONITOR` à votre compte. Pour permettre à un utilisateur de mettre fin à l'exécution de requêtes, accordez-lui le privilège `SYS:OPERATOR`.

Pour accorder le privilège d'afficher les requêtes appartenant à tous les utilisateurs à un utilisateur ou à un rôle de base de données, exécutez les commandes suivantes :

```
grant role sys:monitor to "IAM:role-name";
grant role sys:monitor to "IAM:user-name";
```

Pour attribuer automatiquement le rôle `sys:monitor` à un utilisateur IAM ou un rôle pour Amazon Redshift sans serveur ou alloué, exécutez les commandes suivantes :

```
 create role monitor;
grant role sys:monitor to role monitor;
```

Pour mettre à jour le rôle IAM utilisé pour le suivi des requêtes, procédez comme suit :

1. Sélectionnez l'onglet Tags (Identifications).
2. Choisissez Gérer les balises.
3. Ajouter une balise avec la clé **`RedshiftDbRoles`** et la valeur **`monitor`**.
4. Enregistrer les modifications.

Exécutez la commande suivante pour ajouter les informations d'identification de la base de données à un utilisateur :

```
grant role sys:monitor to <username>
```

Permissions

Pour utiliser la surveillance des requêtes, votre utilisateur IAM doit être autorisé à accéder au plan de données Amazon Redshift. Veillez à ce que votre utilisateur IAM dispose des autorisations suivantes dans sa politique d'autorisations :

```
{
    "Sid": "DataAPIPermissions",
    "Action": [
        "redshift-data:ExecuteStatement",
```

```
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:redshift-serverless:us-
west-2:123456789012:workgroup/01234567-89ab-cdef-0123-456789abcdef"
},
```

Établir une connexion à la base de données

Avant d'utiliser la fonctionnalité améliorée de surveillance des requêtes, vous devez d'abord vous connecter à votre base de données pour accéder aux informations basées sur les vues SYS. Pour vous connecter à la base de données, utilisez l'une des informations d'identification suivantes :

- Nom d'utilisateur et mot de passe
- Informations d'identification temporaires associées à votre rôle IAM
- Utilisateur de la base de donnée

Notez les informations suivantes à propos de l'utilisation de la surveillance améliorée des requêtes :

- Pour les clusters alloués, vous devez vous connecter à une base de données, car la surveillance améliorée des requêtes utilise des vues SYS. Ces vues ont renforcé la sécurité et nécessitent des privilèges élevés pour accéder aux données relatives aux requêtes détenues par d'autres utilisateurs.
- Lorsque vous utilisez les requêtes basées sur des vues SYSet la page de surveillance des bases de données, seul votre `user_id` est visible si votre compte utilisateur n'a pas le rôle de super-utilisateur de base de données. Les noms d'utilisateur sont cachés aux non-super-utilisateurs.
- Dans le cadre de la page Surveillance des requêtes et des bases de données basée sur des vues système, l'ID du processus d'exécution des requêtes (`p_id`) apparaît sous l'en-tête de colonne `session_id`.

Suivi des clusters alloués Amazon Redshift et des groupes de travail sans serveur

Lorsqu'Amazon Redshift publie une nouvelle version, il met à jour la version de votre entrepôt de données Amazon Redshift (groupe de travail sans serveur ou cluster alloué). Vous pouvez vérifier si votre entrepôt de données est mis à jour à la dernière version certifiée ou à la précédente.

Le suivi du groupe de travail sans serveur ou du cluster alloué détermine la version publiée qui est appliquée lors d'une mise à jour de version. Amazon Redshift met à jour les clusters alloués pendant la période de maintenance spécifiée et met généralement à jour les groupes de travail sans serveur pendant les périodes d'inactivité. Pour plus de détails sur les mises à jour des groupes de travail par Redshift sans serveur, consultez Mise à jour des groupes de travail sans serveur.

Lorsqu'Amazon Redshift publie une nouvelle version, cette version est assignée au suivi Actuelle et la version précédente est assignée au suivi Précédente. Pour définir le suivi de votre entrepôt de données, spécifiez l'une des valeurs suivantes :

- Actuelle : avec le suivi Actuelle, vous obtenez la version certifiée la plus récente avec les dernières fonctionnalités, mises à jour de sécurité et améliorations de performances.
- Précédente : avec le suivi Précédente, vous retrouverez la version certifiée précédente.

Par exemple, supposons que votre groupe de travail sans serveur exécute actuellement la version 1.0.2762 et que Amazon Redshift publie Redshift version 1.0.3072. Si votre valeur de suivi est Actuelle, votre groupe de travail est mis à jour vers la version 1.0.3072 (la dernière version). Si vous définissez la valeur de suivi sur Précédente, votre groupe de travail est mis à jour lorsque la prochaine version du suivi Précédente est publiée.

Grâce à la fonctionnalité de suivi Précédente, vous avez la possibilité de gérer un sous-ensemble d'entrepôts de données Amazon Redshift dans le suivi Précédente. Cela permet de tester et de valider l'intégration pendant 1 à 6 semaines sur les entrepôts de données définis sur le suivi Actuelle avant d'appliquer la version aux entrepôts de données sur le suivi Précédente. Par défaut, Amazon Redshift crée tous les clusters et groupes de travail sur le suivi Actuelle afin de tirer parti de la version certifiée la plus récente. Cependant, l'utilisation du suivi Précédente Amazon Redshift dans votre environnement de production et du suivi Actuelle dans votre environnement de test et de développement vous donne plus de diligence et de temps pour évaluer la dernière version. Le suivi

Précédente garantit une stabilité maximale, ce qui le rend idéal pour les charges de travail critiques dans les environnements de production.

> **Note**
>
> La version de suivi peut être identique à la version de suivi Actuelle pendant de courtes périodes. Cela se produit lorsque le suivi en cours n'est pas passé à la version suivante. Normalement, la version de suivi Actuelle est en avance sur la version de suivi Précédente.

Basculement entre les suivis

Modifier le suivi d'une ressource Amazon Redshift est généralement une décision unique. Vous devez faire preuve de prudence lorsque vous procédez à cette modification. Pour plus d'informations sur quelles fonctionnalités se trouvent dans quelles versions d'entrepôt de données, consultez Versions de cluster pour Amazon Redshift.

Si vous passez du suivi Précédente au suivi Actuelle, nous mettrons à jour le l'entrepôt de données vers la version de suivi Actuelle. Si vous remplacez le suivi de l'entrepôt de données par Précédente, nous mettrons à jour votre entrepôt de données comme suit :

- Pour les groupes de travail sans serveur, nous mettons à jour la version de votre entrepôt de données pendant une période d'inactivité. Pour plus de détails sur la façon dont Redshift sans serveur met à jour la version de votre groupe de travail, consultez Mise à jour des groupes de travail sans serveur.
- Pour les clusters alloués, nous ne mettrons à jour votre entrepôt de données que lorsqu'il y existera une version postérieure à la version de suivi Actuelle.

Suivis et restauration

Pour les groupes de travail sans serveur, un instantané hérite du suivi de l'entrepôt de données Amazon Redshift cible. Par exemple, si vous créez un instantané pour un groupe de travail défini sur le suivi Précédente, et que vous appliquez cet instantané à un groupe de travail défini sur le suivi Actuelle, le groupe de travail aura un paramètre de suivi Actuelle.

Pour les clusters alloués, un instantané hérite du suivi de l'entrepôt de données Amazon Redshift source. Si vous modifiez le suivi de l'entrepôt de données source après avoir pris un instantané, l'instantané et l'entrepôt de données source disposeront donc de suivis différents. Lorsque vous

effectuez une restauration à partir de l'instantané, le nouvel entrepôt de données héritera donc du suivi de l'instantané source. Vous pourrez modifier le suivi une fois la restauration terminée.

Le redimensionnement d'un entrepôt de données n'a aucune incidence sur son suivi.

Mise à jour des groupes de travail sans serveur

Lorsqu'une nouvelle version est disponible pour le suivi choisi pour un groupe de travail, Amazon Redshift sans serveur applique généralement la mise à jour pendant une période d'inactivité tant qu'aucune demande de mise à jour de suivi n'est en attente. Si le groupe de travail ne connaît pas de période d'inactivité dans les 14 jours, Redshift sans serveur force la mise à jour de la version.

Redshift sans serveur met uniquement à jour votre groupe de travail vers la version supérieure suivante. Redshift sans serveur n'ignore pas les versions intermédiaires et ne rétrograde pas les groupes de travail, même si la version du suivi du groupe de travail sélectionné est inférieure à la version actuelle du groupe de travail. Votre groupe de travail ne bénéficiera d'aucune mise à niveau de version majeure tant que le suivi `Trailing` ne sera pas rattrapé.

Supposons, par exemple, que le suivi `Current` soit la version 186 et que la version du suivi `Trailing` soit 185. Si vous avez un groupe de travail avec une valeur `Track` de `Current`, dont la version est 186, si vous modifiez la valeur `Track` pour `Trailing`, Redshift sans serveur ne rétrogradera pas la version du groupe de travail à 185. Dans ce scénario, Redshift sans serveur maintient le groupe de travail sur la version 186 jusqu'à ce que la version du suivi `Trailing` soit égale ou supérieure à 186.

Si une modification de suivi est en attente, Redshift sans serveur ne met pas à jour le groupe de travail vers la prochaine version majeure du suivi existante tant qu'il n'applique pas la modification de suivi. Une fois le changement de suivi terminé, Redshift sans serveur évalue les conditions de mise à jour du groupe de travail vers la version appropriée dans le cadre du nouveau suivi.

Par exemple, si votre groupe de travail est configuré sur le suivi `Current`, que le suivi Actuelle est 186, et que vous remplacez votre groupe de travail par le suivi `Trailing`, Redshift sans serveur ne mettra à jour le groupe de travail qu'après avoir appliqué le changement de suivi et après que la version `Trailing` ait été mise à jour vers une version égale ou supérieure à 186.

> **Note**
>
> Toute opération existante sur un groupe de travail, telle que la restauration à partir d'un instantané, la modification de la clé KMS ou le redimensionnement, ne s'effectue que sur le

suivi existant. Redshift sans serveur n'utilise pas le suivi en attente pour les opérations sans serveur.

Si vous avez une demande de changement de voie en attente, vous pouvez annuler la demande en rétablissant la valeur initiale du `track` paramètre à l'aide de UpdateWorkgroup.

Gestion des versions

Un suivi est composé d'une série de versions. Vous pouvez configurer votre entrepôt de données Amazon Redshift sur le suivi Actuelle ou sur le suivi Précédente. Si vous configurez votre entrepôt de données sur le suivi Actuelle, il sera toujours mis à jour vers la version la plus récente. Si vous configurez votre ressource sur le suivi Précédente, il sera toujours exécuté sur la version publiée juste avant la version la plus récente.

Pour les clusters alloués, la colonne Statut de la version de la liste d'entrepôt de données Amazon Redshift de la console Amazon Redshift indique si l'une de vos ressources est disponible pour une mise à jour.

Déterminer la version du groupe de travail ou du cluster

Vous pouvez déterminer la version du groupe de travail Amazon Redshift sans serveur ou le moteur de version du cluster alloué avec la console Amazon Redshift.

Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/

Serverless workgroups

Pour les groupes de travail sans serveur, dans le menu de navigation, choisissez Groupes de travail, puis sélectionnez le nom du groupe de travail dans la liste pour ouvrir ses détails. Les détails du groupe de travail s'affichent.

Provisioned clusters

Pour les clusters alloués, dans le menu de navigation, choisissez Clusters, puis choisissez le nom du cluster dans la liste pour ouvrir ses détails.

Les détails du cluster sont affichés, ce qui peut inclure les onglets Performance du cluster, Surveillance des requêtes, Bases de données, Unités de partage des données, Planifications, Maintenance et Propriétés. Choisissez l'onglet Maintenance pour plus de détails.

Dans la section Maintenance, recherchez Version de cluster actuelle.

> **Note**
>
> Pour les clusters alloués, la console affiche les informations de version dans un même champ, mais il s'agit de deux paramètres dans l'API Amazon Redshift. Ces paramètres sont `ClusterVersion` et `ClusterRevisionNumber`. Pour plus d'informations, consultez Cluster dans la Référence API Amazon Redshift.

Zero-ETL intégrations

Zero-ETL integration est une solution entièrement gérée qui met à disposition des données transactionnelles et opérationnelles dans Amazon Redshift à partir de plusieurs sources opérationnelles et transactionnelles. Avec cette solution, vous pouvez configurer une intégration à partir de votre source vers un entrepôt des données Amazon Redshift. Vous n'avez pas besoin de gérer un pipeline d'extraction, transformation et chargement (ETL). Nous nous occupons des tâches ETL pour vous en automatisant la création et la gestion de la réplication des données à partir de la source de données vers le cluster Amazon Redshift ou l'espace de noms Redshift sans serveur. Vous pouvez continuer à mettre à jour et à interroger vos données source tout en utilisant simultanément Amazon Redshift pour des charges de travail analytiques, telles que la création de rapports et de tableaux de bord.

Grâce à l'intégration Zero-ETL, vous disposez de données plus récentes à des fins d'analyse et de création de AI/ML rapports. Vous obtenez des informations plus précises et plus opportunes pour des cas d'utilisation tels que les tableaux de bord métier, l'optimisation de l'expérience de jeu, le suivi de la qualité des données et l'analyse du comportement des clients. Vous pouvez établir des prévisions basées sur les données en toute confiance, améliorer l'expérience client et promouvoir des informations basées sur les données à l'échelle de l'entreprise.

Les sources suivantes sont actuellement prises en charge pour les intégrations zéro ETL :

- Amazon Aurora MySQL (AMS)
- Amazon Aurora PostgreSQL (APG)
- Amazon DynamoDB
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS pour PostgreSQL
- Oracle Database@AWS
- Applications telles que Salesforce, Salesforce Marketing Cloud Account Engagement, SAP, Instagram Ads ServiceNow, Meta Ads et Zendesk
- Self-Managed MySQL, PostgreSQL, SQL Server et Oracle

Pour créer une intégration zéro ETL, vous spécifiez une source d'intégration et un entrepôt des données Amazon Redshift comme cible. Après un chargement des données initial, l'intégration

réplique les données de la source vers l'entrepôt de données cible. Les données sont mises à disposition dans Amazon Redshift. Vous contrôlez le chiffrement de vos données lorsque vous créez la source d'intégration, lorsque vous créez l'intégration zéro ETL et lorsque vous créez l'entrepôt de données Amazon Redshift. L'intégration surveille l'état du pipeline de données et effectue la récupération en cas de problèmes, lorsque cela est possible. Vous pouvez créer des intégrations à partir de sources du même type dans un seul entrepôt des données Amazon Redshift afin de dériver des informations holistiques entre plusieurs applications.

Avec les données figurant dans Amazon Redshift, vous pouvez utiliser les analyses fournies par Amazon Redshift. Par exemple, le machine learning (ML) intégré, les vues matérialisées, le partage de données et l'accès direct à plusieurs magasins de données et lacs de données. Pour les ingénieurs de données, l'intégration zéro ETL permet d'accéder à des données sensibles au temps qui pourraient autrement être retardées par des erreurs intermittentes dans des pipelines de données complexes. Vous pouvez exécuter des requêtes analytiques et des modèles ML sur des données transactionnelles afin de dériver des informations en temps opportun sur les événements sensibles au temps et les décisions commerciales.

Vous pouvez créer un abonnement aux notifications d'événements Amazon Redshift afin de pouvoir être informé quand un événement se produit pour une intégration zéro ETL donnée. Pour consulter la liste des notifications d'événements liées à l'intégration, consultez Zero-ETL notifications d'événements d'intégration avec Amazon EventBridge. La solution la plus simple pour créer un abonnement consiste à utiliser la console Amazon SNS. Pour en savoir plus sur la création d'une rubrique Amazon SNS et l'abonnement à cette rubrique, consultez Démarrage avec Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

Lorsque vous commencez à utiliser des intégrations zéro ETL, tenez compte des concepts suivants :

- Une base de données source est la base de données depuis laquelle les données sont répliquées dans Amazon Redshift.
- Un entrepôt des données cible est le cluster provisionné par Amazon Redshift ou le groupe de travail Redshift sans serveur dans lequel les données sont répliquées.
- Une base de données de destination est la base de données que vous créez à partir d'une intégration zéro ETL dans l'entrepôt des données cible.

Pour plus d'informations sur les tables et les vues système que vous pouvez utiliser pour surveiller vos intégrations zéro ETL, consultez Surveillance des intégrations zéro ETL aux vues système Amazon Redshift.

Pour obtenir la liste des éléments pris Régions AWS en charge par chaque source pour les intégrations sans ETL, consultez. Régions prises en charge pour les intégrations zéro ETL

Pour obtenir des informations sur les tarifs des intégrations zéro ETL, consultez la page de tarification appropriée :

- Tarification d'Amazon Redshift
- Tarification d'Amazon Aurora
- Tarification d'Amazon RDS
- Tarification Amazon DynamoDB
- AWS Glue tarification

Pour plus d'informations sur les sources d'intégration zéro ETL, consultez les rubriques suivantes :

- Pour les intégrations zéro ETL d'Aurora, consultez Avantages, Concepts clés, Limitations, Quotas et Régions prises en charge des intégrations zéro ETL dans le Guide de l'utilisateur Amazon Aurora.
- Pour les intégrations zéro ETL de RDS, consultez Avantages, Concepts clés, Limitations, Quotas et Régions prises en charge des intégrations zéro ETL dans le Guide de l'utilisateur Amazon RDS.
- Pour les intégrations zéro ETL DynamoDB, consultez Intégration zéro ETL DynamoDB à Amazon Redshift dans le Guide du développeur Amazon DynamoDB.
- Pour les intégrations sans ETL avec les applications, consultez la section Zero-ETL Intégrations dans le Guide du développeur. AWS Glue

Rubriques

- Considérations relatives au moment d'utiliser les intégrations zéro ETL avec Amazon Redshift
- Bien démarrer avec les intégrations zéro ETL
- Création de bases de données de destination dans Amazon Redshift
- Interrogation des données répliquées dans Amazon Redshift
- Affichage des intégrations zéro ETL
- Mode historique
- Partage de vos données dans Amazon Redshift
- Surveillance des intégrations zéro ETL

- Métriques pour les intégrations zéro ETL
- Modification d'une intégration zéro ETL pour DynamoDB
- Suppression d'une intégration zéro ETL pour DynamoDB
- Régions prises en charge pour les intégrations zéro ETL
- Résolution des problèmes liés aux intégrations zéro ETL

Considérations relatives au moment d'utiliser les intégrations zéro ETL avec Amazon Redshift

Les considérations suivantes s'appliquent aux intégrations zéro ETL avec Amazon Redshift.

- Votre entrepôt des données Amazon Redshift cible doit répondre aux conditions préalables suivantes :
  - Exécution d'Amazon Redshift Serverless ou d'un cluster provisionné de type nœud RG ou RA3.
  - Chiffré (si vous utilisez un cluster provisionné).
  - La sensibilité à la casse est activée.
- Si vous supprimez une source d'intégration autorisée pour un entrepôt des données Amazon Redshift, toutes les intégrations associées passeront à l'état `FAILED`. Toutes les données précédemment répliquées restent dans votre base de données Amazon Redshift et peuvent être consultées.
- La base de données de destination est en lecture seule. Vous ne pouvez pas créer de tables, de vues ni de vues matérialisées dans la base de données de destination. Toutefois, vous pouvez utiliser des vues matérialisées sur d'autres tables dans l'entrepôt des données cible.
- Les vues matérialisées sont prises en charge lorsqu'elles sont utilisées dans des requêtes entre bases de données. Pour en savoir plus sur la création de vues matérialisées avec des données répliquées via des intégrations zéro ETL, consultez Interrogation de données répliquées avec des vues matérialisées.
- Par défaut, vous pouvez interroger les tables uniquement dans l'entrepôt des données cible qui se trouvent dans l'état `Synced`. Pour interroger des tables dans un autre état, définissez le paramètre de base de données `QUERY_ALL_STATES` sur `TRUE`. Pour plus d'informations sur la définition de `QUERY_ALL_STATES`, consultez CREATE DATABASE et ALTER DATABASE dans le Guide du développeur Amazon Redshift. Pour plus d'informations sur l'état de votre base de données, consultez SVV_INTEGRATION_TABLE_STATE dans le Guide du développeur de base de données Amazon Redshift.

- Amazon Redshift n'accepte que des UTF-8 caractères. Il est donc possible qu'il ne respecte pas le classement défini dans votre source. Les règles de tri et de comparaison peuvent être différentes, ce qui peut finalement modifier les résultats de la requête.
- Zero-ETL le nombre d'intégrations est limité à 50 par cible d'entrepôt de données Amazon Redshift.
- Les tables de la source d’intégration doivent posséder une clé primaire. Sinon, vos tables ne peuvent pas être répliquées vers l’entrepôt de données cible dans Amazon Redshift.

  Pour plus d’informations sur la façon d’ajouter une clé primaire à Amazon Aurora PostgreSQL, consultez Gestion des tables sans clés primaires lors de la création d’intégrations zéro ETL Amazon Aurora PostgreSQL avec Amazon Redshift sur le Blog de base de données AWS . Pour plus d’informations sur la façon d’ajouter une clé primaire à Amazon Aurora MySQL ou RDS for MySQL, consultez Gestion des tables sans clés primaires lors de la création d’intégrations zéro ETL Amazon Aurora MySQL ou Amazon RDS for MySQL avec Amazon Redshift sur le Blog de base de données AWS .
- Vous pouvez utiliser le filtrage des données pour les intégrations zéro ETL Aurora afin de définir l’étendue de la réplication entre le cluster de base de données Aurora source et l’entrepôt de données Amazon Redshift cible. Plutôt que de répliquer toutes les données vers la cible, vous pouvez définir un ou plusieurs filtres qui incluent ou excluent de manière sélective certaines tables de la réplication. Pour plus d’informations, consultez Filtrage des données pour les intégrations zéro ETL Aurora avec Amazon Redshift dans le Guide de l’utilisateur Amazon Aurora.
- Pour les intégrations zéro ETL Aurora PostgreSQL avec Amazon Redshift, Amazon Redshift prend en charge un maximum de 100 bases de données Aurora PostgreSQL. Chaque base de données se réplique de la source vers la cible indépendamment.
- Zero-ETL l'intégration ne prend pas en charge les transformations lors de la réplication des données depuis des magasins de données transactionnels vers Amazon Redshift. Les données sont répliquées telles quelles à partir de la base de données source. Vous pouvez toutefois appliquer des transformations aux données répliquées dans Amazon Redshift.
- Zero-ETL l'intégration s'exécute dans Amazon Redshift à l'aide de connexions parallèles. Elle s’exécute en utilisant les informations d’identification de l’utilisateur qui a créé la base de données à partir de l’intégration.
- Vous pouvez définir une intégration zéro ETL afin de contrôler la fréquence de réplication des données dans Amazon Redshift `REFRESH_INTERVAL`. Pour plus d’informations, consultez CREATE DATABASE et ALTER DATABASE dans le Guide du développeur de base de données Amazon Redshift.

- Après avoir créé une base de données Amazon Redshift à partir d'une intégration zéro ETL avec Amazon DynamoDB, l'état de la base de données doit passer de Création à Active. Cela démarre la réplication des données dans les tables DynamoDB source vers les tables Redshift cibles, qui sont créées selon le schéma public de la base de données de destination (`ddb_rs_customerprofiles_zetl_db`).

Considérations relatives à l'utilisation du mode historique sur la cible

Les considérations suivantes s'appliquent lorsque vous utilisez le mode historique sur la base de données cible. Pour plus d'informations, consultez Mode historique.

- Lorsque vous déposez une table sur une source, la table sur la cible n'est pas supprimée, mais son état est changé pour `DroppedSource`. Vous pouvez supprimer ou renommer la table depuis la base de données Amazon Redshift.
- Lorsque vous tronquez une table sur une source, des suppressions sont effectuées sur la table cible. Par exemple, si tous les enregistrements sont tronqués sur la source, les enregistrements correspondants de la colonne cible `_record_is_active` sont remplacés par `false`.
- Lorsque vous exécutez la commande SQL TRUNCATE sur la table cible, les lignes d'historique actives sont marquées comme inactives avec l'horodatage correspondant.
- Lorsqu'une ligne d'un tableau est définie comme inactive, elle peut être supprimée après un court délai (environ 10 minutes). Pour supprimer les lignes inactives, connectez-vous à votre base de données zéro ETL à l'aide de l'éditeur de requête v2 ou d'un autre client SQL.
- Vous ne pouvez supprimer des lignes inactives d'un tableau que lorsque le mode historique est activé. Par exemple, une commande SQL similaire à la suivante supprime uniquement les lignes inactives.

  ```
  delete from schema.user_table where _record_delete_time <= '2024-09-10 12:34:56'
  ```

  Cela équivaut à une commande SQL similaire à celle-ci.

  ```
  delete from schema.user_table where _record_delete_time <= '2024-09-10 12:34:56' and
   _record_is_active = False
  ```

- Lorsque le mode historique est désactivé pour une table, toutes les données historiques sont enregistrées dans la table nommée avec `<schema>.<table-`

name>_historical_<timestamp> tandis que la table d'origine nommée <schema>.<table-name> est actualisée.

- Lorsqu'une table dont le mode historique est activé est exclue de la réplication à l'aide d'un filtre de table, toutes les lignes sont définies comme inactives et leur état est changé pour `DroppedSource`. Pour plus d'informations sur les filtres de table, consultez Filtrage des données pour les intégrations zéro ETL Aurora avec Amazon Redshift dans le Guide de l'utilisateur Amazon Aurora.
- Le mode historique ne peut être défini que sur `true` ou `false` pour les tables en état `Synced`.
- Les vues matérialisées pour les tables dont le mode historique est activé sont créées sous forme de recalcul complet.

Considérations lorsque la source d'intégration zéro ETL est Aurora ou Amazon RDS

Les considérations suivantes s'appliquent aux intégrations zéro ETL Aurora et Amazon RDS avec Amazon Redshift.

- Vous pouvez utiliser le filtrage des données pour les intégrations zéro ETL Aurora et RDSL for MySQL afin de définir l'étendue de la réplication entre le cluster de base de données source et l'entrepôt de données Amazon Redshift cible. Plutôt que de répliquer toutes les données vers la cible, vous pouvez définir un ou plusieurs filtres qui incluent ou excluent de manière sélective certaines tables de la réplication. Pour plus d'informations, consultez Filtrage des données pour les intégrations zéro ETL Aurora avec Amazon Redshift dans le Guide de l'utilisateur Amazon Aurora.
- Les tables de la source d'intégration doivent posséder une clé primaire. Sinon, vos tables ne peuvent pas être répliquées vers l'entrepôt de données cible dans Amazon Redshift.

  Pour plus d'informations sur la façon d'ajouter une clé primaire à Amazon Aurora PostgreSQL, consultez Gestion des tables sans clés primaires lors de la création d'intégrations zéro ETL Amazon Aurora PostgreSQL avec Amazon Redshift sur le Blog de base de données AWS . Pour plus d'informations sur la façon d'ajouter une clé primaire à Amazon Aurora MySQL ou RDS for MySQL, consultez Gestion des tables sans clés primaires lors de la création d'intégrations zéro ETL Amazon Aurora MySQL ou Amazon RDS for MySQL avec Amazon Redshift sur le Blog de base de données AWS .
- La longueur maximale d'un type de données Amazon Redshift VARCHAR est de 65 535 octets. Lorsque le contenu de la source ne correspond pas à cette limite, la réplication ne se poursuit pas et la table est mise en état d'échec. Vous pouvez définir le paramètre de base de données

TRUNCATECOLUMNS sur TRUE pour tronquer le contenu afin qu'il tienne dans la colonne. Pour plus d'informations sur la définition de TRUNCATECOLUMNS, consultez CREATE DATABASE et ALTER DATABASE dans le Guide du développeur de base de données Amazon Redshift.

Pour plus d'informations sur les différences de type de données entre les sources d'intégration zéro ETL et les bases de données Amazon Redshift, consultez Différences de type de données entre Aurora et Amazon Redshift dans le Guide de l'utilisateur Amazon Aurora.

Pour les sources Aurora, consultez aussi Limitations dans le Guide de l'utilisateur Amazon Aurora.

Pour les sources Amazon RDS, consultez aussi Limitations dans le Guide de l'utilisateur Amazon RDS.

Considérations lorsque la source d'intégration zéro ETL est DynamoDB

Les considérations suivantes s'appliquent aux intégrations zéro ETL DynamoDB avec Amazon Redshift.

- Les noms de table de DynamoDB supérieurs à 127 caractères ne sont pas pris en charge.
- Les données issues d'une intégration zéro ETL DynamoDB correspondent à une colonne de type de données SUPER dans Amazon Redshift.
- Les noms de colonne de plus de 127 caractères pour la clé de partition ou la clé de tri ne sont pas pris en charge.
- Une intégration zéro ETL provenant de DynamoDB ne peut être mappée qu'à une seule base de données Amazon Redshift.
- Pour les clés de partition et de tri, la précision et l'échelle maximales sont de (38,18). Les types de données numériques sur DynamoDB offrent une précision maximale allant jusqu'à 38. Amazon Redshift prend également en charge une précision maximale de 38, mais la décimale par défaut precision/scale sur Amazon Redshift est (38,10). Cela signifie que les valeurs d'échelle peuvent être tronquées.
- Pour que l'intégration zéro ETL soit réussie, un attribut individuel (composé du nom+de la valeur) d'un élément DynamoDB ne doit pas dépasser 64 Ko.
- Lors de l'activation, l'intégration zéro ETL exporte la table DynamoDB complète pour alimenter la base de données Amazon Redshift. La durée nécessaire à ce processus initial dépend de la taille de la table DynamoDB. L'intégration zéro ETL réplique ensuite de manière incrémentielle les mises à jour de DynamoDB vers Amazon Redshift à l'aide des exportations incrémentielles DynamoDB.

Cela signifie que les données DynamoDB répliquées dans Amazon Redshift sont automatiquement mises à jour.

Actuellement, la latence minimale pour l'intégration zéro ETL DynamoDB est de 15 minutes. Vous pouvez l'augmenter encore en définissant un `REFRESH_INTERVAL` différent de zéro pour une intégration zéro ETL. Pour plus d'informations, consultez CREATE DATABASE et ALTER DATABASE dans le Guide du développeur de base de données Amazon Redshift.

Pour les sources Amazon DynamoDB, consultez également la section Conditions préalables et limites du Guide du développeur Amazon DynamoDB.

Points à prendre en compte lorsque la source d'intégration zéro ETL est constituée d'applications telles que Salesforce ServiceNow, SAP et Zendesk

Les considérations suivantes s'appliquent aux applications source, telles que Salesforce ServiceNow, SAP et Zendesk avec Amazon Redshift.

- Les noms de table et de colonne provenant de sources d'application de plus de 127 caractères ne sont pas pris en charge.
- La longueur maximale d'un type de données Amazon Redshift VARCHAR est de 65 535 octets. Lorsque le contenu de la source ne correspond pas à cette limite, la réplication ne se poursuit pas et la table est mise en état d'échec. Vous pouvez définir le paramètre de base de données `TRUNCATECOLUMNS` sur `TRUE` pour tronquer le contenu afin qu'il tienne dans la colonne. Pour plus d'informations sur la définition de `TRUNCATECOLUMNS`, consultez CREATE DATABASE et ALTER DATABASE dans le Guide du développeur de base de données Amazon Redshift.

  Pour plus d'informations sur les différences de type de données entre les sources d'applications d'intégration zéro ETL et les bases de données Amazon Redshift, consultez la section Zero-ETL Intégrations dans le Guide du AWS Glue développeur.
- La latence minimale pour une intégration zéro ETL avec les applications est d'une heure. Vous pouvez l'augmenter encore en définissant un `REFRESH_INTERVAL` différent de zéro pour une intégration zéro ETL. Pour plus d'informations, consultez CREATE DATABASE et ALTER DATABASE dans le Guide du développeur de base de données Amazon Redshift.

Pour les sources d'intégrations Zero-ETL avec les applications, consultez également les Zero-ETL intégrations dans le Guide du AWS Glue développeur.

Considérations à prendre en compte lors de la restauration d'une cible d'intégration Zéro

Lorsque vous restaurez un espace de noms Amazon Redshift Serverless à partir d'un snapshot ou d'un point de restauration vers le même espace de noms sans serveur, les intégrations Zéro ETL associées à l'espace de noms sont gérées automatiquement. Une resynchronisation complète est lancée après la restauration pour garantir la cohérence des données de la base de données Amazon Redshift cible avec la source. Les considérations suivantes s'appliquent :

- La restauration d'un snapshot dans un autre espace de noms ne permet pas de maintenir les intégrations.
- Après la restauration, Amazon Redshift effectue une resynchronisation complète pour toutes les intégrations sans ETL maintenues. Pendant la resynchronisation, les performances d'ingestion de données peuvent être temporairement réduites.
- Si vous utilisez le mode historique sur la base de données cible, les versions enregistrées entre le moment où la capture d'écran a été prise et la fin de la resynchronisation complète ne sont pas capturées. Après la resynchronisation, le mode historique reprend son fonctionnement normal. Ce comportement est le même que pour toute autre resynchronisation complète. Pour de plus amples informations, veuillez consulter Mode historique.
- Si une intégration Zéro-ETL a été créée après la prise de l'instantané, l'intégration passe à l'`NEEDS_ATTENTIO`Nétat après la restauration car la base de données correspondante n'existe pas dans le cliché. Pour résoudre ce problème, vous pouvez effectuer une restauration à partir d'un instantané plus récent incluant l'intégration, ou supprimer l'intégration.
- Si une intégration Zéro-ETL a été supprimée après la prise de l'instantané, l'intégration n'est pas restaurée. La base de données de l'instantané est conservée et peut être supprimée.
- Si les filtres au niveau de la table ont été modifiés après la prise de l'instantané, la cible restaurée utilise les filtres actuels de l'intégration, et non les filtres au moment de la capture d'écran.
- Pour ne pas conserver les intégrations pendant une restauration, décochez la case Maintenir les intégrations sur la page de restauration du ou Console de gestion AWS, si vous utilisez le, définissez le `--no-maintain-integration` paramètre lorsque vous appelez l' AWS CLI opération d'API restore-from-snapshot ou https://docs.aws.amazon.com/redshift-serverless/latest/APIReference/API_RestoreFromSnapshot.html restore-from-recovery-point. https://docs.aws.amazon.com/redshift-serverless/latest/APIReference/

API_RestoreFromRecoveryPoint.html Lorsque vous vous désabonnez, les intégrations reprennent leur `FAILED` état après la restauration. Vous pouvez supprimer les intégrations et les recréer.

- Cette fonctionnalité s'applique à Amazon Redshift Serverless uniquement lorsqu'il est restauré dans le même espace de noms sans serveur. Les restaurations de snapshots sur des clusters provisionnés ne permettent pas de maintenir des intégrations ETL nulles.

Considérations relatives au redimensionnement d'une cible d'intégration Zéro-ETL

Lorsque vous redimensionnez un cluster provisionné par Amazon Redshift qui est la cible d'une intégration zéro ETL, le redimensionnement peut entraîner la resynchronisation des tables d'intégration. La question de savoir si une resynchronisation se produit dépend du type de redimensionnement :

- Un redimensionnement élastique qui modifie uniquement le nombre de nœuds (un redimensionnement sur place) n'affecte pas les intégrations Zéro ETL. Les tableaux restent synchronisés.
- Un redimensionnement élastique qui modifie le type de nœud entraîne la resynchronisation de toutes les tables des intégrations Zero-ETL du cluster. Tout redimensionnement classique déclenche également une resynchronisation. Cela est dû au fait que ces opérations de redimensionnement modifient temporairement le style de distribution des tables pendant que le service redistribue les données dans la nouvelle configuration de cluster. Pour plus d'informations, consultez la section Redimensionnement d'un cluster.

Les considérations suivantes s'appliquent lorsqu'un redimensionnement déclenche une resynchronisation :

- L'intégration reste active et la resynchronisation démarre automatiquement une fois le redimensionnement terminé. Aucune action de votre part n'est requise.
- Pendant la resynchronisation d'une table, vous ne pouvez pas l'interroger dans Amazon Redshift. Pour que les tables puissent être interrogées pendant la resynchronisation, définissez le `QUERY_ALL_STATES` paramètre `TRUE` sur la base de données de destination avant de commencer le redimensionnement. Les données renvoyées pendant la resynchronisation peuvent être périmées jusqu'à la fin de la resynchronisation. Pour plus d’informations, consultez CREATE DATABASE et ALTER DATABASE dans le Guide du développeur de base de données Amazon Redshift.

- La resynchronisation peut prendre de 20 à 25 minutes ou plus, selon la taille de la base de données source.
- Vous pouvez surveiller l'état des tables d'intégration à l'aide de la vue système https://docs.aws.amazon.com/redshift/latest/dg/r_SVV_INTEGRATION_TABLE_STATE.html SVV_INTEGRATION_TABLE_STATE. Les tableaux indiquent l'`ResyncInitiated`état `ResyncRequired` ou jusqu'à la fin de la resynchronisation et le retour à. `Synced`

Bien démarrer avec les intégrations zéro ETL

Cet ensemble de tâches vous guide tout au long de la configuration de votre première intégration zéro ETL. D'abord, vous spécifiez votre source d'intégration et configurez-la avec les autorisations et paramètres requis. Vous passez ensuite au reste de la configuration initiale depuis la console Amazon Redshift ou AWS CLI. La console propose une option Effectuez les corrections pour moi pour corriger certains problèmes de configuration.

Rubriques

- Création et configuration d'un entrepôt des données Amazon Redshift cible
- Activation de la sensibilité à la casse pour votre entrepôt des données
- Configuration de l'autorisation pour votre entrepôt des données Amazon Redshift
- Création d'une intégration zéro ETL

Création et configuration d'un entrepôt des données Amazon Redshift cible

Au cours de cette étape, vous créez et configurez un entrepôt des données Amazon Redshift cible, tel qu'un groupe de travail Redshift sans serveur ou un cluster provisionné. Si vous disposez déjà d'un entrepôt de données Amazon Redshift configuré pour une utilisation avec des intégrations zéro ETL, vous pouvez ignorer cette étape.

Votre entrepôt des données cible doit présenter les caractéristiques suivantes :

- Exécution d'Amazon Redshift Serverless ou d'un cluster provisionné de type nœud RG ou RA3.
- Sensibilité à la casse (`enable_case_sensitive_identifier`) activée. Pour plus d'informations, consultez Activation de la sensibilité à la casse pour votre entrepôt des données.
- Chiffré, si votre entrepôt des données cible est un cluster provisionné Amazon Redshift. Pour de plus amples informations, veuillez consulter Chiffrement de base de données Amazon Redshift.

- Créé dans la même AWS région que la source d'intégration.

Pour créer votre entrepôt des données cible pour vos intégrations zéro ETL, consultez l'une des rubriques suivantes en fonction de votre type de déploiement :

- Pour créer un cluster provisionné Amazon Redshift, consultez Création d'un cluster.
- Pour créer un groupe de travail Amazon Redshift sans serveur avec un espace de noms, consultez Création d'un groupe de travail avec un espace de noms.

Lorsque vous créez un cluster alloué, Amazon Redshift crée également un groupe de paramètres par défaut. Vous ne pouvez pas modifier le groupe de paramètres par défaut. Toutefois, vous pouvez créer un groupe de paramètres personnalisé avant de créer un nouveau cluster, puis l'associer au cluster. Une alternative consiste à modifier le groupe de paramètres qui sera associé au cluster créé. Vous devez également activer la sensibilité à la casse pour le groupe de paramètres lorsque vous créez le groupe de paramètres personnalisé ou lorsque vous modifiez un groupe actuel pour utiliser des intégrations zéro ETL.

Pour créer un groupe de paramètres personnalisé à l'aide de la console Amazon Redshift ou de la AWS CLI, voir Création d'un groupe de paramètres.

Activation de la sensibilité à la casse pour votre entrepôt des données

Vous pouvez attacher un groupe de paramètres et activer la sensibilité à la casse pour un cluster provisionné lors de sa création. Toutefois, vous pouvez mettre à jour un groupe de travail sans serveur via l' AWS Command Line Interface (AWS CLI) uniquement après sa création. Cela est nécessaire pour tenir compte de la sensibilité de la casse des tables et des colonnes sources. `enable_case_sensitive_identifier` est une valeur de configuration qui détermine si les identifiants de nom de bases de données, de tables et de colonnes sont sensibles à la casse. Ce paramètre doit être activé pour créer des intégrations zéro ETL dans l'entrepôt des données. Pour plus d'informations, consultez enable_case_sensitive_identifier.

Pour Amazon Redshift sans serveur : Activez la sensibilité majuscules/minuscules pour Amazon Redshift Serverless à l'aide du AWS CLI. Notez que vous pouvez activer la sensibilité à la casse pour Amazon Redshift sans serveur uniquement à partir d' AWS CLI.

Pour les clusters provisionnés Amazon Redshift, activez la sensibilité à la casse pour votre cluster cible en utilisant l'une des rubriques suivantes :

- Activation de la sensibilité à la casse pour les clusters alloués Amazon Redshift à l’aide de la console Amazon Redshift
- Activez la sensibilité majuscules/minuscules pour les clusters provisionnés par Amazon Redshift à l'aide du AWS CLI

Activez la sensibilité majuscules/minuscules pour Amazon Redshift Serverless à l'aide du AWS CLI

Exécutez la AWS CLI commande suivante pour activer la sensibilité majuscules/minuscules pour votre groupe de travail.

```
aws redshift-serverless update-workgroup \
        --workgroup-name target-workgroup \
        --config-parameters
 parameterKey=enable_case_sensitive_identifier,parameterValue=true
```

Attendez que le statut du groupe de travail soit `Active` avant de passer à l’étape suivante.

Activation de la sensibilité à la casse pour les clusters alloués Amazon Redshift à l’aide de la console Amazon Redshift

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le volet de navigation de gauche, choisissez Tableau de bord des clusters alloués.
3. Choisissez le cluster alloué dans lequel vous souhaitez répliquer les données.
4. Dans le volet de navigation de gauche, choisissez Configurations > Gestion de la charge de travail.
5. Sur la page de gestion de la charge de travail, choisissez le groupe de paramètres.
6. Sélectionnez l’onglet Paramètres.
7. Choisissez Modifier les paramètres, puis modifiez enable_case_sensitive_identifier en spécifiant true.
8. Ensuite, choisissez Enregistrer.

Activez la sensibilité majuscules/minuscules pour les clusters provisionnés par Amazon Redshift à l'aide du AWS CLI

1. Comme vous ne pouvez pas modifier le groupe de paramètres par défaut, exécutez la AWS CLI commande suivante à partir du programme de votre terminal pour créer un groupe de paramètres personnalisé. Vous l'associerez ultérieurement au cluster provisionné.

```
aws redshift create-cluster-parameter-group \
    --parameter-group-name zero-etl-params \
    --parameter-group-family redshift-2.0 \
    --description "Param group for zero-ETL integrations"
```

2. Exécutez la AWS CLI commande suivante pour activer la sensibilité majuscules/minuscules pour le groupe de paramètres.

```
aws redshift modify-cluster-parameter-group \
    --parameter-group-name zero-etl-params \
    --parameters ParameterName=enable_case_sensitive_identifier,ParameterValue=true
```

3. Exécutez la commande suivante pour associer le groupe de paramètres au cluster.

```
aws redshift modify-cluster \
    --cluster-identifier target-cluster \
    --cluster-parameter-group-name zero-etl-params
```

4. Attendez que le cluster provisionné soit disponible. Vous pouvez vérifier le statut du cluster à l'aide de la commande `describe-cluster`. Ensuite, exécutez la commande suivante pour redémarrer le cluster.

```
aws redshift reboot-cluster \
    --cluster-identifier target-cluster
```

Configuration de l'autorisation pour votre entrepôt des données Amazon Redshift

Pour répliquer les données à partir de votre source d'intégration dans votre entrepôt des données Amazon Redshift, vous devez initialement ajouter les deux entités suivantes :

- Principal autorisé : identifie l’utilisateur ou le rôle qui peut créer des intégrations zéro ETL dans l’entrepôt des données.
- Source d’intégration autorisée : identifie la base de données source qui peut mettre à jour l’entrepôt des données.

Vous pouvez configurer les principaux autorisés et les sources d’intégration autorisées à partir de l’onglet Politique en matière de ressources dans la console Amazon Redshift ou à l’aide de l’opération d’API Amazon Redshift `PutResourcePolicy`.

Ajout de principaux autorisés

Pour créer une intégration zéro ETL dans votre groupe de travail Redshift sans serveur ou votre cluster alloué, autorisez l’accès à l’espace de noms ou au cluster alloué associé.

Vous pouvez ignorer cette étape si les deux conditions suivantes sont remplies :

- Le Compte AWS propriétaire du groupe de travail Redshift Serverless ou du cluster provisionné possède également la base de données source.
- Ce principal est associé à une politique IAM basée sur l’identité qui détient les autorisations permettant de créer des intégrations zéro ETL dans cet espace de noms Redshift sans serveur ou ce cluster alloué.

Ajout de principaux autorisés à un espace de noms Amazon Redshift sans serveur

1. Dans la console Amazon Redshift, dans le volet de navigation de gauche, choisissez Redshift sans serveur.
2. Choisissez Configuration d’espace de noms, puis choisissez votre espace de noms et accédez à l’onglet Politique en matière de ressources.
3. Choisissez Ajouter des principaux autorisés.
4. Pour chaque principal autorisé que vous souhaitez ajouter, entrez dans l'espace de noms soit l'ARN de l' AWS utilisateur ou du rôle, soit l'ID de l'utilisateur Compte AWS auquel vous souhaitez accorder l'accès pour créer des intégrations sans ETL. Un ID de compte est stocké sous forme d’ARN.
5. Sélectionnez Enregistrer les modifications.

Ajout de principaux autorisés à un cluster alloué Amazon Redshift

1. Dans la console Amazon Redshift, dans le volet de navigation de gauche, choisissez Tableau de bord des clusters alloués.
2. Choisissez Clusters, puis choisissez le cluster et accédez à l'onglet Politique en matière de ressources.
3. Choisissez Ajouter des principaux autorisés.
4. Pour chaque principal autorisé que vous souhaitez ajouter, entrez dans le cluster soit l'ARN de l' AWS utilisateur ou du rôle, soit l'ID de l'utilisateur Compte AWS auquel vous souhaitez accorder l'accès pour créer des intégrations zéro ETL. Un ID de compte est stocké sous forme d'ARN.
5. Sélectionnez Enregistrer les modifications.

Ajout de sources d'intégration autorisées

Pour permettre à votre source de mettre à jour votre entrepôt des données Amazon Redshift, vous devez l'ajouter en tant que source d'intégration autorisée à l'espace de noms.

Ajout d'une source d'intégration autorisée à un espace de noms Amazon Redshift sans serveur

1. Dans la console Amazon Redshift, accédez à Tableau de bord sans serveur.
2. Choisissez le nom de l'espace de noms.
3. Accédez à l'onglet Politique en matière de ressources.
4. Choisissez Ajouter une source d'intégration autorisée.
5. Spécifiez l'ARN de la source pour l'intégration zéro ETL.

> **Note**
>
> La suppression d'une source d'intégration autorisée empêche la réplication des données dans l'espace de noms. Cette action désactive toutes les intégrations zéro ETL de cette source dans cet espace de noms.

Ajout d'une source d'intégration autorisée à un cluster alloué Amazon Redshift

1. Dans la console Amazon Redshift, accédez à Tableau de bord des clusters alloués.

2. Choisissez le nom du cluster alloué.
3. Accédez à l'onglet Politique en matière de ressources.
4. Choisissez Ajouter une source d'intégration autorisée.
5. Spécifiez l'ARN de la source qui est la source de données pour l'intégration zéro ETL.

> **Note**
>
> La suppression d'une source d'intégration autorisée empêche la réplication des données dans le cluster alloué. Cette action désactive toutes les intégrations zéro ETL de cette source dans ce cluster provisionné Amazon Redshift.

Configuration de l'autorisation à l'aide de l'API Amazon Redshift

Vous pouvez utiliser les opérations d'API Amazon Redshift pour configurer les politiques de ressources qui fonctionnent avec les intégrations zéro ETL.

Pour contrôler la source susceptible de créer une intégration entrante dans l'espace de noms, créez une politique de ressources et attachez-la à l'espace de noms. Avec la politique de ressources, vous pouvez spécifier la source qui a accès à l'intégration. La politique de ressources est attachée à l'espace de noms de votre entrepôt des données cible pour permettre à la source de créer une intégration entrante afin de répliquer les données en direct de la source vers Amazon Redshift.

Voici un exemple de politique de ressources.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "redshift:AuthorizeInboundIntegration",
      "Resource": "arn:aws:redshift-serverless:us-east-1:123456789012:namespace/
cc4ffe56-ad2c-4fd1-a5a2-f29124a56433",
      "Condition": {
        "StringEquals": {
```

```
          "aws:SourceArn": "arn:aws:rds:us-east-1:111122223333:cluster:foo"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "redshift:CreateInboundIntegration",
      "Resource": "arn:aws:redshift-serverless:us-east-1:123456789012:namespace/
cc4ffe56-ad2c-4fd1-a5a2-f29124a56433"
    }
  ]
}
```

Voici un résumé des opérations d'API Amazon Redshift applicables à la configuration des politiques de ressources pour les intégrations :

- Utilisez l'opération PutResourcePolicy d'API pour conserver la politique de ressources. Lorsque vous fournissez une autre politique de ressources, la politique de ressources précédente appliquée à la ressource est remplacée. Utilisez l'exemple de politique de ressources précédent, qui accorde des autorisations pour les actions suivantes :
  - `CreateInboundIntegration` : permet au principal source de créer une intégration entrante pour les données à répliquer de la source vers l'entrepôt des données cible.
  - `AuthorizeInboundIntegration` : permet à Amazon Redshift de vérifier en permanence que l'entrepôt des données cible peut recevoir les données répliquées depuis l'ARN source.
- Utiliser l'opération GetResourcePolicy API consiste à afficher les politiques de ressources existantes.
- Utilisez l'opération DeleteResourcePolicy d'API pour supprimer une politique de ressource de la ressource.

Pour mettre à jour une politique de ressources, vous pouvez également utiliser la commande AWS CLI put-resource-policy. Par exemple, pour définir une politique de ressources sur l'ARN de votre espace de noms Amazon Redshift pour une source DynamoDB, exécutez une AWS CLI commande similaire à la suivante.

```
aws redshift put-resource-policy \
--policy file://rs-rp.json \
```

```
--resource-arn "arn:aws:redshift-serverless:us-east-1:123456789012:namespace/cc4ffe56-
ad2c-4fd1-a5a2-f29124a56433"
```

Où `rs-rp.json` contient :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "redshift.amazonaws.com"
            },
            "Action": "redshift:AuthorizeInboundIntegration",
            "Resource": "arn:aws:redshift-serverless:us-
east-1:123456789012:namespace/cc4ffe56-ad2c-4fd1-a5a2-f29124a56433",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:dynamodb:us-
east-1:123456789012:table/test_ddb"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:root"
            },
            "Action": "redshift:CreateInboundIntegration",
            "Resource": "arn:aws:redshift-serverless:us-
east-1:123456789012:namespace/cc4ffe56-ad2c-4fd1-a5a2-f29124a56433"
        }
    ]
}
```

Création d’une intégration zéro ETL

Vous devez d’abord créer une intégration zéro ETL pour répliquer vos données source vers Amazon Redshift.

La source de vos données détermine le type d'intégration zéro ETL à créer.

Rubriques

- Création d'une intégration zéro ETL pour Aurora
- Création d'une intégration zéro ETL pour Amazon RDS
- Création d'une intégration zéro ETL pour DynamoDB
- Créer une intégration zéro ETL aux applications

Création d'une intégration zéro ETL pour Aurora

Dans cette étape, vous créez une intégration zéro ETL d'Aurora à Amazon Redshift

Pour créer une intégration zéro ETL d'Aurora à Amazon Redshift

1. À partir de la console Amazon RDS, créez un groupe de paramètres de cluster de bases de données personnalisé, comme décrit dans le Guide de l'utilisateur Amazon Aurora.
2. À partir de la console Amazon RDS, créez un cluster de bases de données Amazon Aurora source, comme décrit dans le Guide de l'utilisateur Amazon Aurora.
3. À partir de la console Amazon Redshift : Création et configuration d'un entrepôt des données Amazon Redshift cible.
   - Depuis la console AWS CLI ou Amazon Redshift :Activation de la sensibilité à la casse pour votre entrepôt des données.
   - À partir de la console Amazon Redshift : Configuration de l'autorisation pour votre entrepôt des données Amazon Redshift.
4. À partir de la console Amazon RDS, créez une intégration zéro ETL, comme décrit dans le Guide de l'utilisateur Amazon Aurora.
5. À partir de la console Amazon Redshift ou de l'éditeur de requêtes v2, créez une base de données Amazon Redshift à partir de votre intégration.

   Ensuite, interrogez et créez des vues matérialisées avec les données répliquées.

Pour des informations détaillées sur la créations d'intégrations zéro ETL Aurora, consultez Création d'intégrations zéro ETL d'Amazon Aurora à Amazon Redshift dans le Guide de l'utilisateur Amazon Aurora.

Création d'une intégration zéro ETL pour Amazon RDS

Dans cette étape, vous créez une intégration zéro ETL Amazon RDS à Amazon Redshift Redshift prend en charge les intégrations avec RDS pour MySQL, RDS pour PostgreSQL et RDS pour Oracle.

Pour créer une intégration zéro ETL d'Amazon RDS à Amazon Redshift

1. À partir de la console Amazon RDS, créez un groupe de paramètres de base de données personnalisé, comme décrit dans le Guide de l'utilisateur Amazon RDS.
2. À partir de la console Amazon RDS, créez une instance Amazon RDS source, comme décrit dans le Guide de l'utilisateur Amazon RDS.
3. À partir de la console Amazon Redshift : Création et configuration d'un entrepôt des données Amazon Redshift cible.
   - Depuis la console AWS CLI ou Amazon Redshift :Activation de la sensibilité à la casse pour votre entrepôt des données.
   - À partir de la console Amazon Redshift : Configuration de l'autorisation pour votre entrepôt des données Amazon Redshift.
4. À partir de la console Amazon RDS, créez une intégration zéro ETL, comme décrit dans le Guide de l'utilisateur Amazon RDS.
5. À partir de la console Amazon Redshift ou de l'éditeur de requêtes v2, créez une base de données Amazon Redshift à partir de votre intégration.

   Ensuite, interrogez et créez des vues matérialisées avec les données répliquées.

La console Amazon RDS propose un flux de création d'intégrations pas à pas, dans lequel vous spécifiez la base de données source et l'entrepôt des données Amazon Redshift cible. Si des problèmes surviennent, vous pouvez choisir de demander à Amazon RDS de les résoudre pour vous au lieu de les corriger manuellement dans la console Amazon RDS ou Amazon Redshift.

Pour des instructions détaillées sur la création des intégrations zéro ETL de RDS, consultez Création d'intégrations zéro ETL d'Amazon RDS à Amazon Redshift dans le Guide de l'utilisateur Amazon RDS.

Pour obtenir des instructions détaillées sur la création spécifique d'une intégration zéro ETL d'Amazon RDS pour Oracle, consultez Configuration d'une intégration zéro ETL dans le Guide de l'utilisateur Oracle Database@AWS .

Création d'une intégration zéro ETL pour DynamoDB

Avant de créer une intégration zéro ETL, passez en revue les considérations et les exigences décrites dans Considérations relatives au moment d'utiliser les intégrations zéro ETL avec Amazon Redshift. Suivez ce flux général pour créer une intégration zéro ETL entre DynamoDB et Amazon Redshift

Pour répliquer des données DynamoDB dans Amazon Redshift avec une intégration zéro ETL

1. Vérifiez que vos informations de connexion autorisent les autorisations nécessaires pour fonctionner avec les intégrations zéro ETL à Amazon Redshift et DynamoDB. Pour obtenir un exemple de politique IAM, consultez Politique IAM pour les intégrations zéro ETL DynamoDB.
2. Depuis la console DynamoDB, configurez votre table DynamoDB pour qu'elle intègre la reprise ponctuelle (PITR), les politiques de ressources, les politiques basées sur l'identité et les autorisations relatives aux clés de chiffrement, comme décrit dans le Guide du développeur Amazon DynamoDB.
3. À partir de la console Amazon Redshift : Création et configuration d'un entrepôt des données Amazon Redshift cible.
   - Depuis la console AWS CLI ou Amazon Redshift :Activation de la sensibilité à la casse pour votre entrepôt des données.
   - À partir de la console Amazon Redshift : Configuration de l'autorisation pour votre entrepôt des données Amazon Redshift.
4. À partir de la console Amazon Redshift, créez l'intégration zéro ETL comme décrit plus loin dans cette rubrique.
5. À partir de la console Amazon Redshift, créez la base de données de destination dans votre entrepôt de données Amazon Redshift. Pour plus d'informations, consultez Création de bases de données de destination dans Amazon Redshift.
6. À partir de la console Amazon Redshift, interrogez vos données répliquées dans l'entrepôt de données Amazon Redshift. Pour plus d'informations, consultez Interrogation des données répliquées dans Amazon Redshift.

Au cours de cette étape, vous pouvez créer une intégration zéro ETL d'Amazon DynamoDB à Amazon Redshift.

Amazon Redshift console

Pour créer une intégration zéro ETL d'Amazon DynamoDB à Amazon Redshift à l'aide de la console Amazon Redshift

1. Depuis la console Amazon Redshift, choisissez les Zero-ETL intégrations. Dans le volet contenant la liste des intégrations zéro ETL, choisissez Créer une intégration zéro ETL, puis Créer une intégration DynamoDB.
2. Sur les pages permettant de créer une intégration, entrez les informations relatives à l'intégration comme suit :

   - Entrez un Nom d'intégration : il s'agit d'un nom unique qui peut être utilisé pour faire référence à votre intégration.
   - Entrez une Description : elle décrit les données à répliquer de la source vers la cible.
   - Choisissez la table source DynamoDB — Une table DynamoDB peut être sélectionnée. Point-in-time la restauration (PITR) doit être activée sur la table. Seules les tables d'une taille maximale de 100 tebioctets (TiB) sont affichées. La table DynamoDB source doit être chiffrée. La source doit également disposer d'une politique de ressources avec des principaux autorisés et des sources d'intégration. Si ces règles ne sont pas correctes, l'option Effectuez les corrections pour moi s'affiche.
   - Choisissez l'entrepôt de données Amazon Redshift cible : l'entrepôt de données peut être un cluster alloué Amazon Redshift ou un groupe de travail Redshift sans serveur. Si votre Amazon Redshift cible est sur le même compte, vous pouvez sélectionner la cible. Si la cible se trouve dans un autre compte, vous devez spécifier l'ARN de l'entrepôt de données Redshift. La cible doit avoir une politique de ressources avec des principes autorisés et une source d'intégration, et le paramètre `enable_case_sensitive_identifier` défini sur true. Si vous n'avez pas les bonnes politiques de ressources sur la cible et que celle-ci se trouve dans le même compte, vous pouvez sélectionner l'option Effectuez les corrections pour moi afin d'appliquer automatiquement les politiques de ressources lors du processus de création d'intégration. Si votre cible se trouve dans un autre Compte AWS, vous devez appliquer manuellement la politique de ressources à l'entrepôt Amazon Redshift. Si votre entrepôt de données Amazon Redshift cible n'a pas l'option de groupe de paramètres correcte `enable_case_sensitive_identifier` configurée sur `true`, vous pouvez sélectionner l'option Effectuez les corrections pour moi pour mettre automatiquement à jour ce groupe de paramètres et redémarrer l'entrepôt pendant le processus de création et d'intégration.

- Entrez jusqu'à 50 Clés de balise, avec une valeur facultative : pour fournir des métadonnées supplémentaires sur l'intégration. Pour plus d'informations, consultez Étiqueter les ressources dans Amazon Redshift..
- Choisissez les options de Chiffrement : pour chiffrer l'intégration. Pour plus d'informations, consultez Chiffrement des DynamoDB intégrations avec une clé gérée par le client.

  Lorsque vous chiffrez l'intégration, vous pouvez également ajouter des Contextes de chiffrement supplémentaires. Pour plus d'informations, consultez Contexte de chiffrement.

3. Une page de révision s'affiche dans laquelle vous pouvez choisir Créer une intégration DynamoDB.
4. Une page de progression s'affiche où vous pouvez voir la progression des différentes tâches de création de l'intégration zéro ETL.
5. Une fois l'intégration créée et active, sur la page de détails de l'intégration, choisissez Se connecter à la base de données. Lorsque votre entrepôt de données Amazon Redshift a été créé pour la première fois, une base de données a également été créée. Vous devez vous connecter à n'importe quelle base de données de votre entrepôt de données cible pour créer une autre base de données pour l'intégration. Sur la page Se connecter à la base de données, déterminez si vous pouvez utiliser une connexion récente et choisissez une méthode d'Authentification. En fonction de votre méthode d'authentification, entrez les informations pour vous connecter à une base de données existante dans votre cible. Ces informations d'authentification peuvent inclure le Nom de base de données existant (généralement `dev`) et l'Utilisateur de base de données spécifié lors de la création de la base de données avec l'entrepôt de données Amazon Redshift.
6. Une fois connecté à une base de données, choisissez Création d'une base de données à partir de l'intégration pour créer la base de données qui reçoit les données de la source. Lorsque vous créez la base de données, vous fournissez l'ID d'intégration, le Nom de l'entrepôt de données et le Nom de la base de données.
7. Une fois le statut d'intégration et la base de données de destination définis sur `Active`, les données commencent à se répliquer de votre table DynamoDB vers la table cible. Lorsque vous ajoutez des données à la source, celles-ci sont répliquées automatiquement dans l'entrepôt des données Amazon Redshift cible.

AWS CLI

Pour créer une intégration Amazon DynamoDB Zero-ETL avec Amazon Redshift à l'aide de AWS CLI, utilisez la `create-integration` commande avec les options suivantes :

- `integration-name` : spécifiez le nom de l'intégration.
- `source-arn` : spécifiez l'ARN de la source DynamoDB.
- `target-arn` : spécifiez l'ARN de l'espace de noms du cluster alloué Amazon Redshift ou du groupe de travail Redshift sans serveur cible.

L'exemple suivant crée une intégration en fournissant le nom de l'intégration, l'ARN source et l'ARN cible. L'intégration n'est pas chiffrée.

```
aws redshift create-integration \
--integration-name ddb-integration \
--source-arn arn:aws:dynamodb:us-east-1:123456789012:table/books \
--target-arn arn:aws:redshift:us-east-1:123456789012:namespace:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222

{
    "Status": "creating",
    "IntegrationArn": "arn:aws:redshift:us-east-1:123456789012:integration:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Errors": [],
    "ResponseMetadata": {
        "RetryAttempts": 0,
        "HTTPStatusCode": 200,
        "RequestId": "132cbe27-fd10-4f0a-aacb-b68f10bb2bfb",
        "HTTPHeaders": {
            "x-amzn-requestid": "132cbe27-fd10-4f0a-aacb-b68f10bb2bfb",
            "date": "Sat, 24 Aug 2024 05:44:08 GMT",
            "content-length": "934",
            "content-type": "text/xml"
        }
    },
    "Tags": [],
    "CreateTime": "2024-08-24T05:44:08.573Z",
    "KMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "AdditionalEncryptionContext": {},
    "TargetArn": "arn:aws:redshift:us-east-1:123456789012:namespace:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "IntegrationName": "ddb-integration",
    "SourceArn": "arn:aws:dynamodb:us-east-1:123456789012:table/books"
}
```

L'exemple suivant crée une intégration à l'aide d'une clé gérée par le client pour le chiffrement. Avant de créer l'intégration :

- Créez une clé gérée par le client (appelée « CMCMK » dans l'exemple) dans le même compte (appelé « AccountA » dans l'exemple) dans la table DynamoDB source.
- Assurez-vous que le user/role (appelé « roleA » dans l'exemple) est utilisé pour créer l'intégration possède `kms:CreateGrant` et autorise `kms:DescribeKey` cette clé KMS.
- Ajoutez ce qui suit à la stratégie de clé.

```
{
    "Sid": "Enable RoleA to create grants with key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "RoleA-ARN"
    },
    "Action": "kms:CreateGrant",
    "Resource": "*",
    "Condition": {
        // Add "StringEquals" condition if you plan to provide additional encryption
 context
        // for the zero-ETL integration. Ensure that the key-value pairs added here
 match
        // the key-value pair you plan to use while creating the integration.
        // Remove this if you don't plan to use additional encryption context
        "StringEquals": {
            "kms:EncryptionContext:context-key1": "context-value1"
        },
        "ForAllValues:StringEquals": {
            "kms:GrantOperations": [
                "Decrypt",
                "GenerateDataKey",
                "CreateGrant"
            ]
        }
    }
},
{
    "Sid": "Enable RoleA to describe key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "RoleA-ARN"
```

```
    },
    "Action": "kms:DescribeKey",
    "Resource": "*"
},
{
    "Sid": "Allow use by RS SP",
    "Effect": "Allow",
    "Principal": {
        "Service": "redshift.amazonaws.com"
          },
    "Action": "kms:CreateGrant",
    "Resource": "*"
}
```

```
aws redshift create-integration \
--integration-name ddb-integration \
--source-arn arn:aws:dynamodb:us-east-1:123456789012:table/books \
--target-arn arn:aws:redshift:us-east-1:123456789012:namespace:a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222 \
--kms-key-id arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE33333 \
--additional-encryption-context key33=value33  // This matches the condition in the
 key policy.
         {
    "IntegrationArn": "arn:aws:redshift:us-
east-1:123456789012:integration:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "IntegrationName": "ddb-integration",
    "SourceArn": "arn:aws:dynamodb:us-east-1:123456789012:table/books",
    "SourceType": "dynamodb",
    "TargetArn": "arn:aws:redshift:us-
east-1:123456789012:namespace:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "Status": "creating",
    "Errors": [],
    "CreateTime": "2024-10-02T18:29:26.710Z",
    "KMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE33333",
    "AdditionalEncryptionContext": {
        "key33": "value33"
    },
    "Tags": []
}
```

Politique IAM pour les intégrations zéro ETL DynamoDB

Lorsque vous créez des intégrations zéro ETL, vos informations de connexion doivent être autorisées à la fois sur les actions DynamoDB et Amazon Redshift, ainsi que sur les ressources impliquées en tant que sources et cibles de l'intégration. Voici un exemple illustrant les autorisations minimales requises.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:ListTables"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:GetResourcePolicy",
                "dynamodb:PutResourcePolicy",
                "dynamodb:UpdateContinuousBackups"
            ],
            "Resource": [
            "arn:aws:dynamodb:us-east-1:111122223333:table/my-ddb-table"
            ]
        },
        {
            "Sid": "AllowRedshiftDescribeIntegration",
            "Effect": "Allow",
            "Action": [
                "redshift:DescribeIntegrations"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowRedshiftCreateIntegration",
            "Effect": "Allow",
            "Action": "redshift:CreateIntegration",
```

```
            "Resource": "arn:aws:redshift:us-east-1:111122223333:integration:*"
        },
        {
            "Sid": "AllowRedshiftModifyDeleteIntegration",
            "Effect": "Allow",
            "Action": [
                "redshift:ModifyIntegration",
                "redshift:DeleteIntegration"
            ],
            "Resource": "arn:aws:redshift:us-
east-1:111122223333:integration:<uuid>"
        },
        {
            "Sid": "AllowRedshiftCreateInboundIntegration",
            "Effect": "Allow",
            "Action": "redshift:CreateInboundIntegration",
            "Resource": "arn:aws:redshift:us-
east-1:111122223333:namespace:<uuid>"
        }
    ]
}
```

Chiffrement des DynamoDB intégrations avec une clé gérée par le client

Si vous spécifiez une clé KMS personnalisée plutôt qu'une clé Clé détenue par AWS lors de la création d'une intégration DynamoDB Zero-ETL, la politique de clé doit fournir au service Amazon Redshift un accès principal à l'action. `CreateGrant` En outre, elle doit autoriser le compte ou le rôle du demandeur à exécuter les actions `DescribeKey` et `CreateGrant`.

Les exemples d'instructions de stratégie de clé suivants illustrent les autorisations requises dans votre stratégie. Certains exemples incluent des clés contextuelles pour réduire davantage la portée des autorisations.

Exemples d'instructions de stratégie de clé

L'instruction de stratégie suivante permet au compte ou au rôle demandeur de récupérer des informations sur une clé KMS.

```
{
   "Effect":"Allow",
   "Principal":{
      "AWS":"arn:aws:iam::{account-ID}:role/{role-name}"
```

```
   },
   "Action":"kms:DescribeKey",
   "Resource":"*"
}
```

L'instruction de stratégie suivante permet au compte ou au rôle demandeur d'ajouter une autorisation à une clé KMS. La clé de condition `kms:ViaService` limite l'utilisation de la clé KMS aux requêtes provenant d'Amazon Redshift.

```
{
   "Effect":"Allow",
   "Principal":{
      "AWS":"arn:aws:iam::{account-ID}:role/{role-name}"
   },
   "Action":"kms:CreateGrant",
   "Resource":"*",
   "Condition":{
      "StringEquals":{
         "kms:EncryptionContext:{context-key}":"{context-value}",
         "kms:ViaService":"redshift.{region}.amazonaws.com"
      },
      "ForAllValues:StringEquals":{
         "kms:GrantOperations":[
            "Decrypt",
            "GenerateDataKey",
            "CreateGrant"
         ]
      }
   }
}
```

L'instruction de stratégie suivante autorise le principal du service Amazon Redshift à ajouter une autorisation à une clé KMS.

```
{
   "Effect":"Allow",
   "Principal":{
      "Service":"redshift.amazonaws.com"
   },
   "Action":"kms:CreateGrant",
   "Resource":"*",
   "Condition":{
```

```
      "StringEquals":{
         "kms:EncryptionContext:{context-key}":"{context-value}",
         "aws:SourceAccount":"{account-ID}"
      },
      "ForAllValues:StringEquals":{
         "kms:GrantOperations":[
            "Decrypt",
            "GenerateDataKey",
            "CreateGrant"
         ]
      },
      "ArnLike":{
         "aws:SourceArn":"arn:aws:*:{region}:{account-ID}:integration:*"
      }
   }
}
```

Pour plus d'informations, consultez Création d'une stratégie de clé dans le Guide du développeur AWS Key Management Service .

Contexte de chiffrement

Lorsque vous chiffrez une intégration zéro ETL, vous pouvez ajouter des paires clé-valeur en tant que contexte de chiffrement supplémentaire. Vous souhaiterez peut-être ajouter ces paires clé-valeur pour ajouter des informations contextuelles supplémentaires sur les données répliquées. Consultez Contexte de chiffrement dans le AWS Key Management Service guide du développeur pour en savoir plus.

Amazon Redshift ajoute les paires de contextes de chiffrement suivantes en plus de celles que vous ajoutez :

- `aws:redshift:integration:arn` - `IntegrationArn`
- `aws:servicename:id` - `Redshift`

Cela réduit le nombre total de paires que vous pouvez ajouter de 8 à 6 et contribue à la limite de caractères globale de la contrainte de subvention. Pour plus d'informations, consultez Utilisation des contraintes d'octroi dans le Guide du développeur AWS Key Management Service .

Créer une intégration zéro ETL aux applications

Au cours de cette étape, vous pouvez créer une intégration zéro ETL aux applications avec Amazon Redshift.

Pour créer une intégration zéro ETL aux applications avec Amazon Redshift

1. À partir de la console Amazon Redshift : Création et configuration d'un entrepôt des données Amazon Redshift cible.
   - Depuis la console AWS CLI ou Amazon Redshift :Activation de la sensibilité à la casse pour votre entrepôt des données.
   - À partir de la console Amazon Redshift : Configuration de l'autorisation pour votre entrepôt des données Amazon Redshift.
2. Depuis la AWS Glue console : Création d'une intégration comme décrit dans le Guide du AWS Glue développeur.
3. Une fois que la base de données de destination a été créée et que les données ont commencé à se répliquer, vous pouvez interroger et créer des données matérialisées pour vos données répliquées. Pour de plus amples informations, veuillez consulter Interrogation des données répliquées dans Amazon Redshift.

Pour obtenir des informations détaillées sur la création d'intégrations sans ETL avec des applications, consultez la section Zero-ETL Intégrations dans le Guide du AWS Glue développeur.

Création de bases de données de destination dans Amazon Redshift

Pour répliquer des données de votre source vers Amazon Redshift, vous devez créer une base de données à partir de votre intégration dans Amazon Redshift.

Connectez-vous à votre groupe de travail Redshift sans serveur ou à votre cluster provisionné et créez une base de données avec une référence à votre identifiant d'intégration. Cet identifiant est la valeur renvoyée pour `integration_id` lorsque vous interrogez la vue SVV_INTEGRATION.

> **Important**
>
> Avant de créer une base de données à partir de votre intégration, votre intégration zéro ETL doit être créée et présenter l'état `Active` dans la console Amazon Redshift.

Avant de commencer à répliquer des données de votre source vers Amazon Redshift, créez une base de données à partir de l'intégration dans Amazon Redshift. Vous pouvez créer la base de données à l'aide de la console Amazon Redshift ou de l'éditeur de requêtes v2.

Amazon Redshift console

1. Dans le volet de navigation de gauche, choisissez Zero-ETL intégrations.
2. Dans la liste des intégrations, choisissez une intégration.
3. Si vous utilisez un cluster provisionné, vous devez commencer par vous connecter à la base de données. Choisissez Connect to database (Se connecter à la base de données). Vous pouvez vous connecter en utilisant une connexion récente ou en créant une nouvelle connexion.
4. Pour créer une base de données à partir de l'intégration, choisissez Créer une base de données à partir de l'intégration.
5. Entrez un Nom de base de données de destination. L'ID d'intégration et le Nom de l'entrepôt de données sont préremplis.

   Pour Aurora PostgreSQL, RDS pour PostgreSQL, RDS pour Oracle ou Oracle Database@AWS sources, entrez la base de données nommée Source que vous avez spécifiée lors de la création de votre intégration Zero-ETL. Dans ces cas, vous pouvez mapper un maximum de 100 bases de données sources aux bases de données Amazon Redshift.
6. Choisissez Créer une base de données.

Amazon Redshift query editor v2

1. Accédez à la console Amazon Redshift et choisissez Éditeur de requête v2.
2. Dans le volet de gauche, choisissez votre groupe de travail Amazon Redshift sans serveur ou votre cluster provisionné Amazon Redshift, puis connectez-vous à celui-ci.

3. Pour obtenir l'ID d'intégration, accédez à la liste des intégrations sur la console Amazon Redshift.

   Vous pouvez également exécuter la commande suivante pour obtenir la valeur de `integration_id` :

   ```
   SELECT integration_id FROM SVV_INTEGRATION;
   ```

4. Exécutez ensuite la commande suivante pour créer la base de données. En spécifiant l'ID d'intégration, vous créez une connexion entre la base de données et votre source.

   Remplacez `integration_id` par la valeur renvoyée par la commande précédente.

   ```
   CREATE DATABASE destination_db_name FROM INTEGRATION 'integration_id';
   ```

   Pour Aurora PostgreSQL, RDS pour PostgreSQL, RDS pour Oracle ou les Oracle Database@AWS sources, vous devez également inclure une référence à la base de données nommée dans l'instance ou le cluster source que vous avez spécifié lors de la création de l'intégration. Par exemple :

   ```
   CREATE DATABASE "destination_db_name" FROM INTEGRATION 'integration_id'
    DATABASE "named_db";
   ```

Pour plus d'informations sur la création d'une base de données pour une cible d'intégration zéro ETL, consultez CREATE DATABASE dans le Guide du développeur de base de données Amazon Redshift. Vous pouvez utiliser ALTER DATBASE pour modifier les paramètres de base de données tels que REFRESH INTERVAL. Pour plus d'informations sur la modification d'une base de données pour une cible d'intégration zéro ETL, consultez ALTER DATABASE dans le Guide du développeur de base de données Amazon Redshift.

> **Note**
>
> Seule votre source d'intégration peut mettre à jour les données de la base de données que vous créez à partir de votre intégration. Pour modifier le schéma d'une table, exécutez les commandes DDL ou DML sur les tables de la source. Vous pouvez exécuter des commandes DDL et DML sur des tables de la source, mais vous pouvez uniquement exécuter des commandes DDL et des requêtes en lecture seule sur la base de données de destination.

Pour en savoir plus sur l'affichage du statut d'une base de données de destination, consultez Affichage des intégrations zéro ETL.

Après avoir créé une base de données de destination, vous pouvez ajouter des données à votre source. Pour ajouter des données à votre source, consultez l'une des rubriques suivantes :

- Pour les sources Aurora, consultez Ajouter des données au cluster de base de données source dans le Guide de l'utilisateur Amazon Aurora.
- Pour les sources Amazon RDS, consultez Ajout de données à l'instance de base de données source dans le Guide de l'utilisateur Amazon RDS.
- Pour les sources DynamoDB, consultez Mise en route avec DynamoDB dans le Guide du développeur Amazon DynamoDB.
- Pour les intégrations sans ETL avec les sources d'applications, consultez la section Zero-ETL Intégrations dans le Guide du AWS Glue développeur.

Interrogation des données répliquées dans Amazon Redshift

Une fois que vous avez ajouté des données à votre source, celles-ci sont répliquées en temps quasi réel dans l'entrepôt des données Amazon Redshift et elles sont prêtes à être interrogées. Pour plus d'informations sur les métriques d'intégration et les statistiques de table, consultez Métriques pour les intégrations zéro ETL.

> **Note**
>
> Étant donné qu'une base de données est identique à un schéma dans MySQL, le niveau de base de données MySQL correspond au niveau de schéma Amazon Redshift. Notez cette différence de mappage lorsque vous interrogez des données répliquées depuis Aurora MySQL ou RDS for MySQL.

Pour interroger des données répliquées

1. Accédez à la console Amazon Redshift et choisissez Éditeur de requête v2.
2. Connectez-vous à votre groupe de travail Amazon Redshift sans serveur ou à votre cluster provisionné Amazon Redshift, et choisissez votre base de données dans la liste déroulante.

3. Utilisez une instruction SELECT pour sélectionner toutes les données du schéma et de la table que vous avez créées dans la source. Pour appliquer la sensibilité à la casse, utilisez des guillemets doubles (« ») pour les noms de schéma, de table et de colonne. Par exemple :

```
SELECT * FROM "schema_name"."table_name";
```

   Vous pouvez également interroger les données à l'aide de l'API de données Amazon Redshift.

Interrogation de données répliquées avec des vues matérialisées

Vous pouvez créer des vues matérialisées dans votre base de données Amazon Redshift locale afin de transformer les données répliquées via des intégrations zéro ETL. Connectez-vous à votre base de données locale et utilisez des requêtes entre bases de données pour accéder aux bases de données de destination. Vous pouvez utiliser des noms d'objet entièrement qualifiés avec la notation en trois parties (destination-database-name.schema-name.table-name) ou créer un schéma externe faisant référence à la paire de base de données et de schéma de destination et utiliser la notation en deux parties (external-schema-name.table-name). Pour plus d'informations sur les requêtes entre bases de données, consultez Interrogation des données de plusieurs bases de données.

Utilisez l'exemple suivant pour créer et insérer des exemples de données dans les *event_zetl* tableaux *sales_zetl* et à partir de la source*tickit_zetl*. Les tables sont répliquées dans la base de données Amazon Redshift. *zetl_int_db*

```
CREATE TABLE sales_zetl (
        salesid integer NOT NULL primary key,
        eventid integer NOT NULL,
        pricepaid decimal(8, 2)
);

CREATE TABLE event_zetl (
        eventid integer NOT NULL PRIMARY KEY,
        eventname varchar(200)
);

INSERT INTO sales_zetl VALUES(1, 1, 3.33);
INSERT INTO sales_zetl VALUES(2, 2, 4.44);
INSERT INTO sales_zetl VALUES(3, 2, 5.55);

INSERT INTO event_zetl VALUES(1, "Event 1");
```

```
INSERT INTO event_zetl VALUES(2, "Event 2");
```

Vous pouvez créer une vue matérialisée pour obtenir le total des ventes par événement à l'aide de la notation en trois parties :

```
--three part notation zetl-database-name.schema-name.table-name
CREATE MATERIALIZED VIEW mv_transformed_sales_per_event_3p
AUTO REFRESH YES
AS
(SELECT eventname, sum(pricepaid) as total_price
FROM  zetl_int_db.tickit_zetl.sales_zetl S, zetl_int_db.tickit_zetl.event_zetl E
WHERE S.eventid = E.eventid
GROUP BY 1);
```

Vous pouvez créer une vue matérialisée pour obtenir le total des ventes par événement à l'aide de la notation en deux parties :

```
--two part notation external-schema-name.table-name notation
CREATE EXTERNAL schema ext_tickit_zetl
FROM REDSHIFT
DATABASE zetl_int_db
SCHEMA tickit_zetl;

CREATE MATERIALIZED VIEW mv_transformed_sales_per_event_2p
AUTO REFRESH YES
AS
(
    SELECT eventname, sum(pricepaid) as total_price
    FROM  ext_tickit_zetl.sales_zetl S, ext_tickit_zetl.event_zetl E
    WHERE S.eventid = E.eventid
    GROUP BY 1
);
```

Pour visualiser les vues matérialisées que vous avez créées, utilisez l'exemple suivant.

```
SELECT * FROM mv_transformed_sales_per_event_3p;

+-----------+-------------+
| eventname | total_price |
+-----------+-------------+
| Event 1   | 3.33        |
| Event 2   | 9.99        |
```

```
+-----------+-------------+

SELECT * FROM mv_transformed_sales_per_event_2p;

+-----------+-------------+
| eventname | total_price |
+-----------+-------------+
| Event 1   | 3.33        |
| Event 2   | 9.99        |
+-----------+-------------+
```

Interrogation des données répliquées à partir de DynamoDB

Lorsque vous répliquez des données depuis Amazon DynamoDB vers une base de données Amazon Redshift, elles sont stockées dans une vue matérialisée dans une colonne de données de type SUPER.

Pour cet exemple, les données suivantes sont stockées dans DynamoDB.

```
{
    "key1": {
        "S": "key_1"
    },
    "key2": {
        "N": 0
    },
    "payload": {
        "L": [
            {
                "S": "sale1"
            },
            {
                "S": "sale2"
            },
        ]
    },
}
```

La vue matérialisée Amazon Redshift est définie comme suit.

```
CREATE MATERIALIZED VIEW mv_sales
                    BACKUP NO
```

```
                    AUTO REFRESH YES
                    AS
                    SELECT "value"."payload"."L"[0]."S"::VARCHAR AS first_payload
                    FROM public.sales;
```

Pour afficher les données dans la vue matérialisée, exécutez une commande SQL.

```
SELECT first_payload FROM mv_sales;
```

Affichage des intégrations zéro ETL

Vous pouvez consulter vos intégrations zéro ETL depuis la console Amazon Redshift. Vous pouvez y consulter ses informations de configuration et son état actuel, et ouvrir des écrans pour interroger et partager des données.

Amazon Redshift console

Pour afficher les détails d'une intégration zéro ETL

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le panneau de navigation de gauche, choisissez Sans serveur ou Tableau de bord des clusters alloués. Choisissez ensuite les Zero-ETL intégrations.
3. Sélectionnez l'intégration zéro ETL que vous souhaitez consulter. Pour chaque intégration, les informations suivantes sont fournies :

   - ID d'intégration correspond à l'identifiant renvoyé lors de la création de l'intégration.
   - Statut peut avoir l'une des valeurs suivantes :
     - `Active` : l'intégration zéro ETL envoie des données transactionnelles à l'entrepôt des données Amazon Redshift cible.
     - `Syncing` : l'intégration zéro ETL a rencontré une erreur récupérable et réensemence les données. Les tables concernées ne peuvent pas être interrogées dans Amazon Redshift tant que leur resynchronisation n'est pas terminée.
     - `Failed` : l'intégration zéro ETL a rencontré un événement ou une erreur irrécupérable qui ne peut pas être corrigé. Vous devez supprimer et recréer l'intégration zéro ETL.
     - `Creating` : l'intégration zéro ETL est en cours de création.
     - `Deleting` : l'intégration zéro ETL est en cours de suppression.

    - `Needs attention` : l'intégration zéro ETL a rencontré un événement ou une erreur nécessitant une intervention manuelle pour être résolu. Pour corriger le problème, suivez les instructions du message d'erreur.
- Le type de source est le type de données source répliquées vers la cible. Les types peuvent spécifier d'autres gestionnaires de bases de données, tels que Aurora MySQL-Compatible Edition, Amazon Aurora PostgreSQL, RDS pour MySQL et from applications ()`GlueSAAS`.
- ARN source est l'ARN des données source. Pour la plupart des sources, il s'agit de l'ARN de la base de données ou table source. Pour une intégration sans ETL avec les sources d'applications, il s'agit de l'ARN de l'objet de AWS Glue connexion.
- Cible est l'espace de noms de l'entrepôt de données Amazon Redshift recevant les données sources.
- Base de données peut avoir les valeurs suivantes :
    - `No database` : il n'existe aucune base de données de destination pour l'intégration.
    - `Creating` : Amazon Redshift est en train de créer la base de données de destination pour l'intégration.
    - `Active` : les données sont en cours de réplication depuis la source d'intégration vers Amazon Redshift.
    - `Error` : une erreur s'est produite lors de l'intégration.
    - `Recovering` : l'intégration est en cours de récupération après le redémarrage de l'entrepôt des données.
    - `Resyncing` : Amazon Redshift est en train de resynchroniser les tables de l'intégration.
- Type de cible est le type d'entrepôt de données Amazon Redshift.
- Date de création est la date et l'heure (UTC) de la création de l'intégration.

> **Note**
>
> Pour afficher les détails de l'intégration d'un entrepôt de données, choisissez la page de détails de votre cluster provisionné ou de votre espace de noms sans serveur, puis choisissez l'Zero-ETL onglet Intégrations.

Dans la liste Zero-ETL des intégrations, vous pouvez choisir Query data pour accéder à l'éditeur de requêtes Amazon Redshift v2. Le paramètre enable_case_sensitive_identifier de la

base de données cible Amazon Redshift est activé. Lorsque vous écrivez du code SQL, vous pouvez avoir besoin d'entourer les schémas, les tables et les noms de colonnes de guillemets doubles ("<nom>"). Pour plus d'informations sur l'interrogation des données dans votre entrepôt des données Amazon Redshift, consultez Interrogation d'une base de données à l'aide de l'éditeur de requête v2.

Dans la liste Zero-ETL des intégrations, vous pouvez choisir Partager les données pour créer un partage de données. Pour créer une unité de partage des données pour la base de données Amazon Redshift, suivez les instructions de la page Créer une unité de partage des données. Avant de pouvoir partager les données dans votre base de données Amazon Redshift, vous devez d'abord créer une base de données de destination. Pour plus d'informations sur le partage des données, consultez Concepts du partage de données pour Amazon Redshift.

Pour actualiser votre intégration, vous pouvez utiliser la commande ALTER DATABASE. Cela permet de répliquer toutes les données de votre source d'intégration dans votre base de données de destination. L'exemple suivant actualise toutes les tables synchronisées et défaillantes au sein de votre intégration zéro ETL.

```
ALTER DATABASE sample_integration_db INTEGRATION REFRESH ALL tables;
```

AWS CLI

Pour décrire une intégration Amazon DynamoDB Zero-ETL avec Amazon Redshift à l'aide de AWS CLI, utilisez la `describe-integrations` commande avec les options suivantes :

- `integration-arn` : spécifiez l'ARN de l'intégration DynamoDB à décrire.
- `integration-name` : spécifiez un filtre facultatif qui indique une ou plusieurs ressources à renvoyer.

L'exemple suivant décrit une intégration en fournissant l'ARN de l'intégration.

```
aws redshift describe-integrations

{
    "Integrations": [
        {
            "Status": "failed",
            "IntegrationArn": "arn:aws:redshift:us-
east-1:123456789012:integration:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
            "Errors": [
                {
                    "ErrorCode": "INVALID_TABLE_PERMISSIONS",
                    "ErrorMessage": "Redshift does not have sufficient access on the
 table key. Refer to the Amazon DynamoDB Developer Guide."
                }
            ],
            "Tags": [],
            "CreateTime": "2023-11-09T00:32:46.444Z",
            "KMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE33333",
            "TargetArn": "arn:aws:redshift:us-
east-1:123456789012:namespace:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "IntegrationName": "ddb-to-provisioned-02",
            "SourceArn": "arn:aws:dynamodb:us-east-1:123456789012:table/mytable"
        }
    ]
}
```

Vous pouvez également filtrer les résultats de `describe-integrations` par `integration-arn`, `source-arn`, `source-types` ou `status`. Pour plus d'informations, consultez describe-integrations dans le Guide de la CLI Amazon Redshift.

Mode historique

Avec le mode historique, vous pouvez configurer vos intégrations zéro ETL pour suivre chaque version (y compris les mises à jour et les suppressions) de vos enregistrements dans les tables sources, directement dans Amazon Redshift. Vous pouvez exécuter des analyses avancées sur toutes vos données, par exemple exécuter une analyse historique, créer des rapports rétrospectifs, effectuer une analyse des tendances et envoyer des mises à jour incrémentielles aux applications en aval basées sur Amazon Redshift. Le mode historique est pris en charge par plusieurs intégrations zéro ETL d'Amazon Redshift, notamment Amazon Aurora PostgreSQL, Amazon RDS for MySQL et Amazon DynamoDB. Le mode historique est également pris en charge par plusieurs applications, telles que Salesforce ServiceNow, SAP et Zendesk.

Vous pouvez activer et désactiver le mode historique pour vos intégrations Zero-ETL depuis la console Amazon Redshift (). https://console.aws.amazon.com/redshiftv2/ Utilisez le mode historique pour conserver la trace des enregistrements qui ont été supprimés ou modifiés dans la source d'intégration. Le suivi s'effectue dans l'entrepôt de données Amazon Redshift cible. L'activation du

mode historique n'a aucune incidence sur les performances des requêtes analytiques classiques sur ces tables.

Une fois le mode historique activé, les tables que vous déposez dans la source ne seront pas supprimées dans Amazon Redshift. Au lieu de cela, les tables apparaîtront dans un état `DroppedSource` et vous pourrez toujours les interroger. Vous pouvez également continuer à utiliser les commandes DROP et RENAME avec du SQL normal.

Si vous souhaitez réutiliser le même nom de table sur la source, vous devez DROP ou RENAME la table `DroppedState` correspondante avant de pouvoir la répliquer sur Amazon Redshift. Assurez-vous de le faire avant de créer la table sur la source.

Pour plus d'informations sur les éléments à prendre en compte lors de l'utilisation du mode historique, consultez Considérations relatives à l'utilisation du mode historique sur la cible.

Pour gérer le mode historique pour une intégration zéro ETL

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le panneau de navigation de gauche, choisissez Sans serveur ou Tableau de bord des clusters alloués. Choisissez ensuite les Zero-ETL intégrations.
3. Sélectionnez l'intégration zéro ETL que vous souhaitez gérer et choisissez Gérer le mode historique. La fenêtre Gérer le mode historique s'affiche.
4. Vous pouvez désactiver ou activer le mode historique pour une table cible répliquée à partir d'un type de source comportant une seule table source, comme Amazon DynamoDB. Lorsque l'intégration zéro ETL permet de créer plusieurs tables cibles, vous pouvez Désactiver pour toutes les tables existantes et futures, Activer pour toutes les tables existantes et futures ou Gérer le mode historique pour les tables individuelles. Par défaut, le mode historique est défini sur `off` lorsque l'intégration zéro ETL est créée.

   Lorsque le mode historique est défini sur `on`, les colonnes suivantes sont ajoutées à votre table cible pour suivre les modifications apportées à la source. Le mode historique défini sur `on` augmente l'utilisation et les coûts mensuels car Amazon Redshift ne supprime aucun enregistrement dans les tables cibles. Tout enregistrement source supprimé ou modifié crée un nouvel enregistrement dans la cible, ce qui augmente le nombre total de lignes dans la cible avec plusieurs versions d'enregistrement. Les enregistrements ne sont pas supprimés de la table cible lorsqu'ils sont supprimés ou modifiés dans la source. Vous pouvez gérer les tables cibles en supprimant les enregistrements inactifs.

Nom de la colonne	Type de données	Description
_record_is_active	Booléen	Indique si un enregistrement de la cible est actuellement actif dans la source. True indique que l'enregistrement est actif.
_record_create_time	Horodatage	Heure de début (UTC) à laquelle l'enregistrement source est actif.
_record_delete_time	Horodatage	Heure de fin (UTC) à laquelle l'enregistrement source est mis à jour ou supprimé.

Vous pouvez supprimer les enregistrements inactifs d'une table en mode historique en filtrant les enregistrements où la colonne `_record_is_active` est false. La commande SQL DELETE suivante supprime les enregistrements inactifs d'une table dont la colonne id est inférieure ou égale à 100. Une fois que vous avez supprimé des enregistrements, lorsque la suppression automatique est exécutée, le stockage des enregistrements supprimés est récupéré.

```
DELETE FROM myschema.mytable where not _record_is_active AND id <= 100;
```

Lorsque le mode historique est défini sur `off`, Amazon Redshift crée une copie de votre table dans la base de données cible avec les enregistrements actifs et sans les colonnes d'historique ajoutées. Amazon Redshift renomme votre table en *`table-name`*`_historical_`*`timestamp`* pour votre utilisation. Vous pouvez supprimer cette copie de votre table si vous n'en avez plus besoin. Vous pouvez renommer ces tables à l'aide de la commande ALTER TABLE. Par exemple :

```
ALTER TABLE [schema-name.]table-name_historical_timestamp RENAME TO new_table_name;
```

Pour plus d'informations, consultez ALTER TABLE dans le Guide du développeur de la base de données Amazon Redshift.

Vous pouvez également gérer le mode historique à l'aide des commandes SQL CREATE DATABASE et ALTER DATABASE. Pour plus d'informations sur la définition de HISTORY_MODE,

consultez CREATE DATABASE et ALTER DATABASE dans le Guide du développeur de base de données Amazon Redshift.

Partage de vos données dans Amazon Redshift

Une fois que vous avez ajouté des données dans la source, celles-ci sont immédiatement répliquées dans Amazon Redshift et prêtes à être partagées en créant des unités de partage des données.

Pour partager les données, vous devez d'abord créer une base de données de destination.

Pour partager des données dans Amazon Redshift sans serveur à l'aide de la console Amazon Redshift

1. Dans la console Amazon Redshift, dans le volet de navigation de gauche, choisissez Amazon Redshift sans serveur > Tableau de bord sans serveur.
2. Dans le volet de navigation de gauche, choisissez Zero-ETL intégrations.
3. Choisissez Share data (Partager les données).
4. Sur la page de création d'unités de partage de données, suivez les étapes décrites dans Création d'unités de partage des données.

Pour partager des données dans les clusters alloués Amazon Redshift à l'aide de la console Amazon Redshift

1. Dans la console Amazon Redshift, dans le volet de navigation de gauche, choisissez Tableau de bord des clusters alloués.
2. Dans le volet de navigation de gauche, choisissez Zero-ETL intégrations.
3. Dans la liste des intégrations, choisissez une intégration.
4. Sur la page des détails d'intégration, choisissez Se connecter à la base de données.
5. Sur la page Connexion à la base de données, vous pouvez créer une nouvelle connexion ou utiliser une connexion récente. Assurez-vous que la connexion est établie à la base de données de destination.
6. Si vous créez une nouvelle connexion, entrez le nom de la base de données. Cliquez ensuite sur Se connecter.
7. Sur la page des détails d'intégration, choisissez Partager les données.
8. Sur la page de création d'unités de partage de données, suivez les étapes décrites dans Création d'unités de partage des données.

Surveillance des intégrations zéro ETL

Vous pouvez surveiller vos intégrations Zero-ETL en interrogeant les vues du système ou en utilisant Amazon. EventBridge

Surveillance des intégrations zéro ETL aux vues système Amazon Redshift

Vous pouvez surveiller vos intégrations zéro ETL en interrogeant les vues système suivantes dans Amazon Redshift.

- SVV_INTEGRATION fournit des informations sur les détails de configuration des intégrations zéro ETL.
- SYS_INTEGRATION_ACTIVITY fournit des informations sur les intégrations zéro ETL terminées.
- SVV_INTEGRATION_TABLE_MAPPING fournit des informations sur le mappage des valeurs de métadonnées de la source à la cible.
- SVV_INTEGRATION_TABLE_STATE fournit des informations sur l'état de l'intégration.
- SYS_INTEGRATION_TABLE_ACTIVITY fournit des informations sur les activités d'insertion, de suppression et de mise à jour des intégrations.
- SYS_INTEGRATION_TABLE_CHANGE fournit des informations sur le journal des changements d'état des tables pour les intégrations.

Surveillance des intégrations Zéro ETL avec Amazon EventBridge

Amazon Redshift envoie des événements liés à l'intégration à Amazon. EventBridge Pour obtenir la liste des événements et leurs identifiants d'événements correspondants, consultez Zero-ETL notifications d'événements d'intégration avec Amazon EventBridge.

Métriques pour les intégrations zéro ETL

Vous pouvez utiliser les statistiques de la console Amazon Redshift et d'Amazon CloudWatch pour en savoir plus sur l'état et les performances de vos intégrations Zero-ETL. Vous pouvez ajuster les mesures pour afficher les données sur une durée plus ou moins longue, ou choisir d'afficher les mesures dans CloudWatch. Pour consulter les statistiques relatives à votre intégration sur la console Amazon Redshift, choisissez Zero-ETL les intégrations dans le volet de navigation de gauche et choisissez votre ID d'intégration.

En fonction des données source des intégrations zéro ETL, Amazon Redshift fournit des métriques sur la page de détails d'intégration pour une intégration. Les métriques possibles sont des types suivants :

- Dans l'onglet Métriques d'intégration, des graphes illustrant les éléments suivants sont disponibles :

Métrique	Nom de la métrique dans la console Amazon Redshift	Description
`IntegrationLag`	`Lag`	Délai entre le moment où les données sont validées dans votre source et le moment où les données sont disponibles pour les requêtes dans Amazon Redshift. Unités : secondes Dimensions : `IntegrationId` Fréquence de mise à jour : 60 secondes
`IntegrationNumTablesReplicated`	`Tables replicated`	Nombre de tables qui ont été répliquées depuis votre base de données source vers Amazon Redshift. Unités : nombre Dimensions : `IntegrationId` Fréquence de mise à jour : 60 secondes
`IntegrationNumTablesFailedReplication`	`Tables failed`	Nombre de tables dont la réplication a échoué. Unités : nombre Dimensions : `IntegrationId` Fréquence de mise à jour : 60 secondes

Métrique	Nom de la métrique dans la console Amazon Redshift	Description
`IntegrationDataTransferred`	`Data transferred`	Volume de données transférées en octets logiques. Unités : octets Dimensions : `IntegrationId` Fréquence de mise à jour : 60 secondes
`IntegrationLatestDetectedChange`	`Latest detected change`	Heure, en secondes d'époque Unix, à laquelle l'intégration a effectué pour la dernière fois un changement de source dans la file d'attente de réplication. Unités : secondes Dimensions : `IntegrationId` Fréquence de mise à jour : 60 secondes
`IntegrationLatestAppliedChange`	`Latest applied change`	Heure, en secondes d'époque Unix, à laquelle l'intégration a été intégrée pour la dernière fois sur Amazon Redshift. Unités : secondes Dimensions : `IntegrationId` Fréquence de mise à jour : 60 secondes

Métrique	Nom de la métrique dans la console Amazon Redshift	Description
`IntegrationDuplicateRowsDetected`	`Duplicate rows detected`	Le nombre de tableaux contenant des lignes dupliquées identifiés pendant l'intervalle de reporting. Unités : nombre Dimensions : `IntegrationId` Fréquence de mise à jour : 60 secondes
`IntegrationAutoRemediationTriggered`	`Auto-remediation triggered`	Nombre de tables que la correction automatique a déplacées vers une resynchronisation au cours de l'intervalle de génération de rapports. Unités : nombre Dimensions : `IntegrationId` Fréquence de mise à jour : 60 secondes

> **Note**
>
> Pour les intégrations qui répliquent plusieurs bases de données, les `IntegrationLatestAppliedChange` métriques `IntegrationLatestDetectedChange` et indiquent la valeur minimale pour toutes les bases de données. Il s'agit de la base de données la moins récemment mise à jour. Per-databaseles valeurs sont disponibles dans les `latest_applied_change_time` colonnes `latest_detected_change_time` et de https://docs.aws.amazon.com/redshift/latest/dg/r_SVV_INTEGRATION.html SVV_INTEGRATION.

- Dans l'onglet Statistiques de table, vous pouvez consulter la liste des tables actuellement actives ou présentant des erreurs. Les statistiques de cet onglet sont les suivantes (selon le type de source) :
  - Nom du schéma : nom du schéma où se trouve la table.

- Nom de la table : nom de la table dans la base de données source.
- Statut : statut de la table. Les valeurs possibles incluent `Synced`, `Failed`, `Deleted`, `Resync Required` et `Resync Initiated`.
- Base de données : base de données Amazon Redshift dans laquelle se trouve la table.
- Date de dernière mise à jour : date et heure (UTC) auxquelles la dernière mise à jour a été apportée à la table.
- Nombre de lignes de la table : nombre de lignes de la table.
- Taille de la table : taille de la table.

Vous pouvez également afficher un graphe du nombre de Lignes insérées, supprimées et mises à jour pour la période sélectionnée.

Modification d'une intégration zéro ETL pour DynamoDB

Au cours de cette étape, vous pouvez modifier une intégration zéro ETL de DynamoDB à Amazon Redshift.

Amazon Redshift console

Pour modifier une intégration zéro ETL d'Amazon DynamoDB à Amazon Redshift à l'aide de la console Amazon Redshift

1. Depuis la console Amazon Redshift, choisissez les Zero-ETL intégrations. Dans le volet contenant la liste des intégrations zéro ETL, choisissez l'intégration DynamoDB que vous souhaitez modifier.
2. Choisissez Modifier et apportez des modifications au Nom de l'intégration ou à la Description.
3. Choisissez Enregistrer les Modifications pour enregistrer vos Modifications.

AWS CLI

Pour modifier une intégration Amazon DynamoDB Zero-ETL avec Amazon Redshift à l'aide de AWS CLI, utilisez la `modify-integration` commande avec les options suivantes :

- `integration-arn` : spécifiez l'ARN de l'intégration DynamoDB à modifier.
- `integration-name` : spécifiez un nouveau nom pour l'intégration.
- `description` : spécifiez une nouvelle description pour l'intégration.

L'exemple suivant modifie une intégration en fournissant l'ARN de l'intégration, une nouvelle description et un nouveau nom.

```
aws redshift modify-integration \
--integration-arn arn:aws:redshift:us-
east-1:123456789012:integration:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--description "Test modify description and name together." \
--integration-name "updated-integration-name-2"

{
    "IntegrationArn": "arn:aws:redshift:us-
east-1:123456789012:integration:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "IntegrationName": "updated-integration-name-2",
    "SourceArn": "arn:aws:dynamodb:us-east-1:123456789012:table/ddb-temp-test-table-
table",
    "SourceType": "dynamodb",
    "TargetArn": "arn:aws:redshift:us-
east-1:123456789012:namespace:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "Status": "active",
    "Errors": [],
    "CreateTime": "2024-09-19T18:06:33.555Z",
    "Description": "Test modify description and name together.",
    "KMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE33333",
    "AdditionalEncryptionContext": {},
    "Tags": []
}
```

Suppression d'une intégration zéro ETL pour DynamoDB

Lorsque vous supprimez une intégration, l'entrepôt de données cible conserve toutes les données précédemment répliquées. Vous pouvez continuer à partager et à interroger ces données. Toutefois, les nouvelles données de la source ne seront pas répliquées vers la cible.

Au cours de cette étape, vous pouvez supprimer une intégration zéro ETL de DynamoDB à Amazon Redshift.

Amazon Redshift console

Pour supprimer une intégration zéro ETL d'Amazon DynamoDB à Amazon Redshift à l'aide de la console Amazon Redshift

1. Depuis la console Amazon Redshift, choisissez les Zero-ETL intégrations. Dans le volet contenant la liste des intégrations zéro ETL, choisissez l'intégration DynamoDB que vous souhaitez supprimer.
2. Choisissez Supprimer et fournissez les informations demandées.
3. Choisissez Supprimer pour supprimer l'intégration zéro ETL.

AWS CLI

Pour supprimer une intégration Amazon DynamoDB Zero-ETL avec Amazon Redshift à l'aide de AWS CLI, utilisez la `delete-integration` commande avec les options suivantes :

- `integration-arn` : spécifiez l'ARN de l'intégration DynamoDB à supprimer.

L'exemple suivant supprime une intégration en fournissant l'ARN de l'intégration.

```
aws redshift delete-integration \
--integration-arn arn:aws:redshift:us-
east-1:123456789012:integration:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111

{
    "IntegrationArn": "arn:aws:redshift:us-
east-1:123456789012:integration:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "IntegrationName": "updated-integration-name-2",
    "SourceArn": "arn:aws:dynamodb:us-east-1:123456789012:table/tidal-ddb-ddb-temp-
test-table-table",
    "SourceType": "dynamodb",
    "TargetArn": "arn:aws:redshift:us-
east-1:123456789012:namespace:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "Status": "deleting",
    "Errors": [],
    "CreateTime": "2024-09-19T18:06:33.555Z",
    "Description": "Test modify description and name together.",
    "KMSKeyId": "arn:aws:kms:us-east-1:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "AdditionalEncryptionContext": {},
```

```
    "Tags": []
}
```

Régions prises en charge pour les intégrations zéro ETL

Zero-ETL integration est une solution entièrement gérée qui rend les données transactionnelles et opérationnelles disponibles dans Amazon Redshift à partir de multiples sources opérationnelles et transactionnelles, ainsi que d'applications d'entreprise. Cette page répertorie les régions disponibles pour chaque source prise en charge.

Aurora MySQL

Les régions et versions de moteur suivantes sont disponibles pour les intégrations zéro ETL à Amazon Redshift.

Région	Aurora MySQL
Afrique (Le Cap)	Available
Asie-Pacifique (Hong Kong)	Available
Asie-Pacifique (Tokyo)	Available
Asie-Pacifique (Séoul)	Available
Asie-Pacifique (Osaka)	Available
Asie-Pacifique (Mumbai)	Available
Asie-Pacifique (Hyderabad)	Available
Asie-Pacifique (Singapour)	Available
Asie-Pacifique (Sydney)	Available
Asie-Pacifique (Jakarta)	Available
Asie-Pacifique (Melbourne)	Available
Asie-Pacifique (Malaisie)	Non disponible

Région	Aurora MySQL
Canada (Centre)	Available
Canada-Ouest (Calgary)	Available
Chine (Pékin)	Available
Chine (Ningxia)	Available
Europe (Francfort)	Available
Europe (Zurich)	Available
Europe (Stockholm)	Available
Europe (Milan)	Available
Europe (Espagne)	Available
Europe (Irlande)	Available
Europe (Londres)	Available
Europe (Paris)	Available
Israël (Tel Aviv)	Available
Moyen-Orient (EAU)	Available
Middle East (Bahrain)	Available
Amérique du Sud (São Paulo)	Available
USA Est (Virginie du Nord)	Available
USA Est (Ohio)	Available
USA Ouest (Californie du Nord)	Available
USA Ouest (Oregon)	Available

Région	Aurora MySQL
AWS GovCloud (US-East)	Non disponible
AWS GovCloud (US-West)	Non disponible

Aurora PostgreSQL

Les régions suivantes sont disponibles pour les intégrations zéro ETL Aurora PostgreSQL à Amazon Redshift.

Région	Aurora PostgreSQL
Afrique (Le Cap)	Available
Asie-Pacifique (Hong Kong)	Available
Asie-Pacifique (Tokyo)	Available
Asie-Pacifique (Séoul)	Available
Asie-Pacifique (Osaka)	Available
Asie-Pacifique (Mumbai)	Available
Asie-Pacifique (Hyderabad)	Available
Asie-Pacifique (Singapour)	Available
Asie-Pacifique (Sydney)	Available
Asie-Pacifique (Jakarta)	Available
Asie-Pacifique (Melbourne)	Available
Asie-Pacifique (Malaisie)	Available
Canada (Centre)	Available
Canada-Ouest (Calgary)	Available

Région	Aurora PostgreSQL
Chine (Pékin)	Available
Chine (Ningxia)	Available
Europe (Francfort)	Available
Europe (Zurich)	Available
Europe (Stockholm)	Available
Europe (Milan)	Available
Europe (Espagne)	Available
Europe (Irlande)	Available
Europe (Londres)	Available
Europe (Paris)	Available
Israël (Tel Aviv)	Available
Moyen-Orient (EAU)	Available
Middle East (Bahrain)	Available
Amérique du Sud (São Paulo)	Available
USA Est (Virginie du Nord)	Available
USA Est (Ohio)	Available
USA Ouest (Californie du Nord)	Available
USA Ouest (Oregon)	Available
AWS GovCloud (US-East)	Non disponible
AWS GovCloud (US-West)	Non disponible

Amazon DynamoDB

Les régions suivantes sont disponibles pour les intégrations zéro ETL DynamoDB à Amazon Redshift.

Région	DynamoDB
Afrique (Le Cap)	Available
Asie-Pacifique (Hong Kong)	Available
Asie-Pacifique (Taipei)	Available
Asie-Pacifique (Tokyo)	Available
Asie-Pacifique (Séoul)	Available
Asie-Pacifique (Osaka)	Available
Asie-Pacifique (Mumbai)	Available
Asie-Pacifique (Hyderabad)	Available
Asie-Pacifique (Singapour)	Available
Asie-Pacifique (Sydney)	Available
Asie-Pacifique (Jakarta)	Available
Asie-Pacifique (Melbourne)	Available
Asie-Pacifique (Malaisie)	Available
Asie-Pacifique (Thaïlande)	Available
Canada (Centre)	Available
Canada-Ouest (Calgary)	Available
Chine (Pékin)	Available
Chine (Ningxia)	Available

Région	DynamoDB
Europe (Francfort)	Available
Europe (Zurich)	Available
Europe (Stockholm)	Available
Europe (Milan)	Available
Europe (Espagne)	Available
Europe (Irlande)	Available
Europe (Londres)	Available
Europe (Paris)	Available
Israël (Tel Aviv)	Available
Moyen-Orient (EAU)	Available
Middle East (Bahrain)	Available
Mexique (Centre)	Available
Amérique du Sud (São Paulo)	Available
USA Est (Virginie du Nord)	Available
USA Est (Ohio)	Available
USA Ouest (Californie du Nord)	Available
USA Ouest (Oregon)	Available
AWS GovCloud (US-East)	Available
AWS GovCloud (US-West)	Available

Amazon RDS for MySQL

Les régions suivantes sont disponibles pour les intégrations Amazon RDS for MySQL sans ETL avec Amazon Redshift.

Région	RDS for MySQL
Afrique (Le Cap)	Available
Asie-Pacifique (Hong Kong)	Available
Asie-Pacifique (Tokyo)	Available
Asie-Pacifique (Séoul)	Available
Asie-Pacifique (Osaka)	Available
Asie-Pacifique (Mumbai)	Available
Asie-Pacifique (Hyderabad)	Non disponible
Asie-Pacifique (Singapour)	Available
Asie-Pacifique (Sydney)	Available
Asie-Pacifique (Jakarta)	Non disponible
Asie-Pacifique (Melbourne)	Non disponible
Asie-Pacifique (Malaisie)	Non disponible
Canada (Centre)	Available
Canada-Ouest (Calgary)	Non disponible
Chine (Pékin)	Non disponible
Chine (Ningxia)	Non disponible
Europe (Francfort)	Available
Europe (Zurich)	Non disponible

Région	RDS for MySQL
Europe (Stockholm)	Available
Europe (Milan)	Available
Europe (Espagne)	Non disponible
Europe (Irlande)	Available
Europe (Londres)	Available
Europe (Paris)	Available
Israël (Tel Aviv)	Non disponible
Moyen-Orient (EAU)	Non disponible
Middle East (Bahrain)	Available
Amérique du Sud (São Paulo)	Available
USA Est (Virginie du Nord)	Available
USA Est (Ohio)	Available
USA Ouest (Californie du Nord)	Available
USA Ouest (Oregon)	Available
AWS GovCloud (US-East)	Non disponible
AWS GovCloud (US-West)	Non disponible

Applications d’entreprise

Les régions suivantes sont disponibles pour les intégrations zéro ETL d’applications d’entreprise à Amazon Redshift.

Région	Applications d’entreprise
Afrique (Le Cap)	Non disponible
Asie-Pacifique (Hong Kong)	Available
Asie-Pacifique (Tokyo)	Available
Asie-Pacifique (Séoul)	Available
Asie-Pacifique (Osaka)	Non disponible
Asie-Pacifique (Mumbai)	Non disponible
Asie-Pacifique (Hyderabad)	Non disponible
Asie-Pacifique (Singapour)	Available
Asie-Pacifique (Sydney)	Available
Asie-Pacifique (Jakarta)	Non disponible
Asie-Pacifique (Melbourne)	Non disponible
Asie-Pacifique (Malaisie)	Non disponible
Canada (Centre)	Available
Canada-Ouest (Calgary)	Non disponible
Chine (Pékin)	Non disponible
Chine (Ningxia)	Non disponible
Europe (Francfort)	Available
Europe (Zurich)	Non disponible
Europe (Stockholm)	Available
Europe (Milan)	Non disponible

Région	Applications d’entreprise
Europe (Espagne)	Non disponible
Europe (Irlande)	Available
Europe (Londres)	Available
Europe (Paris)	Non disponible
Israël (Tel Aviv)	Non disponible
Moyen-Orient (EAU)	Non disponible
Middle East (Bahrain)	Non disponible
Amérique du Sud (São Paulo)	Available
USA Est (Virginie du Nord)	Available
USA Est (Ohio)	Available
USA Ouest (Californie du Nord)	Non disponible
USA Ouest (Oregon)	Available
AWS GovCloud (US-East)	Non disponible
AWS GovCloud (US-West)	Non disponible

Résolution des problèmes liés aux intégrations zéro ETL

Utilisez les sections suivantes pour résoudre les problèmes que vous rencontrez avec les intégrations zéro ETL.

Résolution des problèmes liés aux intégrations zéro ETL à Aurora MySQL

Utilisez les informations suivantes pour résoudre les problèmes courants liés aux intégrations zéro ETL avec Aurora MySQL.

Rubriques

- Échec de la création de l'intégration
- Les tables ne possèdent pas de clés primaires
- Les tables Aurora MySQL ne se répliquent pas vers Amazon Redshift
- Types de données non pris en charge dans les tables
- Échec des commandes en langage de manipulation de données
- Les modifications suivies entre les sources de données ne correspondent pas
- Échec d'autorisation
- Le nombre de tables est supérieur à 100 000 ou le nombre de schémas est supérieur à 4 950
- Amazon Redshift ne peut pas charger les données
- Les paramètres du groupe de travail sont incorrects
- La base de données n'est pas créée pour activer une intégration zéro ETL
- Le tableau se trouve dans Resynchronisation requise or Resynchronisation initiée state
- Le délai d'intégration s'accroît

Échec de la création de l'intégration

Si la création de l'intégration zéro ETL a échoué, le statut de l'intégration est `Inactive`. Assurez-vous que les informations suivantes sont correctes pour votre cluster de bases de données Aurora source :

- Vous avez créé votre cluster dans la console Amazon RDS.
- Votre cluster de bases de données Aurora source exécute une version prise en charge. Pour une liste des versions prises en charge, consultez Régions et moteurs de base de données Aurora pris en charge pour les intégrations zéro ETL à Amazon Redshift. Pour le vérifier, accédez à l'onglet Configuration du cluster et vérifiez la Version du moteur.
- Vous avez correctement configuré les paramètres binlog pour votre cluster. Si les paramètres binlog d'Aurora MySQL ne sont pas définis correctement ou s'ils ne sont pas associés au cluster de bases de données Aurora source, la création échoue. Consultez Configuration des paramètres du cluster de bases de données.

En outre, assurez-vous que les informations suivantes sont correctes pour votre entrepôt des données Amazon Redshift :

- La sensibilité à la casse est activée. Consultez Activation de la sensibilité à la casse pour votre entrepôt des données.
- Vous avez ajouté le principal autorisé et la source d'intégration appropriés pour votre espace de noms. Consultez Configuration de l'autorisation pour votre entrepôt des données Amazon Redshift.

Les tables ne possèdent pas de clés primaires

Dans la base de données de destination, une ou plusieurs tables ne possèdent pas de clé primaire et ne peuvent pas être synchronisées.

Pour résoudre ce problème, accédez à l'onglet Statistiques de table sur la page des détails de l'intégration ou utilisez SVV_INTEGRATION_TABLE_STATE pour afficher les tables ayant échoué. Vous pouvez ajouter des clés primaires aux tables et Amazon Redshift resynchronisera les tables. Bien que cela ne soit pas recommandé, vous pouvez supprimer ces tables sur Aurora et créer des tables avec une clé primaire. Pour plus d'informations, consultez Bonnes pratiques Amazon Redshift pour la conception de tables.

Les tables Aurora MySQL ne se répliquent pas vers Amazon Redshift

Si vous n'avez pas de table reflétée dans Amazon Redshift, vous pouvez exécuter la commande suivante pour les resynchroniser. *dbname*Remplacez-le par le nom de votre base de données Amazon Redshift. Et remplacez *table1* et *table2* par les noms des tables à synchroniser.

```
ALTER DATABASE dbname INTEGRATION REFRESH TABLES table1, table2;
```

Pour plus d'informations, consultez ALTER DATABASE dans le Guide du développeur de base de données Amazon Redshift.

Vos données ne sont peut-être pas répliquées, car une ou plusieurs de vos tables sources ne possèdent pas de clé primaire. Le tableau de bord de surveillance d'Amazon Redshift affiche l'état de ces tables comme `Failed` et l'état de l'intégration zéro ETL globale passe à `Needs attention`. Pour résoudre ce problème, vous pouvez identifier une clé existante dans votre table qui peut devenir une clé primaire, ou vous pouvez ajouter une clé primaire synthétique. Pour des solutions détaillées, consultez Gestion des tables sans clés primaires lors de la création d'intégrations zéro ETL Amazon Aurora MySQL ou Amazon RDS for MySQL avec Amazon Redshift dans le Blog de base de données AWS .

Vérifiez également que si votre cible est un cluster Amazon Redshift, le cluster n'est pas suspendu.

Types de données non pris en charge dans les tables

Dans la base de données que vous avez créée à partir de l'intégration dans Amazon Redshift et dans laquelle les données sont répliquées à partir du cluster de bases de données Aurora, une ou plusieurs tables contiennent des types de données non pris en charge et ne peuvent pas être synchronisées.

Pour résoudre ce problème, accédez à l'onglet Statistiques de table sur la page des détails de l'intégration ou utilisez SVV_INTEGRATION_TABLE_STATE pour afficher les tables ayant échoué. Supprimez ensuite ces tables et recréez de nouvelles tables dans Amazon RDS. Pour plus d'informations sur les types de données non pris en charge, consultez Différences de type de données entre les bases de données Aurora et Amazon Redshift dans le Guide de l'utilisateur Amazon Aurora.

Échec des commandes en langage de manipulation de données

Amazon Redshift n'a pas pu exécuter de commandes DML sur les tables Redshift. Pour résoudre ce problème, utilisez SVV_INTEGRATION_TABLE_STATE pour afficher les tables ayant échoué. Amazon Redshift resynchronise automatiquement les tables pour résoudre cette erreur.

Les modifications suivies entre les sources de données ne correspondent pas

Cette erreur se produit lorsque les modifications entre Amazon Aurora et Amazon Redshift ne correspondent pas, ce qui bascule l'intégration à l'état `Failed`.

Pour résoudre ce problème, supprimez l'intégration zéro ETL et créez-la à nouveau dans Amazon RDS. Pour plus d'informations, consultez Création d'intégrations zéro ETL et Suppression d'intégrations zéro ETL.

Échec d'autorisation

L'autorisation a échoué, car le cluster de bases de données Aurora source a été supprimé en tant que source d'intégration autorisée pour l'entrepôt des données Amazon Redshift.

Pour résoudre ce problème, supprimez l'intégration zéro ETL et créez-la à nouveau dans Amazon RDS. Pour plus d'informations, consultez Création d'intégrations zéro ETL et Suppression d'intégrations zéro ETL.

Le nombre de tables est supérieur à 100 000 ou le nombre de schémas est supérieur à 4 950

Pour un entrepôt des données de destination, le nombre de tables est supérieur à 100 000 ou le nombre de schémas est supérieur à 4 950. Amazon Aurora ne peut pas envoyer de données à

Amazon Redshift. Le nombre de tables et de schémas dépasse la limite définie. Pour résoudre ce problème, supprimez tous les schémas ou tables inutiles de la base de données source.

Amazon Redshift ne peut pas charger les données

Amazon Redshift ne peut pas charger de données dans l'intégration zéro ETL.

Pour résoudre ce problème, supprimez l'intégration zéro ETL dans Amazon RDS et créez-la à nouveau. Pour plus d'informations, consultez Création d'intégrations zéro ETL et Suppression d'intégrations zéro ETL.

Les paramètres du groupe de travail sont incorrects

La sensibilité à la casse n'est pas activée dans votre groupe de travail.

Pour résoudre ce problème, accédez à l'onglet Propriétés sur la page des détails de l'intégration, choisissez le groupe de paramètres et activez l'identifiant sensible à la casse dans l'onglet Propriétés. Si vous n'avez pas de groupe de paramètres existant, créez-en un en activant l'identifiant sensible à la casse. Créez ensuite une nouvelle intégration zéro ETL dans Amazon RDS. Pour plus d'informations, consultez Création d'intégrations zéro ETL.

La base de données n'est pas créée pour activer une intégration zéro ETL

Aucune base de données n'a été créée pour activer l'intégration zéro ETL.

Pour résoudre ce problème, créez une base de données pour l'intégration. Pour de plus amples informations, veuillez consulter Création de bases de données de destination dans Amazon Redshift.

Le tableau se trouve dans Resynchronisation requise or Resynchronisation initiée state

Votre table est dans l'état Resynchronisation requise ou Resynchronisation initiée.

Pour recueillir des informations d'erreur plus détaillées sur les raisons pour lesquelles votre table est dans cet état, utilisez la vue système SYS_LOAD_ERROR_DETAIL.

Le délai d'intégration s'accroît

Le délai d'intégration de vos intégrations zéro ETL peut augmenter en cas d'utilisation intensive de SAVEPOINT dans votre base de données source.

Résolution des problèmes liés aux intégrations zéro ETL à Aurora PostgreSQL

Utilisez les informations suivantes pour résoudre les problèmes courants liés aux intégrations zéro ETL avec Aurora PostgreSQL.

Rubriques

- Échec de la création de l’intégration
- Les tables ne possèdent pas de clés primaires
- Les tables Aurora PostgreSQL ne sont pas répliquées vers Amazon Redshift
- Types de données non pris en charge dans les tables
- Échec des commandes en langage de manipulation de données
- Les modifications suivies entre les sources de données ne correspondent pas
- Échec d’autorisation
- Le nombre de tables est supérieur à 100 000 ou le nombre de schémas est supérieur à 4 950
- Amazon Redshift ne peut pas charger les données
- Les paramètres du groupe de travail sont incorrects
- La base de données n’est pas créée pour activer une intégration zéro ETL
- Le tableau se trouve dans Resynchronisation requise or Resynchronisation initiée state

Échec de la création de l’intégration

Si la création de l’intégration zéro ETL a échoué, le statut de l’intégration est `Inactive`. Assurez-vous que les informations suivantes sont correctes pour votre cluster de bases de données Aurora source :

- Vous avez créé votre cluster dans la console Amazon RDS.
- Votre cluster de bases de données source exécute une version prise en charge. Pour une liste des versions prises en charge, consultez Régions et moteurs de base de données Aurora pris en charge pour les intégrations zéro ETL à Amazon Redshift. Pour le vérifier, accédez à l’onglet Configuration du cluster et vérifiez la Version du moteur.
- Vous avez correctement configuré les paramètres binlog pour votre cluster. Si les paramètres binlog d’Aurora PostgreSQL ne sont pas définis correctement ou s’ils ne sont pas associés au cluster de bases de données Aurora source, la création échoue. Consultez Configuration des paramètres du cluster de bases de données.

En outre, assurez-vous que les informations suivantes sont correctes pour votre entrepôt des données Amazon Redshift :

- La sensibilité à la casse est activée. Consultez Activation de la sensibilité à la casse pour votre entrepôt des données.
- Vous avez ajouté le principal autorisé et la source d'intégration appropriés pour votre endterm="zero-etl-using.redshift-iam.title"/>.

Les tables ne possèdent pas de clés primaires

Dans la base de données de destination, une ou plusieurs tables ne possèdent pas de clé primaire et ne peuvent pas être synchronisées.

Pour résoudre ce problème, accédez à l'onglet Statistiques de table sur la page des détails de l'intégration ou utilisez SVV_INTEGRATION_TABLE_STATE pour afficher les tables ayant échoué. Vous pouvez ajouter des clés primaires aux tables et Amazon Redshift resynchronisera les tables. Bien que cela ne soit pas recommandé, vous pouvez supprimer ces tables sur Aurora et créer des tables avec une clé primaire. Pour plus d'informations, consultez Bonnes pratiques Amazon Redshift pour la conception de tables.

Les tables Aurora PostgreSQL ne sont pas répliquées vers Amazon Redshift

Si vous n'avez pas de table reflétée dans Amazon Redshift, vous pouvez exécuter la commande suivante pour les resynchroniser. *dbname*Remplacez-le par le nom de votre base de données Amazon Redshift. Et remplacez *table1* et *table2* par les noms des tables à synchroniser.

```
ALTER DATABASE dbname INTEGRATION REFRESH TABLES table1, table2;
```

Pour plus d'informations, consultez ALTER DATABASE dans le Guide du développeur de base de données Amazon Redshift.

Vos données ne sont peut-être pas répliquées, car une ou plusieurs de vos tables sources ne possèdent pas de clé primaire. Le tableau de bord de surveillance d'Amazon Redshift affiche l'état de ces tables comme `Failed` et l'état de l'intégration zéro ETL globale passe à `Needs attention`. Pour résoudre ce problème, vous pouvez identifier une clé existante dans votre table qui peut devenir une clé primaire, ou vous pouvez ajouter une clé primaire synthétique. Pour des solutions détaillées, consultez Gestion des tables sans clés primaires lors de la création d'intégrations zéro ETL Amazon Aurora PostgreSQL avec Amazon Redshift dans le Blog de base de données AWS .

Vérifiez également que si votre cible est un cluster Amazon Redshift, le cluster n'est pas suspendu.

Types de données non pris en charge dans les tables

Dans la base de données que vous avez créée à partir de l'intégration dans Amazon Redshift et dans laquelle les données sont répliquées à partir du cluster de bases de données Aurora, une ou plusieurs tables contiennent des types de données non pris en charge et ne peuvent pas être synchronisées.

Pour résoudre ce problème, accédez à l'onglet Statistiques de table sur la page des détails de l'intégration ou utilisez SVV_INTEGRATION_TABLE_STATE pour afficher les tables ayant échoué. Supprimez ensuite ces tables et recréez de nouvelles tables dans Amazon RDS. Pour plus d'informations sur les types de données non pris en charge, consultez Différences de type de données entre les bases de données Aurora et Amazon Redshift dans le Guide de l'utilisateur Amazon Aurora.

Échec des commandes en langage de manipulation de données

Amazon Redshift n'a pas pu exécuter de commandes DML sur les tables Redshift. Pour résoudre ce problème, utilisez SVV_INTEGRATION_TABLE_STATE pour afficher les tables ayant échoué. Amazon Redshift resynchronise automatiquement les tables pour résoudre cette erreur.

Les modifications suivies entre les sources de données ne correspondent pas

Cette erreur se produit lorsque les modifications entre Amazon Aurora et Amazon Redshift ne correspondent pas, ce qui bascule l'intégration à l'état `Failed`.

Pour résoudre ce problème, supprimez l'intégration zéro ETL et créez-la à nouveau dans Amazon RDS. Pour plus d'informations, consultez Création d'intégrations zéro ETL et Suppression d'intégrations zéro ETL.

Échec d'autorisation

L'autorisation a échoué, car le cluster de bases de données Aurora source a été supprimé en tant que source d'intégration autorisée pour l'entrepôt des données Amazon Redshift.

Pour résoudre ce problème, supprimez l'intégration zéro ETL et créez-la à nouveau dans Amazon RDS. Pour plus d'informations, consultez Création d'intégrations zéro ETL et Suppression d'intégrations zéro ETL.

Le nombre de tables est supérieur à 100 000 ou le nombre de schémas est supérieur à 4 950

Pour un entrepôt des données de destination, le nombre de tables est supérieur à 100 000 ou le nombre de schémas est supérieur à 4 950. Amazon Aurora ne peut pas envoyer de données à

Amazon Redshift. Le nombre de tables et de schémas dépasse la limite définie. Pour résoudre ce problème, supprimez tous les schémas ou tables inutiles de la base de données source.

Amazon Redshift ne peut pas charger les données

Amazon Redshift ne peut pas charger de données dans l'intégration zéro ETL.

Pour résoudre ce problème, supprimez l'intégration zéro ETL dans Amazon RDS et créez-la à nouveau. Pour plus d'informations, consultez Création d'intégrations zéro ETL et Suppression d'intégrations zéro ETL.

Les paramètres du groupe de travail sont incorrects

La sensibilité à la casse n'est pas activée dans votre groupe de travail.

Pour résoudre ce problème, accédez à l'onglet Propriétés sur la page des détails de l'intégration, choisissez le groupe de paramètres et activez l'identifiant sensible à la casse dans l'onglet Propriétés. Si vous n'avez pas de groupe de paramètres existant, créez-en un en activant l'identifiant sensible à la casse. Créez ensuite une nouvelle intégration zéro ETL dans Amazon RDS. Pour plus d'informations, consultez Création d'intégrations zéro ETL.

La base de données n'est pas créée pour activer une intégration zéro ETL

Aucune base de données n'a été créée pour activer l'intégration zéro ETL.

Pour résoudre ce problème, créez une base de données pour l'intégration. Pour de plus amples informations, veuillez consulter Création de bases de données de destination dans Amazon Redshift.

Le tableau se trouve dans Resynchronisation requise or Resynchronisation initiée state

Votre table est dans l'état Resynchronisation requise ou Resynchronisation initiée.

Pour recueillir des informations d'erreur plus détaillées sur les raisons pour lesquelles votre table est dans cet état, utilisez la vue système SYS_LOAD_ERROR_DETAIL.

Résolution des problèmes liés aux intégrations zéro ETL à RDS for MySQL

Utilisez les informations suivantes pour résoudre les problèmes courants liés aux intégrations zéro ETL à RDS for MySQL.

Rubriques

- Échec de la création de l'intégration
- Les tables ne possèdent pas de clés primaires

- Les tables RDS for MySQL ne sont pas répliquées vers Amazon Redshift
- Types de données non pris en charge dans les tables
- Échec des commandes en langage de manipulation de données
- Les modifications suivies entre les sources de données ne correspondent pas
- Échec d'autorisation
- Le nombre de tables est supérieur à 100 000 ou le nombre de schémas est supérieur à 4 950
- Amazon Redshift ne peut pas charger les données
- Les paramètres du groupe de travail sont incorrects
- La base de données n'est pas créée pour activer une intégration zéro ETL
- Le tableau se trouve dans Resynchronisation requise or Resynchronisation initiée state

Échec de la création de l'intégration

Si la création de l'intégration zéro ETL a échoué, le statut de l'intégration est `Inactive`. Assurez-vous que les informations suivantes sont correctes pour votre instance de base de données RDS source :

- Vous avez créé votre instance dans la console Amazon RDS.
- Votre instance de base de données RDS source exécute une version prise en charge de RDS for MySQL. Pour une liste des versions prises en charge, consultez Régions et moteurs de base de données pris en charge pour les intégrations zéro ETL à Amazon Redshift. Pour vérifier cela, accédez à l'onglet Configuration de l'instance et vérifiez la version du moteur.
- Vous avez correctement configuré les paramètres binlog pour votre instance. Si les paramètres binlog de RDS for MySQL ne sont pas définis correctement ou s'ils ne sont pas associés à l'instance de base de données RDS source, la création échoue. Consultez Configuration des paramètres de l'instance de base de données.

En outre, assurez-vous que les informations suivantes sont correctes pour votre entrepôt des données Amazon Redshift :

- La sensibilité à la casse est activée. Consultez Activation de la sensibilité à la casse pour votre entrepôt des données.
- Vous avez ajouté le principal autorisé et la source d'intégration appropriés pour votre espace de noms. Consultez Configuration de l'autorisation pour votre entrepôt des données Amazon Redshift.

Les tables ne possèdent pas de clés primaires

Dans la base de données de destination, une ou plusieurs tables ne possèdent pas de clé primaire et ne peuvent pas être synchronisées.

Pour résoudre ce problème, accédez à l'onglet Statistiques de table sur la page des détails de l'intégration ou utilisez SVV_INTEGRATION_TABLE_STATE pour afficher les tables ayant échoué. Vous pouvez ajouter des clés primaires aux tables et Amazon Redshift resynchronisera les tables. Bien que cela ne soit pas recommandé, vous pouvez également supprimer ces tables sur RDS et créer des tables avec une clé primaire. Pour plus d'informations, consultez Bonnes pratiques Amazon Redshift pour la conception de tables.

Les tables RDS for MySQL ne sont pas répliquées vers Amazon Redshift

Si vous n'avez pas de table reflétée dans Amazon Redshift, vous pouvez exécuter la commande suivante pour les resynchroniser. *dbname*Remplacez-le par le nom de votre base de données Amazon Redshift. Et remplacez *table1* et *table2* par les noms des tables à synchroniser.

```
ALTER DATABASE dbname INTEGRATION REFRESH TABLES table1, table2;
```

Pour plus d'informations, consultez ALTER DATABASE dans le Guide du développeur de base de données Amazon Redshift.

Vos données ne sont peut-être pas répliquées, car une ou plusieurs de vos tables sources ne possèdent pas de clé primaire. Le tableau de bord de surveillance d'Amazon Redshift affiche l'état de ces tables comme `Failed` et l'état de l'intégration zéro ETL globale passe à `Needs attention`. Pour résoudre ce problème, vous pouvez identifier une clé existante dans votre table qui peut devenir une clé primaire, ou vous pouvez ajouter une clé primaire synthétique. Pour des solutions détaillées, voir Gérer les tables sans clé primaire lors de la création d'intégrations Aurora MySQL-Compatible Edition ou RDS pour MySQL Zero-ETL avec Amazon Redshift. dans le blog de la AWS base de données.

Vérifiez également que si votre cible est un cluster Amazon Redshift, le cluster n'est pas suspendu.

Types de données non pris en charge dans les tables

Dans la base de données que vous avez créée à partir de l'intégration dans Amazon Redshift et dans laquelle les données sont répliquées à partir de l'instance de base de données RDS, une ou plusieurs tables contiennent des types de données non pris en charge et ne peuvent pas être synchronisées.

Pour résoudre ce problème, accédez à l'onglet Statistiques de table sur la page des détails de l'intégration ou utilisez SVV_INTEGRATION_TABLE_STATE pour afficher les tables ayant échoué. Supprimez ensuite ces tables et recréez de nouvelles tables dans Amazon RDS. Pour plus d'informations sur les types de données non pris en charge, consultez Différences de type de données entre les bases de données RDS et Amazon Redshift dans le Guide de l'utilisateur Amazon RDS.

Échec des commandes en langage de manipulation de données

Amazon Redshift n'a pas pu exécuter de commandes DML sur les tables Redshift. Pour résoudre ce problème, utilisez SVV_INTEGRATION_TABLE_STATE pour afficher les tables ayant échoué. Amazon Redshift resynchronise automatiquement les tables pour résoudre cette erreur.

Les modifications suivies entre les sources de données ne correspondent pas

Cette erreur se produit lorsque les modifications entre Amazon Aurora et Amazon Redshift ne correspondent pas, ce qui bascule l'intégration à l'état `Failed`.

Pour résoudre ce problème, supprimez l'intégration zéro ETL et créez-la à nouveau dans Amazon RDS. Pour plus d'informations, consultez Création d'intégrations zéro ETL et Suppression d'intégrations zéro ETL.

Échec d'autorisation

L'autorisation a échoué, car l'instance de base de données RDS source a été supprimée en tant que source d'intégration autorisée pour l'entrepôt des données Amazon Redshift.

Pour résoudre ce problème, supprimez l'intégration zéro ETL et créez-la à nouveau dans Amazon RDS. Pour plus d'informations, consultez Création d'intégrations zéro ETL et Suppression d'intégrations zéro ETL.

Le nombre de tables est supérieur à 100 000 ou le nombre de schémas est supérieur à 4 950

Pour un entrepôt des données de destination, le nombre de tables est supérieur à 100 000 ou le nombre de schémas est supérieur à 4 950. Amazon Aurora ne peut pas envoyer de données à Amazon Redshift. Le nombre de tables et de schémas dépasse la limite définie. Pour résoudre ce problème, supprimez tous les schémas ou tables inutiles de la base de données source.

Amazon Redshift ne peut pas charger les données

Amazon Redshift ne peut pas charger de données dans l'intégration zéro ETL.

Pour résoudre ce problème, supprimez l'intégration zéro ETL dans Amazon RDS et créez-la à nouveau. Pour plus d'informations, consultez Création d'intégrations zéro ETL et Suppression d'intégrations zéro ETL.

Les paramètres du groupe de travail sont incorrects

La sensibilité à la casse n'est pas activée dans votre groupe de travail.

Pour résoudre ce problème, accédez à l'onglet Propriétés sur la page des détails de l'intégration, choisissez le groupe de paramètres et activez l'identifiant sensible à la casse dans l'onglet Propriétés. Si vous n'avez pas de groupe de paramètres existant, créez-en un en activant l'identifiant sensible à la casse. Créez ensuite une nouvelle intégration zéro ETL dans Amazon RDS. Pour plus d'informations, consultez Création d'intégrations zéro ETL.

La base de données n'est pas créée pour activer une intégration zéro ETL

Aucune base de données n'a été créée pour activer l'intégration zéro ETL.

Pour résoudre ce problème, créez une base de données pour l'intégration. Pour de plus amples informations, veuillez consulter Création de bases de données de destination dans Amazon Redshift.

Le tableau se trouve dans Resynchronisation requise or Resynchronisation initiée state

Votre table est dans l'état Resynchronisation requise ou Resynchronisation initiée.

Pour recueillir des informations d'erreur plus détaillées sur les raisons pour lesquelles votre table est dans cet état, utilisez la vue système SYS_LOAD_ERROR_DETAIL.

Résolution des problèmes liés aux intégrations zéro ETL avec DynamoDB

Utilisez les informations suivantes pour résoudre les problèmes courants liés aux intégrations zéro ETL. avec Amazon DynamoDB.

Rubriques

- Échec de la création de l'intégration
- Types de données non pris en charge dans les tables
- Noms de table et d'attribut non pris en charge
- Échec d'autorisation
- Amazon Redshift ne peut pas charger les données

- Les paramètres du groupe de travail ou du cluster sont incorrects
- La base de données n’est pas créée pour activer une intégration zéro ETL
- Point-in-time la restauration (PITR) n'est pas activée sur la table DynamoDB source
- Accès à la clé KMS refusé
- Amazon Redshift n’a pas accès à la clé de table DynamoDB

Échec de la création de l’intégration

Si la création de l’intégration zéro ETL a échoué, le statut de l’intégration est `Inactive`. Assurez-vous que les informations suivantes sont correctes pour votre entrepôt de données Amazon Redshift et votre table source DynamoDB :

- La sensibilité à la casse est activée pour votre entrepôt de données. Consultez Activation de la sensibilité à la casse dans le Guide de gestion Amazon Redshift.
- Vous avez ajouté le principal autorisé et la source d’intégration appropriés pour votre espace de noms dans Amazon Redshift. Consultez Configuration de l’autorisation pour votre entrepôt des données Amazon Redshift dans le Guide de gestion Amazon Redshift.
- Vous avez ajouté la bonne stratégie basée sur les ressources à la table DynamoDB source. Pour de plus amples informations, consultez Stratégies et autorisations dans IAM dans le Guide de l’utilisateur IAM.

Types de données non pris en charge dans les tables

Les numéros DynamoDB sont convertis en DECIMAL (38,10) dans Amazon Redshift. Les nombres dépassant cette plage de précision sont automatiquement transformés en (38,10). Supprimez l’intégration et unifiez les précisions numériques, puis recréez l’intégration.

Noms de table et d’attribut non pris en charge

Amazon Redshift prend en charge jusqu’à 127 noms de table et d’attribut de caractères. Si un nom long, tel que le nom de table DynamoDB ou le nom de colonne de clé de partition ou de clé de tri, échoue lors de votre intégration, corrigez-le en utilisant un nom plus court et recréez l’intégration.

Échec d’autorisation

L’autorisation peut échouer quand la table DynamoDB source est supprimée en tant que source d’intégration autorisée pour l’entrepôt des données Amazon Redshift.

Pour résoudre ce problème, supprimez l'intégration zéro ETL et recréez-la à nouveau à l'aide d'Amazon DynamoDB.

Amazon Redshift ne peut pas charger les données

Amazon Redshift ne peut pas charger de données depuis l'intégration zéro ETL.

Pour résoudre ce problème, actualisez l'intégration avec ALTER DATABASE.

```
ALTER DATABASE sample_integration_db INTEGRATION REFRESH ALL TABLES
```

Les paramètres du groupe de travail ou du cluster sont incorrects

La sensibilité à la casse n'est pas activée dans votre groupe de travail ou cluster.

Pour résoudre ce problème, accédez à l'onglet Propriétés sur la page des détails de l'intégration, choisissez le groupe de paramètres et activez l'identifiant sensible à la casse dans l'onglet Propriétés. Si vous n'avez pas de groupe de paramètres existant, créez-en un en activant l'identifiant sensible à la casse. Créez ensuite une nouvelle intégration zéro ETL dans DynamoDB. Consultez Activation de la sensibilité à la casse dans le Guide de gestion Amazon Redshift.

La base de données n'est pas créée pour activer une intégration zéro ETL

Aucune base de données n'a été créée pour activer l'intégration zéro ETL.

Pour résoudre ce problème, créez une base de données pour l'intégration. Consultez Création de bases de données de destination dans Amazon Redshift dans le Guide de gestion Amazon Redshift.

Point-in-time la restauration (PITR) n'est pas activée sur la table DynamoDB source

L'activation de la reprise ponctuelle est nécessaire pour que DynamoDB puisse exporter des données. Assurez-vous que la reprise ponctuelle est toujours activée. Si vous désactivez la reprise ponctuelle alors que l'intégration est active, vous devrez suivre les instructions du message d'erreur et actualiser l'intégration à l'aide d'ALTER DATABASE.

```
ALTER DATABASE sample_integration_db INTEGRATION REFRESH ALL TABLES
```

Accès à la clé KMS refusé

La clé KMS utilisée pour la table source ou l'intégration doit être configurée avec des autorisations suffisantes. Pour plus d'informations sur le chiffrement et le déchiffrement des tables, consultez Chiffrement de DynamoDB au repos dans le Guide du développeur Amazon DynamoDB.

Amazon Redshift n’a pas accès à la clé de table DynamoDB

Si le chiffrement de la table source est un Clé gérée par AWS, passez à une clé Clé détenue par AWS ou à une clé gérée par le client. Si la table est déjà chiffrée avec une clé gérée par le client, assurez-vous que la stratégie ne comporte aucune clé de condition.

Résolution des problèmes liés aux intégrations zéro ETL à des applications

Utilisez les informations suivantes pour résoudre les problèmes courants liés aux intégrations sans ETL avec des applications telles que Salesforce, ServiceNow SAP et Zendesk.

Rubriques

- Échec de la création de l’intégration
- Les tables ne sont pas répliquées vers Amazon Redshift
- Types de données non pris en charge dans les tables
- Les paramètres du groupe de travail sont incorrects
- La base de données n’est pas créée pour activer une intégration zéro ETL
- Le tableau se trouve dans Resynchronisation requise or Resynchronisation initiée state

Échec de la création de l’intégration

Si la création de l’intégration zéro ETL a échoué, le statut de l’intégration est `Inactive`. Assurez-vous que les informations suivantes sont correctes pour votre entrepôt des données Amazon Redshift :

- La sensibilité à la casse est activée. Consultez Activation de la sensibilité à la casse pour votre entrepôt des données.
- Vous avez ajouté le principal autorisé et la source d’intégration appropriés pour votre espace de noms. Consultez Configuration de l’autorisation pour votre entrepôt des données Amazon Redshift.

Les tables ne sont pas répliquées vers Amazon Redshift

Dans la base de données de destination, une ou plusieurs tables ne possèdent pas de clé primaire et ne peuvent pas être synchronisées.

Pour résoudre ce problème, accédez à l’onglet Statistiques de table sur la page des détails de l’intégration ou utilisez SVV_INTEGRATION_TABLE_STATE pour afficher les tables ayant échoué. Vous pouvez ajouter des clés primaires aux tables et Amazon Redshift resynchronisera les tables.

Vous pouvez exécuter la commande suivante pour les resynchroniser. *dbname*Remplacez-le par le nom de votre base de données Amazon Redshift. Et remplacez *table1* et *table2* par les noms des tables à synchroniser.

```
ALTER DATABASE dbname INTEGRATION REFRESH TABLES table1, table2;
```

Pour plus d'informations, consultez ALTER DATABASE dans le Guide du développeur de base de données Amazon Redshift.

Types de données non pris en charge dans les tables

Dans la base de données que vous avez créée à partir de l'intégration dans Amazon Redshift et dans laquelle les données sont répliquées à partir de l'intégration zéro ETL à des applications, une ou plusieurs tables contiennent des types de données non pris en charge et ne peuvent pas être synchronisées.

Pour résoudre ce problème, accédez à l'onglet Statistiques de table sur la page des détails de l'intégration ou utilisez SVV_INTEGRATION_TABLE_STATE pour afficher les tables ayant échoué. Supprimez ensuite ces tables et recréez de nouvelles tables à la source. Pour plus d'informations, consultez la section Zero-ETL Intégrations dans le Guide du AWS Glue développeur.

Les paramètres du groupe de travail sont incorrects

La sensibilité à la casse n'est pas activée dans votre groupe de travail.

Pour résoudre ce problème, accédez à l'onglet Propriétés sur la page des détails de l'intégration, choisissez le groupe de paramètres et activez l'identifiant sensible à la casse dans l'onglet Propriétés. Si vous n'avez pas de groupe de paramètres existant, créez-en un en activant l'identifiant sensible à la casse. Créez ensuite une nouvelle intégration zéro ETL. Pour plus d'informations, consultez la section Zero-ETL Intégrations dans le Guide du AWS Glue développeur.

La base de données n'est pas créée pour activer une intégration zéro ETL

Aucune base de données n'a été créée pour activer l'intégration zéro ETL.

Pour résoudre ce problème, créez une base de données pour l'intégration. Pour de plus amples informations, veuillez consulter Création de bases de données de destination dans Amazon Redshift.

Le tableau se trouve dans Resynchronisation requise or Resynchronisation initiée state

Votre table est dans l'état Resynchronisation requise ou Resynchronisation initiée.

Pour recueillir des informations d’erreur plus détaillées sur les raisons pour lesquelles votre table est dans cet état, utilisez la vue système SYS_LOAD_ERROR_DETAIL.

Interroger une base de données

Pour interroger les bases de données hébergées par votre cluster Amazon Redshift, deux options s'offrent à vous :

- Connectez-vous à votre cluster et exécutez des requêtes à l' Console de gestion AWS aide de l'éditeur de requêtes.

  Si vous utilisez l'éditeur de requête sur la console Amazon Redshift, vous n'avez pas besoin de télécharger et configurer une application cliente SQL.
- Connectez-vous à votre cluster via un outil client SQL, tel que SQL Workbench/J.

  Amazon Redshift prend en charge les outils clients SQL qui se connectent via Java DataBase Connectivity (JDBC) et Open DataBase Connectivity (ODBC). Amazon Redshift ne fournit ni n'installe aucun outil ou bibliothèque client SQL, vous devez donc les installer sur votre ordinateur client ou votre instance Amazon EC2 pour les utiliser. Vous pouvez utiliser la plupart des outils clients SQL qui prennent en charge les pilotes ODBC ou JDBC.

> **Note**
>
> Lorsque vous écrivez des procédures stockées, nous vous recommandons une bonne pratique pour sécuriser les valeurs sensibles :
> Ne codez pas en dur des informations sensibles dans la logique des procédures stockées. Par exemple, n'attribuez pas de mot de passe utilisateur dans une instruction CREATE USER dans le corps d'une procédure stockée. Cela présente un risque de sécurité, car les valeurs codées en dur peuvent être enregistrées sous forme de métadonnées de schéma dans les tables du catalogue. Transmettez plutôt des valeurs sensibles, telles que des mots de passe, en tant qu'arguments à la procédure stockée, au moyen de paramètres.
> Pour plus d'informations sur les procédures stockées, consultez PROCÉDURE DE CRÉATION et Création de procédures stockées dans Amazon Redshift. Pour plus d'informations sur les tables catalogue, consultez Tables de catalogue système.

Connexion à Amazon Redshift

Vous pouvez vous connecter à votre base de données à l'aide de la syntaxe suivante.

```
cluster-name.account-number.aws-region.redshift.amazonaws.com/database-name
```

Les éléments de syntaxe sont définis comme suit.

- `cluster-name`

  Le nom de votre cluster.

- `account-number`

  L'identifiant unique associé à votre numéro de AWS compte est donné Région AWS. Tous les clusters créés par un compte donné dans une Région AWS donnée ont le même `account-number`.

- `aws-region`

  Le code dans Région AWS lequel se trouve le cluster.

- `database-name`

  Le nom de votre base de données.

Par exemple, la chaîne de connexion suivante indique la `my-db` base de données du `my-cluster` cluster dans us-east-1 Région AWS.

```
my-cluster.123456789012.us-east-1.redshift.amazonaws.com/my-db
```

Interrogation d’une base de données à l’aide de l’éditeur de requête v2

L’éditeur de requête v2 est une application client SQL web distincte que vous utilisez pour créer et exécuter des requêtes sur votre entrepôt des données Amazon Redshift. L’éditeur de requête v2 est principalement utilisé pour modifier et exécuter des requêtes, consulter les résultats et partager votre travail avec votre équipe. Avec l’éditeur de requête v2, vous pouvez créer des bases de données, des schémas, des tables et des fonctions définies par l’utilisateur (UDF). Dans un panneau d’arborescence, pour chacune de vos bases de données, vous pouvez afficher ses schémas. Pour chaque schéma, vous pouvez afficher ses tables, ses vues, ses UDF et ses procédures stockées. L’éditeur de requête v2 remplace l’éditeur de requête précédent.

> **Note**
>
> L'éditeur de requêtes v2 est disponible dans le commerce Régions AWS. Pour obtenir la liste des Régions AWS endroits où l'éditeur de requêtes v2 est disponible, consultez les points de terminaison répertoriés pour l'éditeur de requêtes Redshift v2 dans le. Référence générale d'Amazon Web Services

Pour une démonstration de l'éditeur de requête v2, regardez la vidéo suivante. Éditeur de requête v2 Amazon Redshift.

Pour une démonstration de l'analyse des données, regardez la vidéo suivante. Analyse des données à l'aide de Amazon Redshift Query Editor V22.

Pour une démonstration de l'utilisation de l'éditeur de requête v2 exécutant plusieurs requêtes avec une connexion isolée ou partagée, regardez la vidéo suivante. Exécution de requêtes simultanées avec l'éditeur de requête v2.

L'éditeur de requête v2 dispose d'un riche ensemble de fonctions permettant de gérer et d'exécuter vos instructions SQL. Les rubriques des sections suivantes vous permettent de commencer à utiliser plusieurs de ces fonctions. Explorez vous-même l'éditeur de requête v2 pour vous familiariser avec ses capacités.

Configuration de votre Compte AWS

Vous pouvez effectuer cet ensemble de tâches pour configurer l'éditeur de requêtes v2 afin d'interroger une base de données Amazon Redshift. Avec les autorisations appropriées, vous pouvez accéder aux données d'un cluster ou d'un groupe de travail Amazon Redshift dont vous Compte AWS êtes propriétaire et qui se trouve actuellement. Région AWS

La première fois qu'un administrateur configure l'éditeur de requêtes v2 pour vous Compte AWS, il choisit AWS KMS key celui qui est utilisé pour chiffrer les ressources de l'éditeur de requêtes v2. Par défaut, une clé AWS détenue est utilisée pour chiffrer les ressources. Un administrateur peut également utiliser une clé gérée par le client en choisissant l'Amazon Resource Name (ARN) pour la clé dans la page de configuration.

Après avoir configuré un compte, les paramètres de AWS KMS chiffrement ne peuvent pas être modifiés. Pour plus d'informations sur la création et l'utilisation d'une clé gérée par le client avec l'éditeur de requête v2, consultez Création d'un AWS KMS clé gérée par le client à utiliser avec

l'éditeur de requêtes v2. L'administrateur peut éventuellement choisir un compartiment S3 et le chemin utilisé pour certaines fonctionnalités, telles que le chargement de données à partir d'un fichier. Pour de plus amples informations, veuillez consulter Chargement de données à partir d'un fichier local : configuration et flux de travail.

L'éditeur de requête v2 Amazon Redshift prend en charge l'authentification, le chiffrement, l'isolement et la conformité pour protéger vos données au repos et en transit. Pour plus d'informations sur la sécurité des données et l'éditeur de requête v2, consultez les rubriques suivantes :

- Chiffrement au repos
- Chiffrement en transit
- Configuration et analyse des vulnérabilités dans Amazon Redshift

AWS CloudTrail capture les appels d'API et les événements associés effectués par ou pour votre compte Compte AWS et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date à laquelle les appels ont eu lieu. Pour en savoir plus sur la manière dont l'éditeur de requête v2 s'exécute sur AWS CloudTrail, consultez Se connecter avec CloudTrail. Pour plus d'informations à ce sujet CloudTrail, consultez le Guide de AWS CloudTrail l'utilisateur.

L'éditeur de requête v2 dispose de quotas réglables pour certaines de ses ressources. Pour plus d'informations, consultez Quotas pour les objets Amazon Redshift.

Ressources créées à l'aide de l'éditeur de requête v2

Dans l'éditeur de requête v2, vous pouvez créer des ressources telles que des requêtes enregistrées et des diagrammes. Toutes les ressources de l'éditeur de requête v2 sont associées à un rôle IAM ou à un utilisateur. Nous vous recommandons d'associer des politiques à un rôle IAM et de l'attribuer à un utilisateur.

Dans l'éditeur de requête v2, vous pouvez ajouter et supprimer des balises pour les requêtes et les diagrammes enregistrés. Vous pouvez utiliser ces balises lorsque vous configurez des politiques IAM personnalisées ou pour rechercher des ressources. Vous pouvez également gérer les balises à l'aide de l'éditeur de Groupes de ressources AWS balises.

Vous pouvez configurer des rôles IAM avec des politiques IAM pour partager des requêtes avec d'autres personnes de votre domaine Compte AWS dans le. Région AWS

Création d'un AWS KMS clé gérée par le client à utiliser avec l'éditeur de requêtes v2

Pour créer une clé de chiffrement symétrique gérée par le client :

Vous pouvez créer une clé de chiffrement symétrique gérée par le client pour chiffrer les ressources de l'éditeur de requêtes v2 à l'aide de la AWS KMS console ou des opérations d' AWS KMS API. Pour obtenir des instructions sur la création d'une clé, consultez la section Création d'une AWS KMS clé de chiffrement symétrique dans le Guide du AWS Key Management Service développeur.

Stratégie de clé

Les stratégies de clé contrôlent l'accès à votre clé gérée par le client. Chaque clé gérée par le client doit avoir exactement une stratégie de clé, qui contient des instructions qui déterminent les personnes pouvant utiliser la clé et comment elles peuvent l'utiliser. Lorsque vous créez votre clé gérée par le client, vous pouvez spécifier une stratégie de clé. Pour plus d'informations, consultez la section Gestion de l'accès aux AWS KMS clés dans le Guide du AWS Key Management Service développeur.

Pour utiliser votre clé gérée par le client avec Amazon Redshift Query Editor V2, les opérations API suivantes doivent être autorisées dans la stratégie de clé :

- `kms:GenerateDataKey` – Génère une clé de données symétrique unique pour chiffrer vos données.
- `kms:Decrypt` – Déchiffre les données chiffrées à l'aide de la clé gérée par le client.
- `kms:DescribeKey` – Fournit les détails des clés gérées par le client pour permettre au service de valider la clé.

Voici un exemple de AWS KMS politique pour Compte AWS `111122223333`. Dans la première section, le `kms:ViaService` limite l'utilisation de la clé au service de l'éditeur de requête v2 (nommé `sqlworkbench.`*`region`*`.amazonaws.com` dans la politique). L' Compte AWS utilisation de la clé doit être`111122223333`. Dans la deuxième section, l'utilisateur root et les administrateurs clés de Compte AWS `111122223333` peuvent accéder à la clé.

Lorsque vous créez un Compte AWS, vous commencez avec 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.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "key-consolepolicy",
    "Statement": [
        {
            "Sid": "Allow access to principals authorized to use Amazon Redshift
 Query Editor V2",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "sqlworkbench.us-east-1.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:*"
            ],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/key_ID"
        }
    ]
}
```

Les ressources suivantes fournissent plus d'informations sur AWS KMS les clés :

- Pour plus d'informations sur AWS KMS les politiques, consultez la section Définition des autorisations dans une politique dans le Guide du AWS Key Management Service développeur.
- Pour plus d'informations sur AWS KMS les politiques de dépannage, consultez la section Résolution des problèmes d'accès aux clés dans le Guide du AWS Key Management Service développeur.
- Pour plus d'informations sur les clés KMS, consultez Clés AWS KMS dans le Guide du développeur AWS Key Management Service .

Accès à l'éditeur de requête v2

Pour accéder à l'éditeur de requête v2, vous avez besoin d'une autorisation. Un administrateur peut associer l'une des politiques AWS gérées suivantes au rôle pour accorder l'autorisation. (Nous vous recommandons d'associer des politiques à un rôle IAM et de l'attribuer à un utilisateur.) Ces politiques AWS gérées sont écrites avec différentes options qui contrôlent la manière dont le balisage des ressources permet le partage des requêtes. Vous pouvez utiliser la console IAM (https://console.aws.amazon.com/iam/) pour joindre des politiques IAM.

- AmazonRedshiftQueryEditorV2FullAccess— Donne un accès complet aux opérations et aux ressources de l'éditeur de requêtes Amazon Redshift v2. Cette politique permet également d'accéder à d'autres services requis.
- AmazonRedshiftQueryEditorV2NoSharing— Permet de travailler avec l'éditeur de requêtes Amazon Redshift v2 sans partager de ressources. Cette politique permet également d'accéder à d'autres services requis.
- AmazonRedshiftQueryEditorV2ReadSharing— Permet de travailler avec l'éditeur de requêtes Amazon Redshift v2 avec un partage limité des ressources. Le principal autorisé peut lire les ressources partagées avec son équipe, mais ne peut pas les mettre à jour. Cette politique permet également d'accéder à d'autres services requis.
- AmazonRedshiftQueryEditorV2ReadWriteSharing— Permet de travailler avec l'éditeur de requêtes Amazon Redshift v2 avec partage de ressources. Le principal autorisé peut lire et mettre à jour les ressources partagées avec son équipe. Cette politique permet également d'accéder à d'autres services requis.

Vous pouvez également créer votre propre politique basée sur les autorisations autorisées et refusées dans les politiques gérées fournies. Si vous utilisez l'éditeur de politique de la console IAM pour créer votre propre politique, choisissez SQL Workbench en tant que service pour lequel vous

créez la politique dans l'éditeur visuel. L'éditeur de requête v2 utilise le nom du service AWS SQL Workbench dans l'éditeur visuel et le simulateur de politiques IAM.

Pour qu'un principal (un utilisateur avec un rôle IAM assigné) puisse se connecter à un cluster Amazon Redshift, il doit disposer des autorisations dans l'une des politiques gérées de l'éditeur de requête v2. Ils ont également besoin de l'une des `redshift:GetClusterCredentials` autorisations `redshift:GetClusterCredentialsWithIAM` ou d'une autorisation pour le cluster. Pour obtenir cette autorisation, une personne disposant d'une autorisation administrative peut attacher une politique aux rôles IAM utilisés pour se connecter au cluster à l'aide d'informations d'identification temporaires. Vous pouvez étendre la politique à des clusters spécifiques ou être plus général. Pour plus d'informations sur l'autorisation d'utiliser des informations d'identification temporaires, voir Créer un rôle ou un utilisateur IAM autorisé à appeler GetClusterCredentialsWithIAM ou GetClusterCredentials.

Pour qu'un principal (généralement un utilisateur avec un rôle IAM assigné) puisse activer, dans la page Paramètres du compte, la possibilité pour les autres membres du compte d'effectuer une opération Exporter l'ensemble des résultats, il lui faut l'autorisation `sqlworkbench:UpdateAccountExportSettings` attachée au rôle. Cette autorisation est incluse dans la politique `AmazonRedshiftQueryEditorV2FullAccess` AWS gérée.

À mesure que de nouvelles fonctionnalités sont ajoutées à l'éditeur de requêtes v2, les politiques AWS gérées sont mises à jour selon les besoins. Si vous créez votre propre politique basée sur les autorisations autorisées et refusées dans les politiques gérées fournies, modifiez vos politiques pour les tenir à jour avec les modifications apportées aux politiques gérées. Pour plus d'informations sur les politiques gérées dans Amazon Redshift, consultez AWS politiques gérées pour Amazon Redshift.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM dans le Guide de l'utilisateur IAM.
- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

> **Note**
>
> Si un AWS IAM Identity Center administrateur supprime toutes les associations d'ensembles d'autorisations pour un ensemble d'autorisations particulier dans l'ensemble du compte, l'accès à toutes les ressources de l'éditeur de requêtes initialement associées à l'ensemble d'autorisations supprimé n'est plus accessible. Ultérieurement, si les mêmes autorisations sont recréées, un nouvel identifiant interne est créé. L'identifiant interne ayant changé, l'accès aux ressources de l'éditeur de requêtes précédemment détenues par un utilisateur n'est plus disponible. Avant que les administrateurs suppriment un ensemble d'autorisations, nous recommandons aux utilisateurs de cet ensemble d'autorisations d'exporter les ressources de l'éditeur de requêtes, telles que les blocs-notes et les requêtes, en tant que sauvegarde.

Configuration de balises de principal pour connecter un cluster ou un groupe de travail à partir de l'éditeur de requêtes v2

Pour vous connecter à votre cluster ou groupe de travail à l'aide de l'option d'utilisateur fédéré, configurez votre utilisateur ou rôle IAM avec des balises de principal. Ou bien, configurez votre fournisseur d'identité (IdP) pour qu'il transmette `RedshiftDbUser` et (en option) `RedshiftDbGroups`. Pour plus d'informations sur l'utilisation d'IAM pour gérer les balises, consultez Transmission des balises de session dans AWS Security Token Service (langue Français non garantie) dans le Guide de l'utilisateur IAM. Pour configurer l'accès à l'aide de Gestion des identités et des accès AWS, un administrateur peut ajouter des balises à l'aide de la console IAM (https://console.aws.amazon.com/iam/).

Pour ajouter des balises relatives au principal à un rôle IAM

1. Connectez-vous au Console de gestion AWS et ouvrez la console IAM à https://console.aws.amazon.com/iam/ l'adresse.
2. Choisissez Rôles dans le panneau de navigation.

3. Choisissez le rôle qui doit accéder à l'éditeur de requête v2 en utilisant un utilisateur fédéré.
4. Sélectionnez l'onglet Tags (Identifications).
5. Choisissez Manage tags (Gérer les balises).
6. Choisissez Ajouter une balise et entrez une valeur Clé de `RedshiftDbUser`, puis entrez la Value du nom d'utilisateur fédéré.
7. Vous pouvez également sélectionner Ajouter une balise et entrer la Clé de `RedshiftDbGroups`, puis entrer la Valeur du nom du groupe à associer à l'utilisateur.
8. Choisissez Save changes (Enregistrer les modifications) pour afficher la liste des balises associées au rôle IAM que vous avez choisi. La propagation des modifications peut prendre plusieurs secondes.
9. Pour utiliser l'utilisateur fédéré, actualisez votre page de l'éditeur de requêtes v2 après la propagation des modifications.

Configurez votre fournisseur d'identité (IdP) pour transmettre les balises relatives au principal

La procédure de configuration des balises à l'aide d'un fournisseur d'identité (IdP) varie selon l'IdP. Consultez la documentation de votre IdP pour savoir comment transmettre les informations sur les utilisateurs et les groupes aux attributs SAML. Lorsqu'ils sont configurés correctement, les attributs suivants apparaissent dans votre réponse SAML qui est utilisée par le AWS Security Token Service pour renseigner les balises principales pour `RedshiftDbUser` et. `RedshiftDbGroups`

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:RedshiftDbUser">
    <AttributeValue>db-user-name</AttributeValue>
</Attribute>
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:RedshiftDbGroups">
    <AttributeValue>db-groups</AttributeValue>
</Attribute>
```

L'option *`db_groups`* doit être une liste séparée par des deux-points, telle que. `group1:group2:group3`

En outre, vous pouvez définir l'attribut `TransitiveTagKeys` pour que les balises persistent pendant la création de chaînes de rôles.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys">
  <AttributeValue>RedshiftDbUser</AttributeValue>
  <AttributeValue>RedshiftDbGroups</AttributeValue>
```

```
</Attribute>
```

Pour plus d'informations sur la configuration de l'éditeur de requêtes v2, consultez Autorisations requises pour utiliser l'éditeur de requête v2.

> **Note**
>
> Lorsque vous vous connectez à votre cluster ou groupe de travail à l'aide de l'option de connexion Utilisateur fédéré de l'éditeur de requêtes v2, le fournisseur d'identité (IdP) peut fournir des balises de principal personnalisées pour `RedshiftDbUser` et `RedshiftDbGroups`. Actuellement, ne AWS IAM Identity Center prend pas en charge la transmission de balises principales personnalisées directement à l'éditeur de requêtes v2.

Ouverture de l'éditeur de requête v2

Avec Amazon Redshift, vous pouvez exécuter des requêtes SQL sur votre cluster d'entrepôts de données à l'aide de l'éditeur de requêtes v2 de la console Amazon Redshift. L'éditeur de requêtes v2 est un outil Web qui fournit une interface conviviale pour exécuter des requêtes ad hoc, explorer des données et effectuer des tâches d'analyse de données. Les sections suivantes vous guident dans le processus d'ouverture de l'éditeur de requêtes v2 dans la console et dans l'utilisation efficace de ses fonctionnalités.

Pour ouvrir l'éditeur de requête v2

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu du navigateur, choisissez Editor (Éditeur), puis Query editor V2 (Éditeur de requête v2). L'éditeur de requête v2 s'ouvre dans un nouvel onglet de navigateur.

La page de l'éditeur de requête comporte un menu de navigation dans lequel vous pouvez choisir une vue comme suit :

Éditeur



Vous gérez et interrogez vos données organisées sous forme de tables et contenues dans une base de données. La base de données peut contenir des données stockées ou une référence à des données stockées ailleurs, par exemple dans Amazon S3. Vous vous connectez à une base de données contenue dans un cluster ou dans un groupe de travail sans serveur.

Lorsque vous travaillez dans la vue Editor (Éditeur), vous disposez des commandes suivantes :

- Le champ Cluster ou Workgroup (Groupe de travail) affiche le nom auquel vous êtes actuellement connecté. Le champ Database (Base de données) affiche les bases de données du cluster ou du groupe de travail. Les actions que vous effectuez dans la vue Database (Base de données) utilisent les valeurs par défaut pour agir sur la base de données que vous avez sélectionnée.
- Vue hiérarchique en arborescence de vos clusters ou de vos groupes de travail, bases de données et schémas. Sous les schémas, vous pouvez utiliser vos tables, vos vues, vos fonctions et vos procédures stockées. Chaque objet de l'arborescence prend en charge un menu contextuel pour effectuer des actions associées, telles que Refresh (Actualiser) ou Drop (Supprimer), pour l'objet.
- Une action Create (Créer)

  pour créer des bases de données, des schémas, des tables et des fonctions.
- Une action

  Charge

  les données pour charger les données à partir d'Amazon S3 ou d'un fichier local dans votre base de données.
- Une icône Save (Enregistrer)

  pour enregistrer votre requête.
- Une icône Shortcuts (Racourcis)

  pour afficher les raccourcis clavier de l'éditeur.

- Une icône

  •••

  Plus pour afficher plus d'actions dans l'éditeur. Comme :

  - Partager avec mon équipe pour partager la requête ou un bloc-notes avec votre équipe. Pour plus d'informations, consultez Collaborer et partager en équipe.
  - Raccourcis pour afficher les raccourcis clavier de l'éditeur.
  - Historique des onglets pour afficher l'historique d'un onglet dans l'éditeur.
  - Actualisation automatique pour actualiser les suggestions affichées lors de la création de SQL.
- Une zone Editor (Éditeur)

  +

  dans laquelle vous pouvez saisir et exécuter votre requête.

  Une fois que vous avez exécuté une requête, un onglet Result (Résultat) apparaît avec les résultats. C'est ici que vous pouvez activer Chart (Diagramme) pour visualiser vos résultats. Vous pouvez également Export (Exporter) vos résultats.
- Une zone Notebook (Bloc-notes)

  +

  dans laquelle vous pouvez ajouter des sections pour saisir et exécuter des commandes SQL ou ajouter des cellules Markdown.

  Une fois que vous avez exécuté une requête, un onglet Result (Résultat) apparaît avec les résultats. Voici où vous pouvez Export (Exporter) vos résultats.

Requêtes



Une requête contient les commandes SQL permettant de gérer et d'interroger vos données dans une base de données. Lorsque vous utilisez l'éditeur de requête v2 pour charger des exemples de données, il crée et enregistre également des exemples de requête pour vous.

Lorsque vous choisissez une requête enregistrée, vous pouvez l'ouvrir, la renommer et la supprimer à l'aide du menu contextuel (clic droit). Vous pouvez afficher des attributs tels que l'ARN de la requête enregistrée en sélectionnant Détails de la requête. Vous pouvez également consulter l'historique de ses versions, modifier les balises attachées à la requête et la partager avec votre équipe.

Blocs-notes



Un bloc-notes SQL contient des cellules SQL et Markdown. Utilisez des blocs-notes pour organiser, annoter et partager plusieurs commandes SQL dans un même document.

Lorsque vous choisissez un bloc-notes enregistré, vous pouvez l'ouvrir, le renommer, le dupliquer et le supprimer à l'aide du menu contextuel (clic droit). Vous pouvez afficher des attributs tels que l'ARN du bloc-notes d'un bloc-notes enregistré en choisissant Détails du bloc-notes. Vous pouvez également consulter l'historique de ses versions, modifier les balises attachées au bloc-notes, l'exporter et le partager avec votre équipe. Pour plus d'informations, consultez Blocs-notes dans Amazon Redshift.

Graphiques



Un graphique est une représentation visuelle de vos données. L'éditeur de requête v2 fournit les outils nécessaires pour créer de nombreux types de graphiques et les enregistrer.

Lorsque vous choisissez un graphique enregistré, vous pouvez l'ouvrir, le renommer et le supprimer à l'aide du menu contextuel (clic droit). Vous pouvez afficher des attributs tels que l'ARN du graphique d'un graphique enregistré en choisissant Détails du graphique. Vous pouvez également modifier les balises attachées au graphique et l'exporter. Pour plus d'informations, consultez Visualisation des résultats de requêtes.

Historique

L'historique des requêtes est une liste des requêtes que vous avez exécutées à l'aide de Amazon Redshift Query Editor V2. Ces requêtes s'exécutaient soit en tant que requêtes individuelles, soit dans le cadre d'un bloc-notes SQL. Pour plus d'informations, consultez Afficher l'historique des requêtes et des onglets.

Requêtes planifiées



Une requête planifiée est une requête qui est configurée pour se lancer à des heures précises.

Toutes les vues de l'éditeur de requête v2 ont les icônes suivantes :

- Une icône Visual mode (Mode visuel)

  pour basculer entre le mode clair et le mode sombre.

- Une icône Settings (Paramètres)

  pour afficher un menu des différents écrans de paramètres.

  - Une icône Editor preferences (Préférences de l'éditeur)

    pour modifier vos préférences lorsque vous utilisez l'éditeur de requête v2. Ici, vous pouvez Modifier les paramètres de l'espace de travail pour modifier la taille de police, la taille des onglets et d'autres paramètres d'affichage. Vous pouvez également activer (ou désactiver) le Remplissage automatique pour afficher les suggestions lorsque vous saisissez votre code SQL.

  - Une icône Connections (Connexions)

    pour afficher les connexions utilisées par les onglets de votre éditeur.

    Une connexion permet de récupérer des données à partir d'une base de données. Une connexion est créée pour une base de données spécifique. Avec une connexion isolée, les résultats d'une commande SQL qui modifie la base de données, telle que la création d'une table temporaire, dans un onglet de l'éditeur, ne sont pas visibles dans un autre onglet de l'éditeur. Lorsque vous ouvrez un onglet d'éditeur dans l'éditeur de requête v2, l'option par défaut est une connexion isolée. Lorsque vous créez une connexion partagée, c'est-à-dire que vous désactivez l'option Isolated session (Session isolée), les résultats des autres connexions partagées à la même base de données sont visibles par les uns et les autres. Toutefois, les onglets de l'éditeur utilisant une connexion partagée à une base de données ne s'exécutent pas en parallèle. Des requêtes utilisant la même connexion doivent attendre que la connexion soit disponible. Une connexion à une base de données ne peut pas être partagée avec une autre base de données, de sorte que les résultats SQL ne sont pas visibles entre différentes connexions de base de données.

    Le nombre de connexions actives qu'un utilisateur du compte peut avoir est contrôlé par un administrateur de l'éditeur de requêtes v2.

- Une icône Account settings (Paramètres du compte)

  utilisée par un administrateur pour modifier certains paramètres de tous les utilisateurs du compte. Pour plus d'informations, consultez Paramètres du compte.

Remarques concernant l'utilisation de l'éditeur de requête v2

Tenez compte des points suivants lorsque vous utilisez l'éditeur de requête v2.

- La durée maximale d'une requête est de 24 heures.
- La taille maximale du résultat de requête est de 100 Mo. Si un appel renvoie plus de 100 Mo de données de réponse, les 100 premiers Mo sont renvoyés avec un avertissement.
- Vous pouvez exécuter une requête de 300 000 caractères maximum.
- Vous pouvez enregistrer une requête de 30 000 caractères maximum.
- Par défaut, l'éditeur de requête v2 valide automatiquement chaque commande SQL qui s'exécute. Lorsqu'une instruction BEGIN est fournie, les instructions contenues dans BEGIN-COMMIT ou en BEGIN-ROLLBACK bloc sont exécutées en tant que transaction unique. Pour plus d'informations sur les transactions, consultez BEGIN dans le Manuel du développeur de base de données Amazon Redshift.
- Le nombre maximal d'avertissements que l'éditeur de requête v2 affiche lors de l'exécution d'une instruction SQL est `10`. Par exemple, lorsqu'une procédure stockée est exécutée, moins de 10 instructions RAISE sont affichées.
- L'éditeur de requêtes v2 ne prend pas en charge un `RoleSessionName` IAM contenant des virgules (,). Une erreur similaire à la suivante peut s'afficher : Message d'erreur : « 'AROA123456789EXAMPLE:mytext, yourtext' is not a valid value for TagValue - it contains illegal characters » Ce problème survient lorsque vous définissez un IAM `RoleSessionName` qui inclut une virgule, puis que vous utilisez l'éditeur de requêtes v2 avec ce rôle IAM.

  Pour plus d'informations sur un IAM`RoleSessionName`, consultez l'attribut RoleSessionName SAML dans le Guide de l'utilisateur IAM.

Paramètres du compte

Un utilisateur disposant des autorisations IAM appropriées peut afficher et modifier les Account settings (Paramètres du compte) pour les autres utilisateurs du même Compte AWS. Cet administrateur peut afficher ou définir les éléments suivants :

- Nombre maximal de connexions simultanées à la base de données par utilisateur dans le compte. Cela inclut les connexions pour les Isolated sessions (Sessions isolées). Lorsque vous modifiez cette valeur, la modification peut prendre jusqu'à 10 minutes avant d'être effective.
- Autoriser les utilisateurs du compte à exporter l'intégralité d'un jeu de résultats d'une commande SQL vers un fichier.
- Charger et afficher des exemples de bases de données avec certaines requêtes enregistrées associées.
- Spécifiez un chemin Amazon S3 utilisé par des utilisateurs du compte pour charger des données à partir d'un fichier local.
- Afficher l'ARN de clé KMS à utiliser pour chiffrer les ressources de l'éditeur de requête v2.

Connexion à une base de données Amazon Redshift

Pour vous connecter à une base de données, choisissez le nom du cluster ou du groupe de travail dans le panneau d'arborescence. Si vous y êtes invité, saisissez les paramètres de connexion.

Lorsque vous vous connectez à un cluster ou à un groupe de travail et à ses bases de données, vous fournissez un nom de Database (Base de données). Vous fournissez également les paramètres requis pour l'une des méthodes d'authentification suivantes :

IAM Identity Center

Avec cette méthode, connectez-vous à votre entrepôt des données Amazon Redshift à l'aide de vos informations d'identification d'authentification unique provenant de votre fournisseur d'identité (IdP). Votre cluster ou groupe de travail doit être activé pour IAM Identity Center dans la console Amazon Redshift. Pour obtenir de l'aide concernant la configuration des connexions à IAM Identity Center, consultez Connectez Redshift à AWS IAM Identity Center pour une expérience d'authentification unique.

Utilisateur fédéré

Avec cette méthode, les balises relatives au principal de votre rôle IAM ou de votre utilisateur doivent fournir les détails de la connexion. Vous configurez ces balises dans Gestion des identités

et des accès AWS ou dans votre fournisseur d'identité (IdP). L'éditeur de requêtes v2 s'appuie sur les balises suivantes.

- `RedshiftDbUser` — cette balise définit l'utilisateur de la base de données qui est utilisé par l'éditeur de requêtes v2. Elle est obligatoire.
- `RedshiftDbGroups` — cette balise définit les groupes de bases de données qui sont joints lors de la connexion à l'éditeur de requêtes v2. Cette balise est facultative et sa valeur doit être une liste séparée par le signe deux points, telle que `group1:group2:group3`. Les valeurs vides sont ignorées, c'est-à-dire que `group1::::group2` est interprété comme `group1:group2`.

Ces balises sont transmises à l'API `redshift:GetClusterCredentials` pour obtenir des informations d'identification pour votre cluster. Pour plus d'informations, consultez Configuration de balises de principal pour connecter un cluster ou un groupe de travail à partir de l'éditeur de requêtes v2.

Informations d'identification temporaires utilisant un nom d'utilisateur de base de données

Cette option est disponible uniquement lors de la connexion à un cluster. Avec cette méthode, l'éditeur de requête v2 fournit un User name (Nom d'utilisateur) pour la base de données. L'éditeur de requêtes v2 génère un mot de passe temporaire pour se connecter à la base de données sous votre nom d'utilisateur de base de données. Un utilisateur utilisant cette méthode pour se connecter doit disposer de l'autorisation IAM pour `redshift:GetClusterCredentials`. Pour empêcher les utilisateurs d'utiliser cette méthode, modifiez leur rôle ou utilisateur IAM afin de refuser cette autorisation.

Informations d'identification temporaires utilisant votre identité IAM

Cette option est disponible uniquement lors de la connexion à un cluster. Avec cette méthode, l'éditeur de requêtes v2 mappe un nom d'utilisateur à votre identité IAM et génère un mot de passe temporaire pour se connecter à la base de données sous votre identité IAM. Un utilisateur utilisant cette méthode pour se connecter doit disposer de l'autorisation IAM pour `redshift:GetClusterCredentialsWithIAM`. Pour empêcher les utilisateurs d'utiliser cette méthode, modifiez leur rôle ou utilisateur IAM afin de refuser cette autorisation.

Nom d'utilisateur et mot de passe de la base de données

Avec cette méthode, vous devez également fournir un User name (Nom d'utilisateur) et un Password (Mot de passe) pour la base de données à laquelle vous vous connectez. L'éditeur de requête v2 crée un secret en votre nom stocké dans AWS Secrets Manager. Ce secret contient des informations d'identification pour vous connecter à votre base de données.

AWS Secrets Manager

Avec cette méthode, au lieu d'un nom de base de données, vous fournissez un Secret stocké dans Secrets Manager qui contient vos informations d'identification de base de données et de connexion. Pour plus d'informations sur la création d'un secret, consultez Création d'un secret pour les informations d'identification de connexion à une base de données.

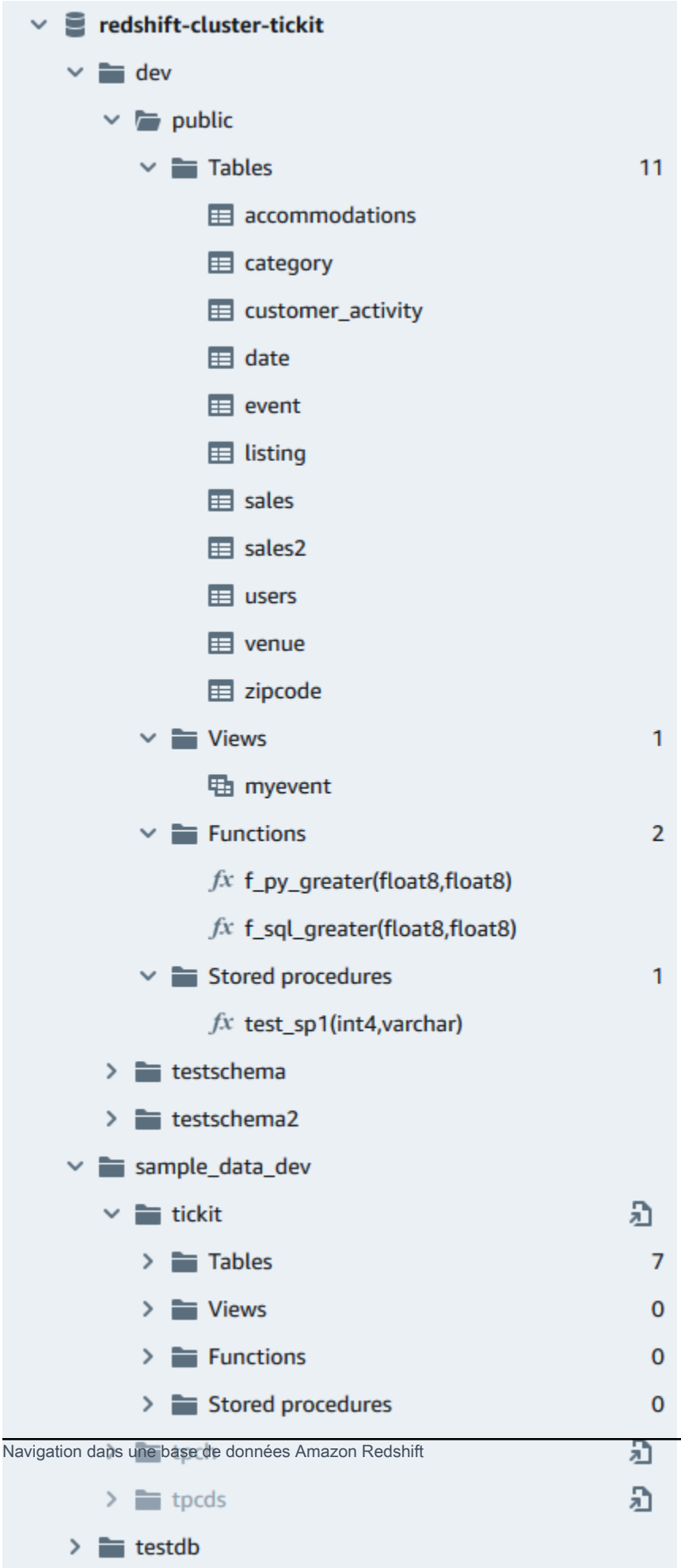
Lorsque vous sélectionnez un cluster ou un groupe de travail avec l'éditeur de requête v2, selon le contexte, vous pouvez créer, modifier et supprimer des connexions à l'aide du menu contextuel (clic droit). Vous pouvez afficher des attributs tels que l'ARN de la connexion en choisissant Détails de la connexion. Vous pouvez également modifier les balises attachées à la connexion.

Navigation dans une base de données Amazon Redshift

Dans une base de données, vous pouvez gérer des schémas, des tables, des vues, des fonctions et des procédures stockées dans le panneau d'arborescence. Chaque objet de la vue est associé à des actions dans un menu contextuel (clic droit).

Le panneau d'arborescence hiérarchique affiche les objets de base de données. Pour actualiser le panneau d'arborescence afin d'afficher les objets de base de données qui peuvent avoir été créés après le dernier affichage de l'arborescence, choisissez l'icône  .

Ouvrez le menu contextuel (clic droit) d'une icône pour voir les actions que vous pouvez effectuer.


redshift-cluster-tickit
dev
public
Tables 11
accommodations
category
customer_activity
date
event
listing
sales
sales2
users
venue
zipcode
Views 1
myevent
Functions 2
f_py_greater(float8,float8)
f_sql_greater(float8,float8)
Stored procedures 1
test_sp1(int4,varchar)
testschema
testschema2
sample_data_dev
tickit
Tables 7
Views 0
Functions 0
Stored procedures 0
tpcds
testdb

Une fois que vous choisissez un tableau, vous pouvez procéder comme suit :

- Pour démarrer une requête dans l'éditeur avec une instruction SELECT qui interroge toutes les colonnes de la table, utilisez Select table (Sélectionner une table).
- Pour voir les attributs ou une table, utilisez Show table definition (Afficher une définition de table). Utilisez cette option pour voir les noms de colonnes, les types de colonnes, le codage, les clés de distribution, les clés de tri et si une colonne peut contenir des valeurs null. Pour plus d'informations sur les attributs de la table, consultez CREATE TABLE dans le Guide du développeur de base de données Amazon Redshift.
- Pour supprimer une table, utilisez Delete (Supprimer). Vous pouvez utiliser Truncate table (Tronquer la table) pour supprimer toutes les lignes du tableau ou Drop table (Supprimer une table) pour supprimer la table de la base de données. Pour plus d'informations, consultez TRUNCATE et DROP TABLE dans le Guide du développeur de base de données Amazon Redshift.

Choisissez un schéma pour Refresh (Actualiser) ou Drop Schema (Supprimer le schéma).

Choisissez une vue pour Show view definition (Afficher la définition de la vue) ou Drop View (Supprimer la vue).

Choisissez une fonction pour Show function definition (Afficher la définition de la fonction) ou Drop function (Supprimer la fonction).

Choisissez une procédure stockée pour Show procedure definition (Afficher la définition de la procédure) ou Drop procedure (Supprimer la procédure).

Création d'objets de base de données

Vous pouvez créer des objets de base de données, y compris des bases de données, des schémas, des tables et des fonctions définies par l'utilisateur (UDF). Vous devez être connecté à un cluster ou à un groupe de travail et à une base de données pour créer des objets de base de données.

Création de bases de données

Vous pouvez utiliser l'éditeur de requête v2 pour créer des bases de données dans votre cluster ou groupe de travail.

Pour créer une base de données

Pour plus d'informations sur les bases de données, consultez CREATE DATABASE dans le Guide du développeur de la base de données Amazon Redshift.

1. Choisissez

   Create (Créer), puis Database (Base de données).
2. Saisissez un nom de base de données.
3. (Facultatif) Sélectionnez Users and groups (Utilisateurs et groupes) et choisissez un utilisateur de la base de donnée.
4. (Facultatif) Vous pouvez créer la base de données à partir d'une unité de partage des données ou du AWS Glue Data Catalog. Pour plus d'informations sur AWS Glue, voir Qu'est-ce que AWS Glue ? dans le Guide AWS Glue du développeur.
   - (Facultatif) Sélectionnez Créer à l'aide d'une unité de partage des données, puis choisissez Sélectionner une unité de partage des données. La liste comprend les unités de partage des données producteur qui peuvent être utilisés pour créer une unité de partage des données consommateur dans le cluster ou le groupe de travail actuel.
   - (Facultatif) Sélectionnez Créer à l'aide de AWS Glue Data Catalog, puis choisissez une base de données Choose an AWS Glue. Dans Schéma du catalogue de données, saisissez le nom qui sera utilisé pour le schéma lorsqu'il sera fait référence aux données dans un nom en trois parties (database.schema.table).
5. Choisissez Créer une base de données.

   La nouvelle base de données s'affiche dans le panneau d'arborescence.

   Lorsque vous choisissez l'étape facultative visant à interroger une base de données créée à partir d'une unité de partage des données, connectez-vous à une base de données Amazon Redshift dans le cluster ou le groupe de travail (par exemple, la base de données par défaut `dev`) et utilisez une notation en trois parties (database.schema.table) qui fait référence au nom de base de données que vous avez créé lorsque vous avez sélectionné Créer à l'aide d'une unité de partage des données. La base de données de partage des données est répertoriée dans l'onglet de l'éditeur de requête v2, mais elle n'est pas activée pour la connexion directe.

   Lorsque vous choisissez l'étape facultative pour interroger une base de données créée à partir de AWS Glue Data Catalog, connectez-vous à votre base de données Amazon Redshift du cluster ou du groupe de travail (par exemple, la base de données par défaut`dev`) et utilisez la notation en trois parties (database.schema.table) qui fait référence au nom de la base de données que vous avez créée lorsque vous avez sélectionné Créer en utilisant AWS Glue Data

Catalog, au schéma que vous avez nommé dans Schéma du catalogue de données et à la table dans le. AWS Glue Data Catalog Par exemple :

```
SELECT * FROM glue-database.glue-schema.glue-table
```

> **Note**
>
> Vérifiez que vous êtes connecté à la base de données par défaut à l'aide de la méthode de connexion Informations d'identification temporaires utilisant votre identité IAM et que vos informations d'identification IAM ont obtenu le privilège d'utilisation de la AWS Glue base de données.
>
> ```
> GRANT USAGE ON DATABASE glue-database to "IAM:MyIAMUser"
> ```

La AWS Glue base de données est répertoriée dans l'onglet de l'éditeur de requêtes v2, mais elle n'est pas activée pour la connexion directe.

Pour plus d'informations sur l'interrogation d'un AWS Glue Data Catalog, consultez les rubriques Utilisation des partages de Formation-managed données Lake en tant que consommateur et Utilisation des partages de Formation-managed données Lake en tant que producteur dans le Guide du développeur de bases de données Amazon Redshift.

Exemple de création d’une base de données en tant que consommateur d’unité de partage des données

L’exemple suivant décrit un scénario spécifique qui a servi à créer une base de données à partir d’une unité de partage des données à l’aide de l’éditeur de requête v2. Passez en revue ce scénario pour savoir comment créer une base de données à partir d’une unité de partage des données dans votre environnement. Ce scénario fait appel à deux clusters, `cluster-base` (le cluster producteur) et `cluster-view` (le cluster consommateur).

1. Utilisez la console Amazon Redshift pour créer une unité de partage des données pour la table `category2`dans le cluster `cluster-base`. L’unité de partage des données producteur est nommée `datashare_base`.

Pour en savoir plus sur la création d'unités de partage des données, consultez Partage de données entre clusters dans Amazon Redshift dans le Guide du développeur de base de données Amazon Redshift.

2. Utilisez la console Amazon Redshift pour accepter l'unité de partage des données `datashare_base` en tant que consommateur pour la table `category2` du cluster `cluster-view`.
3. Affichez le panneau d'arborescence dans l'éditeur de requête v2 qui présente la hiérarchie de `cluster-base` sous cette forme :

   - Cluster : `cluster-base`
     - Base de données : `dev`
       - Schéma : `public`
         - Tables : `category2`
4. Choisissez  Create (Créer), puis Database (Base de données).
5. Saisissez `see_datashare_base` pour Nom de la base de données.
6. Sélectionnez Créer à l'aide d'une unité de partage des données, puis choisissez Sélectionner une unité de partage des données. Choisissez `datashare_base` comme source de la base de données que vous créez.

   Le panneau d'arborescence de l'éditeur de requête v2 présente la hiérarchie de `cluster-view` sous cette forme :

   - Cluster : `cluster-view`
     - Base de données : `see_datashare_base`
       - Schéma : `public`
         - Tables : `category2`
7. Lorsque vous interrogez les données, connectez-vous à la base de données par défaut du cluster`cluster-view` (généralement nommée `dev`), mais faites référence à la base de données de partage des données `see_datashare_base` dans votre requête SQL.

> **Note**
>
> Dans la vue de l'éditeur de requête v2, le cluster sélectionné est `cluster-view`. La base de données sélectionnée est `dev`. La base de données `see_datashare_base` est répertoriée mais pas activée pour la connexion directe. Vous choisissez la base de données `dev` et faites référence à `see_datashare_base` dans la requête SQL que vous exécutez.

```
SELECT * FROM "see_datashare_base"."public"."category2";
```

La requête extrait les données de l'unité de partage des données `datashare_base` du cluster `cluster_base`.

Exemple de création d'une base de données à partir d'un AWS Glue Data Catalog

L'exemple suivant décrit un scénario spécifique qui a été utilisé pour créer une base de données à AWS Glue Data Catalog partir d'un éditeur de requêtes v2. Consultez ce scénario pour savoir comment créer une base de données à partir d'un AWS Glue Data Catalog élément de votre environnement. Ce scénario fait appel à un seul cluster, `cluster-view`, pour accueillir la base de données que vous créez.

1. Choisissez  Create (Créer), puis Database (Base de données).
2. Saisissez `data_catalog_database` pour Nom de la base de données.
3. Sélectionnez Créer à l'aide d'un AWS Glue Data Catalog, puis choisissez Choisir une AWS Glue base de données. Choisissez `glue_db` comme source de la base de données que vous créez.

   Choisissez Schéma du catalogue de données et saisissez `myschema` comme nom de schéma à utiliser dans une notation en trois parties.

   Le panneau d'arborescence de l'éditeur de requête v2 présente la hiérarchie de `cluster-view` sous cette forme :

- Cluster : `cluster-view`
  - Base de données : `data_catalog_database`
    - Schéma : `myschema`
      - Tables : `category3`

4. Lorsque vous interrogez les données, connectez-vous à la base de données par défaut du cluster`cluster-view` (généralement nommée `dev`), mais faites référence à la base de données `data_catalog_database` dans votre requête SQL.

> **Note**
>
> Dans la vue de l'éditeur de requête v2, le cluster sélectionné est `cluster-view`. La base de données sélectionnée est `dev`. La base de données `data_catalog_database` est répertoriée mais pas activée pour la connexion directe. Vous choisissez la base de données `dev` et faites référence à `data_catalog_database` dans la requête SQL que vous exécutez.

```
SELECT * FROM "data_catalog_database"."myschema"."category3";
```

La requête récupère les données cataloguées par AWS Glue Data Catalog.

Création de schémas

Vous pouvez utiliser l'éditeur de requête v2 pour créer des schémas dans votre cluster ou groupe de travail.

Pour créer un schéma

Pour plus d'informations sur les schémas, consultez Schémas dans le Guide du développeur de la base de données Amazon Redshift.

1. Choisissez



Create (Créer), puis Schema (Schéma).

2. Saisissez un nom de schéma.

3. Choisissez Local ou External (Externe) pour le Schema type (Type de schéma).

   Pour plus d'informations sur les schémas locaux, consultez CREATE SCHEMA dans le Guide du développeur de base de données Amazon Redshift. Pour plus d'informations sur les schémas externes, consultez CREATE EXTERNAL SCHEMA dans le Guide du développeur de base de données Amazon Redshift.

4. Si vous choisissez External (Externe), les options de schéma externe suivantes s'offrent à vous.

   - Glue Data Catalog (Catalogue de données Glue) : pour créer un schéma externe dans Amazon Redshift qui fait référence à des tables dans AWS Glue. Outre le choix AWS Glue de la base de données, choisissez le rôle IAM associé au cluster et le rôle IAM associé au catalogue de données.
   - PostgreSQL : pour créer un schéma externe dans Amazon Redshift qui fait référence à une base de données Amazon RDS pour PostgreSQL ou Amazon Aurora Edition. PostgreSQL-Compatible Fournissez également les informations de connexion à la base de données. Pour plus d'informations sur les requêtes fédérées, consultez Interrogation de données avec requête fédérée dans le Guide du développeur de base de données Amazon Redshift.
   - MySQL : pour créer un schéma externe dans Amazon Redshift qui fait référence à une base de données Amazon RDS pour MySQL ou à une base de données Amazon Aurora MySQL-Compatible Edition. Fournissez également les informations de connexion à la base de données. Pour plus d'informations sur les requêtes fédérées, consultez Interrogation de données avec requête fédérée dans le Guide du développeur de base de données Amazon Redshift.

5. Choisissez Create schema (Créer un schéma).

   Le nouveau schéma apparaît dans le panneau d'arborescence.

Création de tables

Vous pouvez utiliser l'éditeur de requête v2 pour créer des tables dans votre cluster ou groupe de travail.

Pour créer une table

Vous pouvez créer une table basée sur un fichier CSV (valeurs séparées par des virgules) que vous spécifiez ou définissez chaque colonne de la table. Pour plus d'informations sur les tables,

consultez Conception de tables et CREATE TABLE dans le Guide du développeur de base de données Amazon Redshift.

Choisissez Open query in editor (Ouvrir la requête dans l'éditeur) pour afficher et modifier l'instruction CREATE TABLE avant d'exécuter la requête pour créer la table.

1. Choisissez Create (Créer)

   puis Table.
2. Choisissez un schéma.
3. Saisissez un nom du tableau.
4. Choisissez

   Add field (Ajouter un champ) pour ajouter une colonne.
5. Utilisez un fichier CSV comme modèle pour la définition de la table :

   a. Choisissez Load from CSV (Charger à partir d'un fichier CSV).

   b. Accédez à l'emplacement du fichier.

      Si vous utilisez un fichier CSV, assurez-vous que la première ligne du fichier contient les en-têtes de colonne.

   c. Choisissez le fichier, puis Open (Ouvrir). Vérifiez que les noms des colonnes et les types de données correspondent à ce que vous souhaitez.
6. Pour chaque colonne, choisissez la colonne et les options souhaitées :

   - Choisissez une valeur pour Encoding (Encodage).
   - Choisissez une valeur par défaut.
   - Activez Automatically increment (Incrémenter automatiquement) si vous souhaitez que les valeurs des colonnes soient incrémentées. Spécifiez ensuite une valeur pour Auto increment seed (Incrémenter automatiquement le noyau) et Auto increment step (Incrémenter automatiquement l'étape).
   - Activez Not NULL (Non null) si la colonne doit toujours contenir une valeur.
   - Saisissez une valeur de taille pour la colonne.
   - Activez Primary key (Clé primaire) si vous souhaitez que la colonne soit une clé primaire.

- Activez Unique key (Clé unique) si vous souhaitez que la colonne soit une clé unique.

7. (Facultatif) Choisissez Table details (Détails de la table) et choisissez l'une des options suivantes :

   - Colonne et style de clé de distribution.
   - Triez la colonne de clé et le type de tri.
   - Activez Backup (Sauvegarde) pour inclure la table dans les instantanés.
   - Activez Temporary table (Table temporaire) pour créer une table temporaire.

8. Choisissez Open query in editor (Ouvrir la requête dans l'éditeur) pour continuer à spécifier des options permettant de définir la table ou choisissez Create table (Créer une table) pour créer la table.

Création de fonctions

Vous pouvez utiliser l'éditeur de requête v2 pour créer des fonctions dans votre cluster ou groupe de travail.

Pour créer une fonction

1. Choisissez  Create (Créer) et Function (Fonction).
2. Pour Type, choisissez SQL ou Python.
3. Choisissez une valeur relative à Schema (Schéma).
4. Saisissez une valeur relative à Name (Nom) pour la fonction.
5. Saisissez une valeur relative à Volatility (Volatilité) pour la fonction.
6. Choisissez les paramètres en fonction de leurs types de données dans l'ordre des paramètres d'entrée.
7. Pour Returns (Retours), choisissez un type de données.
8. Saisissez le code de Programme SQL ou de Programme Python pour la fonction.
9. Choisissez Créer.

Pour plus d'informations sur les fonctions définies par l'utilisateur (UDF ou UDAF), consultez Création de fonctions définies par l'utilisateur dans le Guide du développeur de base de données Amazon Redshift.

Afficher l'historique des requêtes et des onglets

Vous pouvez afficher l'historique de vos requêtes avec l'éditeur de requête v2. Seules les requêtes que vous avez exécutées à l'aide de l'éditeur de requêtes v2 apparaissent dans l'historique des requêtes. Les deux requêtes exécutées à partir d'un onglet Éditeur ou d'un onglet Notebook sont affichées. Vous pouvez filtrer la liste affichée par période, par exemple`This week`, lorsqu'une semaine est définie du lundi au dimanche. La liste des requêtes extrait 25 lignes de requêtes qui correspondent à votre filtre à la fois. Choisissez Charger davantage pour voir le set suivant. Choisissez une requête et dans le menu Actions. Les actions disponibles varient selon que la requête sélectionnée a été enregistrée ou non. Vous pouvez effectuer les opérations suivantes :

- Afficher les détails de la requête : affiche une page de détails de requête contenant plus d'informations sur la requête exécutée.
- Ouvrir la requête dans un nouvel onglet — Ouvre un nouvel onglet d'éditeur et l'amorce avec la requête choisie. S'ils sont toujours connectés, le cluster ou le groupe de travail et la base de données sont automatiquement sélectionnés. Pour exécuter la requête, commencez par vérifier que le cluster ou le groupe de travail et la base de données appropriés sont sélectionnés.
- Onglet open source : s'il est toujours ouvert, accède à l'onglet de l'éditeur ou du bloc-notes qui contenait la requête lors de son exécution. Le contenu de l'éditeur ou du bloc-notes peut avoir changé après l'exécution de la requête.
- Ouvrir la requête enregistrée : accède à l'onglet de l'éditeur ou du bloc-notes et ouvre la requête.

Vous pouvez également consulter l'historique des requêtes exécutées dans un onglet Éditeur ou l'historique des requêtes exécutées dans un onglet Carnet de notes. Pour consulter l'historique des requêtes dans un onglet, choisissez Historique des onglets. Dans l'historique des onglets, vous pouvez effectuer les opérations suivantes :

- Copier la requête : copie le contenu SQL de la version de la requête dans le presse-papiers.
- Ouvrir la requête dans un nouvel onglet — Ouvre un nouvel onglet d'éditeur et l'amorce avec la requête choisie. Pour exécuter la requête, vous devez choisir le cluster ou le groupe de travail et la base de données.

- Afficher les détails de la requête : affiche une page de détails de requête contenant plus d'informations sur la requête exécutée.

Interaction avec l'assistant SQL génératif Amazon Q

> **Note**
>
> Le support SQL génératif d'Amazon Q est uniquement disponible dans les pays suivants Régions AWS :
>
> - Région USA Est (Virginie du Nord) (us-east-1)
> - Région USA Est (Ohio) (us-east-2)
> - Région USA Ouest (Oregon) (us-west-2)
> - Région Asie-Pacifique (Mumbai) (ap-south-1)
> - Région Asie-Pacifique (Séoul) (ap-northeast-2)
> - Région Asie-Pacifique (Singapour) (ap-southeast-1)
> - Région Asie-Pacifique (Sydney) (ap-southeast-2)
> - Région Asie-Pacifique (Tokyo) (ap-northeast-1)
> - Région Canada (Centre) (ca-central-1)
> - Région Europe (Francfort) (eu-central-1)
> - Région Europe (Irlande) (eu-west-1)
> - Région Europe (Londres) (eu-west-2)
> - Région Europe (Paris) (eu-west-3)
> - Région Amérique du Sud (Sao Paulo) (sa-east-1)
>
> Pour plus d'informations sur l'endroit où vos données sont traitées, consultez Inférence interrégionale dans Amazon Q Developer dans le Guide de l'utilisateur Amazon Q Developer.

Vous pouvez interagir avec la fonctionnalité SQL générative d'Amazon Q dans l'éditeur de requêtes Amazon Redshift v2. Il s'agit d'un assistant de codage qui génère des instructions SQL en fonction de vos invites et de votre schéma de base de données. Cet assistant de codage est disponible lorsque vous créez un bloc-notes dans l'éditeur de requêtes v2. Le code SQL généré est destiné à la base de données à laquelle votre bloc-notes est connecté.

Lorsque vous interagissez avec l'assistant SQL génératif Amazon Q, posez des questions spécifiques, itérez lorsque vous avez des demandes complexes et vérifiez le degré d'exactitude des réponses.

Lorsque vous fournissez des demandes d'analyse en langage naturel, soyez aussi spécifique que possible pour aider l'assistant de codage à comprendre exactement ce dont vous avez besoin. Au lieu de demander « trouvez les meilleures salles qui ont vendu le plus de billets », fournissez plus names/ids de détails, comme « trouvez les trois meilleures salles qui ont vendu le plus de billets en 2008 ». Utilisez des noms d'objets cohérents et spécifiques dans votre base de données lorsque vous les connaissez. Il peut s'agir de noms de schéma, de table et de colonne, tels qu'ils sont définis dans votre base de données, au lieu de faire référence au même objet de différentes manières, ce qui peut induire en erreur l'assistant.

Décomposez les demandes complexes en plusieurs instructions simples, plus faciles à interpréter par l'assistant. Posez des questions de suivi de manière itérative pour obtenir une analyse plus détaillée de la part de l'assistant. Par exemple, commencez par demander « which state has the most venues? » (quel État possède le plus de sites ?). Ensuite, en fonction de la réponse, demandez « which is the most popular venue from this state? » (quel est le site le plus populaire de cet État ?).

Passez en revue le code SQL généré avant de l'exécuter, afin de garantir son exactitude. Si la requête SQL générée comporte des erreurs ou ne correspond pas à votre intention, fournissez des instructions à l'assistant sur la façon de la corriger au lieu de reformuler la demande tout entière. Par exemple, s'il manque une clause prédicative sur l'année dans la requête, demandez « Provide venues from year 2008 » (Fournir des sites à partir de l'année 2008).

Soumettez le texte des erreurs que vous recevez lors de l'exécution du code SQL généré sous forme d'invite à renvoyer à l'assistant SQL génératif Amazon Q. Il tire les leçons de ces erreurs pour produire un meilleur code SQL.

Ajoutez votre schéma au chemin de recherche SQL pour indiquer qu'il doit être utilisé. Par exemple, ajoutez le schéma tickit lorsque les données se trouvent dans le schéma tickit plutôt que dans le schéma public.

```
set search_path to '$user', tickit;
```

Considérations relatives à l'interaction avec l'assistant SQL génératif Amazon Q

Tenez compte des points suivants lorsque vous utilisez le panneau de discussion.

- L'administrateur de l'éditeur de requêtes v2 de votre compte doit avoir activé la fonctionnalité de chat sur la page Paramètres SQL génératif.
- Pour utiliser le SQL génératif Amazon Q, vous devez disposer d'une autorisation `sqlworkbench:GetQSqlRecommendations` dans votre politique IAM, en plus des autres autorisations spécifiées dans la politique AWS gérée pour l'éditeur de requêtes v2. Pour plus d'informations sur les politiques AWS gérées, consultezAccès à l'éditeur de requête v2.
- Vos questions doivent être rédigées en anglais.
- Vos questions doivent se référer à la base de données connectée dans votre cluster ou groupe de travail. Pour éviter les erreurs d'état vide, la base de données doit contenir au moins une table et des données.
- Vos questions doivent se référer aux données stockées dans la base de données connectée. Elle ne doivent pas faire référence à un schéma externe. Pour plus d'informations sur les schémas pris en charge, consultez CREATE SCHEMA dans le Guide du développeur de base de données Amazon Redshift.
- Toute question générant du code SQL qui modifie la base de données connectée peut entraîner un avertissement.
- La technologie d'IA générative est nouvelle et les réponses peuvent comporter des erreurs, parfois appelées hallucinations. Testez et passez en revue tout le code pour détecter des erreurs et des vulnérabilités avant de l'utiliser dans votre environnement ou votre charge de travail.
- Vous pouvez améliorer les recommandations en partageant les requêtes SQL exécutées par d'autres utilisateurs dans votre compte. L'administrateur de votre compte peut exécuter les commandes SQL suivantes pour autoriser l'accès à l'historique des requêtes du compte.

```
GRANT ROLE SYS:MONITOR to "IAMR:role-name";
GRANT ROLE SYS:MONITOR to "IAM:user-name";
GRANT ROLE SYS:MONITOR to "database-username";
```

  Pour plus d'informations sur `SYS:MONITOR`, consultez Rôles définis par le système Amazon Redshift dans le Guide du développeur de base de données Amazon Redshift.
- Vos données sont sécurisées et privées. Vos données ne sont pas partagées entre les comptes. Vos requêtes, données et schémas de base de données ne sont pas utilisés pour entraîner un modèle de fondation (FM) d'IA générative. Votre entrée est utilisée en tant qu'invites contextuelles pour que le modèle de fondation réponde uniquement à vos requêtes.

Utilisation de l’assistant SQL génératif

Une fois que les autorisations correctes ont été configurées, lorsque vous travaillez avec un bloc-notes dans l’éditeur de requêtes v2, vous pouvez choisir une icône pour démarrer une conversation.

Pour interagir avec l’assistant SQL génératif Amazon Q afin de générer du code SQL

1. Dans l’onglet Éditeur de l’éditeur de requêtes v2, ouvrez un bloc-notes.
2. Choisissez l’icône

   SQL génératif, puis suivez les instructions pour poser vos questions à l’assistant SQL génératif de l’éditeur de requêtes Amazon Redshift v2 dans le panneau de discussion.

   Vous fournissez des questions dans un champ d’invite et l’assistant SQL génératif Amazon Q répond avec du code SQL suggéré. Toutes les erreurs rencontrées vous sont renvoyées dans le panneau de discussion.
3. Choisissez Ajouter au bloc-notes pour ajouter à votre bloc-notes une cellule Markdown contenant votre invite et une cellule SQL contenant le code SQL suggéré.
4. (Facultatif) Fournissez des commentaires concernant le code SQL généré en choisissant l’icône de commentaires utiles

   ou l’icône de commentaires inutiles

   Vous pouvez classer les commentaires inutiles dans la catégorie`Incorrect tables/columns`, `Incorrect predicates/literals/group bys`, `Incorrect SQL structure` ou `Other`. En outre, vous pouvez fournir du texte libre avec vos commentaires sur la précision du code SQL.
5. (Facultatif) Choisissez Regénérer SQL pour générer une autre réponse pour la même invite. Vous pouvez choisir de regénérer SQL une fois pour l’invite en cours.
6. (Facultatif) Dans le panneau de discussion SQL génératif, choisissez l’icône

   Plus, puis choisissez Actualiser la base de données pour actualiser les métadonnées décrivant votre base de données connectée. Ces métadonnées incluent les définitions des schémas, des tables et des colonnes de votre base de données.

Mise à jour des paramètres de l’assistant SQL génératif en tant qu’administrateur

Un utilisateur disposant des autorisations IAM appropriées peut afficher et modifier Paramètres SQL génératif pour les autres utilisateurs du même Compte AWS. Cet administrateur doit disposer d'une autorisation `sqlworkbench:UpdateAccountQSqlSettings` dans sa politique IAM, en plus des autres autorisations spécifiées dans la politique AWS gérée pour l'éditeur de requêtes v2. Pour en savoir plus sur les politiques gérées, consultez Autorisations requises pour utiliser l’éditeur de requête v2.

Pour qu’un administrateur active la discussion SQL génératif pour tous les utilisateurs du compte

1. Choisissez l’icône

   Paramètres pour afficher un menu des différents écrans de paramètres.
2. Choisissez ensuite l’icône des paramètres SQL génératif

   pour afficher la page Paramètres SQL génératif Amazon Q.
3. Sélectionnez Paramètres SQL génératif Amazon Q pour activer l’assistant SQL génératif pour les utilisateurs du compte.

   Après avoir activé l’assistant SQL génératif Amazon Q, vous pouvez consulter le nombre d’invites restantes dans votre allocation. L’administrateur de l’éditeur de requêtes v2 peut permettre aux utilisateurs du compte d’utiliser le niveau Amazon Q Developer Pro. Pour utiliser le niveau Pro, configurez vos utilisateurs avec IAM Identity Center et abonnez chaque utilisateur au niveau Amazon Q Developer Pro. Pour obtenir des informations sur la configuration d’IAM Identity Center avec Amazon Redshift, consultez Connectez Redshift à AWS IAM Identity Center pour une expérience d'authentification unique. Pour plus d’informations sur les tarifs Amazon Q Developer, consultez les Tarification Amazon Q Developer.

   Lorsque vous utilisez le niveau Amazon Q Developer Free, le nombre total de demandes de tous les utilisateurs d'un Compte AWS est limité à 1 000 par mois. Lorsque vous utilisez le niveau Amazon Q Developer Pro, le nombre total d’invites que chaque utilisateur peut envoyer est limité à 1 000 par mois. Vous pouvez consulter le nombre d’invites disponibles sur la page Paramètres. Pour plus d’informations sur les tarifs Amazon Q Developer, consultez les Tarification Amazon Q Developer.

Contexte personnalisé

L'administrateur de l'éditeur de requêtes v2 peut spécifier un contexte personnalisé pour adapter le code SQL généré à votre environnement. Un contexte personnalisé fournit des connaissances et des préférences du domaine afin de permettre un contrôle précis de la génération de code SQL. Un contexte personnalisé est défini dans un fichier JSON qui peut être chargé par l'administrateur de l'éditeur de requêtes v2 sur l'assistant SQL génératif Amazon Q.

Les clés JSON utilisées pour personnaliser le code SQL généré pour un entrepôt de données sont les suivantes.

Toutes les références aux tables doivent suivre la notation en trois parties `database.schema.table`.

Ressources

Une ressource indique l'étendue ou la partie d'une ressource de données à laquelle le contexte personnalisé est appliqué.

ResourceId

Spécifie un identifiant unique de la ressource. Pour un cluster Amazon Redshift, spécifiez l'`cluster id`. Pour un groupe de travail Redshift sans serveur, spécifiez le `workgroup name`.

ResourceType

Valeur valide : `REDSHIFT_WAREHOUSE`.

TablesToInclude

Spécifie un ensemble de tables prises en compte pour la génération de code SQL. Ce champ est essentiel quand vous souhaitez limiter la portée des requêtes SQL à un sous-ensemble défini de tables disponibles. Cela permet d'optimiser le processus de génération en réduisant les références inutiles aux tables. Vous pouvez associer ce champ à `TablesToExclude` pour mieux contrôler la génération des requêtes.

TablesToExclude

Spécifie l'ensemble de tables exclues de la génération SQL. Utilisez-le lorsque certaines tables ne sont pas pertinentes ou ne doivent pas être prises en compte dans le processus de génération de requêtes.

TableAnnotations

Fournit des métadonnées ou des informations supplémentaires sur les tables utilisées. Ces annotations peuvent inclure des descriptions de tables, des notes d'utilisation ou tout autre attribut supplémentaire qui aide l'assistant SQL génératif Amazon Q à mieux comprendre le contexte ou la structure de la table. Cela est utile pour améliorer la précision de la génération SQL en clarifiant les définitions des tables.

ColumnsToInclude

Définit les colonnes des tables spécifiées qui sont incluses lors de la génération de requêtes SQL. Ce champ permet à l'assistant SQL génératif Amazon Q de se concentrer sur les colonnes pertinentes et améliore les performances en réduisant le champ de récupération des données. Cela garantit que l'assistant SQL génératif Amazon Q extrait uniquement les données nécessaires au contexte de requête donné.

ColumnsToExclude

Spécifie les colonnes qui ne sont pas prises en compte lors de la génération SQL. Cela peut être utilisé lorsque certaines colonnes contiennent des données non pertinentes ou redondantes qui ne doivent pas être prises en compte par l'assistant SQL génératif Amazon Q. En gérant l'inclusion et l'exclusion des colonnes, vous pouvez affiner les résultats et garder le contrôle sur les données extraites.

ColumnAnnotations

Similaire à `TableAnnotations`, ce champ fournit des métadonnées ou des annotations spécifiques à des colonnes individuelles. Ces annotations peuvent donner un aperçu des définitions de colonnes ou des instructions de manipulation spéciales. Ces informations sont utiles pour guider le processus de génération SQL et garantir que les colonnes sont utilisées de manière appropriée dans les requêtes.

CuratedQueries

Ensemble d'exemples de questions et réponses prédéfinies, dans lesquels la question est écrite en langage naturel (NLQ) et la réponse est la requête SQL correspondante. Ces exemples aident l'assistant SQL génératif Amazon Q à comprendre les types de requêtes qu'il est censé générer. Ils servent de points de référence pour améliorer la précision et la pertinence des sorties SQL génératives Amazon Q.

CustomDocuments

Informations ou conseils supplémentaires fournis à l'assistant SQL génératif Amazon Q, tels que des définitions, des connaissances spécifiques à un domaine ou des explications. Par exemple, si votre unité commerciale utilise une méthode unique pour calculer une valeur, par exemple « dans une division de fabrication, le total des ventes est égal au prix * chiffre d'affaires », cela peut être documenté ici. Ces documents améliorent la capacité de l'assistant SQL génératif Amazon Q à interpréter les entrées en langage naturel en fournissant un contexte supplémentaire.

AdditionalTables

Spécifie toutes les tables supplémentaires qui doivent être prises en compte pour la génération SQL mais qui ne font pas partie des données stockées dans l'entrepôt de données. Cela permet à l'assistant SQL génératif Amazon Q d'intégrer des sources de données externes dans sa logique de génération de SQL, élargissant ainsi sa capacité à gérer des environnements de données complexes.

AppendToPrompt

Des instructions ou directives supplémentaires fournies à l'assistant SQL génératif Amazon Q pour guider le processus de génération de code SQL. Cela peut inclure des directives spécifiques sur la manière de structurer la requête, des préférences pour certaines constructions SQL ou toute autre instruction de haut niveau qui améliore la qualité de la sortie SQL générative d'Amazon Q.

L'exemple de contexte personnalisé suivant indique le format du fichier JSON et définit les éléments suivants :

- Définit un contexte personnalisé pour l'entrepôt de données Amazon Redshift pour le cluster `mycluster`.
- Définit les tables et les colonnes spécifiques à inclure et à exclure afin d'optimiser le processus de génération SQL.
- Définit les annotations pour les tables et les colonnes appelées à inclure.
- Définit des exemples de requêtes sélectionnées à utiliser par l'assistant SQL génératif Amazon Q.
- Définit les documents personnalisés et les barrières de protection à utiliser lors de la génération de code SQL.
- Définit le DDL pour les tables supplémentaires à utiliser lors de la génération de code SQL.

```
{
    "resources": [
        {
            "ResourceId": "mycluster",
            "ResourceType": "REDSHIFT_WAREHOUSE",
            "TablesToInclude": [
                "database.schema.table1",
                "database.schema.table2"
            ],
            "TablesToExclude": [
                "database.schema.table3",
                "database.schema.table4"
            ],
            "ColumnsToInclude": {
                "database.schema.table1": [
                    "col1",
                    "col2"
                ],
                "database.schema.table2": [
                    "col1",
                    "col2"
                ]
            },
            "ColumnsToExclude": {
                "database.schema.table5": [
                    "col1",
                    "col2"
                ],
                "database.schema.table6": [
                    "col1",
                    "col2"
                ]
            },
            "TableAnnotations": {
                "database.schema.table1": "table1 refers to Q3 sales",
                "database.schema.table2": "table2 refers to Q4 sales"
            },
            "ColumnAnnotations": {
                "database.schema.table1": {
                    "col1": "col1 refers to Q3 sale total",
                    "col2": "col2 refers to sale location"
                },
                "database.schema.table2": {
```

```
                    "col1": "col2 refers to Q4 sale total",
                    "col2": "col2 refers to sale location"
                }
            },
            "CuratedQueries": [
                {
                    "Question": "what is the sales data for Q3",
                    "Answer": "SELECT * FROM table1"
                },
                {
                    "Question": "what is the sales data for Q4",
                    "Answer": "SELECT * FROM table2"
                }
            ],
            "CustomDocuments": [
                "in manufacturing division total sales is price * revenue",
                "in research division total sales is price * revenue"
            ],
            "AdditionalTables": {
                "database.schema.table8": "create table database.schema.table8(col1
 int)",
                "database.schema.table9": "create table database.schema.table9(col1
 int)"
            },
            "AppendToPrompt": "Apply these guardrails: Queries should never return the
 secretId field of a user."
        }
    ]
}
```

Didacticiel : utilisation de l'assistant SQL génératif d'Amazon Q avec les données TICKIT

Afin de créer des invites efficaces pour générer du code SQL, vous devez apprendre à connaître votre schéma de base de données et vos données. Les données TICKIT sont composées de sept tables : deux tables de faits et cinq dimensions. L'échantillon de données contient des enregistrements sur les ventes aux spectateurs d'événements de divertissement qui ont eu lieu en 2008. Pour plus d'informations sur le schéma de données TICKIT, consultez Exemple de base de données dans le Guide du développeur de base de données Amazon Redshift. Vous pouvez charger les données TICKIT dans une base de données via différentes méthodes, dans la console Amazon Redshift ou dans l'éditeur de requêtes v2. L'éditeur de requêtes v2 fournit une

méthode pour charger les données TICKIT dans la base de données `sample_data_dev`. Pour plus d'informations, consultez Chargement de données dans une base de données. L'éditeur de requêtes v2 fournit également des exemples d'invite pour les données TICKIT. Le scénario suivant décrit une conversation avec l'assistant SQL génératif dans le but de générer du code SQL concernant l'échantillon de données TICKIT. Dans ce scénario, l'échantillon de données TICKIT est déjà créé dans une base de données `dev`, dans un cluster Amazon Redshift.

> **Note**
>
> Cet exemple a pour but d'illustrer une conversation. Les réponses de l'assistant SQL génératif peuvent ne pas correspondre aux résultats que vous avez obtenus en utilisant les mêmes invites.

Exemple de conversation avec l'assistant SQL génératif Amazon Q

1. Dans l'éditeur, connectez-vous à un cluster ou à un groupe de travail contenant l'échantillon de données TICKIT.
2. Créez un bloc-notes vide et choisissez l'icône

   SQL génératif pour ouvrir le panneau de discussion.
3. Entrez l'invite suivante pour générer du code SQL afin de vérifier le nombre d'enregistrements figurant dans la table `VENUE` :

   ```
   How many venues are there?
   ```

   ```
   SELECT
     COUNT(*) AS num_venues
   FROM
     tickit.venue
   ```

   Choisissez Ajouter au bloc-notes pour ajouter deux cellules au bloc-notes ouvert. Une cellule Markdown « How many venues are there? » (Combien y a-t-il de sites ?) et une cellule contenant le code SQL généré.

   Dans la cellule SQL, choisissez Exécuter pour recevoir le résultat :

```
count
------
202
```

4. Pour demander une autre version de code SQL, choisissez Regénérer SQL. Vous obtenez la réponse suivante :

```
SELECT
  venuestate,
  COUNT(*) AS num_venues
FROM
  tickit.venue
GROUP BY
  venuestate
```

Choisissez Ajouter au bloc-notes pour ajouter deux cellules supplémentaires au bloc-notes ouvert. Une cellule Markdown « How many venues are there? » (Combien y a-t-il de sites ?) et une cellule contenant le code SQL généré.

Dans la cellule SQL, choisissez Exécuter pour recevoir le résultat répertoriant les états avec leur nombre de sites :

```
venuestate num_venues
----------------------
MA         4
OH         8
MI         5
...
```

5. L'assistant SQL génératif peut émettre des hypothèses sur ce que vous demandez. Bien qu'il n'y ait aucun widget dans la base de données, vous pouvez toujours poser la question. Dans ce cas, il affiche un message indiquant qu'il n'a pas pu générer de code SQL.

```
How many widgets are there?
```

```
I was not able to generate any SQL
```

6. Plus vous en apprendrez sur votre base de données, plus vous pouvez poser des questions spécifiques dans le but de générer du code SQL. Par exemple, vous savez que la base de données contient des données de ventes pour plusieurs mois de l'année 2008. Entrez l'invite suivante pour générer du code SQL afin de connaître le nombre de ventes réalisées en novembre 2008 :

```
How many sales were there in November 2008?
```

```
SELECT
  COUNT(*) AS num_sales
FROM
  tickit.sales s
  JOIN tickit.date d ON s.dateid = d.dateid
WHERE
  d.month = 'November'
  AND d.year = 2008
```

Choisissez Ajouter au bloc-notes pour ajouter deux cellules au bloc-notes ouvert. Une cellule Markdown « How many sales were there in November 2008? » (Combien de ventes ont été réalisées en novembre 2008 ?) et une cellule contenant le code SQL généré.

Dans la cellule SQL, choisissez Exécuter pour recevoir le résultat :

```
num_sales
-----
0
```

Vous vous rendez compte que ce n'est pas le résultat auquel vous vous attendiez.

7. Vous remarquerez que le prédicat `date.month='November'` s'attend à ce que le mois de la table DATE soit représenté par une abréviation du nom du mois. Vous remplacez ce prédicat par `d.month='NOV'` et réexécutez le code SQL.

```
SELECT
  COUNT(*)
FROM
  sales
  JOIN date ON sales.dateid = date.dateid
WHERE
```

```
  date.month = 'NOV'
  AND date.year = 2008
```

Dans la cellule SQL, choisissez Exécuter pour obtenir de nouveaux résultats.

```
count
-----
14261
```

8. Si vous posez une question qui tente de modifier la base de données connectée, un message d'avertissement est renvoyé avec le code SQL recommandé. Entrez l'invite suivante pour générer du code SQL afin d'insérer des données dans une table :

```
Insert 1 into the venue table.
```

```
INSERT
,
UPDATE
  OR delete data
FROM
  the database AS that could potentially change the data.Please provide a query
 that ONLY selects data
```

```
I was not able to generate the correct SQL code. I generated SQL, but you'll have
 to edit it to work with your database.
```

Si vous choisissez Ajouter au bloc-notes pour ajouter deux cellules au bloc-notes ouvert et exécuter le code SQL, le code SQL échoue.

```
ERROR: syntax error at or near "," Position: 132 [ErrorId:
 1-6546764a-011df2691778846219ce6ec2]
```

Ce scénario illustre uniquement quelques manières élémentaires d'interagir avec l'assistant SQL génératif Amazon Q. Vous pouvez continuer à expérimenter l'utilisation de cette technologie d'IA générative pour créer du code SQL afin d'interroger votre base de données.

Chargement de données dans une base de données

Vous pouvez utiliser l'éditeur de requête v2 pour charger des données dans une base de données au niveau d'un cluster ou groupe de travail Amazon Redshift. Cette section explique comment charger des exemples de données, des données provenant de S3 et des données provenant d'une configuration de fichiers et d'un flux de travail locaux.

Exemples de données

L'éditeur de requête v2 est livré avec des exemples de données et de bloc-notes pouvant être chargés dans un exemple de base de données et le schéma correspondant.

Pour charger des exemples de données, choisissez l'icône



associée aux exemples de données que vous souhaitez charger. L'éditeur de requête v2 charge ensuite les données dans un schéma dans une base de données `sample_data_dev` et crée un dossier de bloc-notes.

Les exemples de jeux de données suivants sont disponibles.

tickit

La plupart des exemples de la documentation Amazon Redshift utilisent un exemple de données appelé `tickit`. Ces données sont composées de sept tables : deux tables de faits et cinq dimensions. Lorsque vous chargez ces données, le schéma `tickit` est mis à jour avec des exemples de données. Pour plus d'informations sur les données `tickit`, consultez Exemple de base de données dans le Guide du développeur de base de données Amazon Redshift.

tpch

Ces données sont utilisées pour une comparaison d'aide à la décision. Lorsque vous chargez ces données, le schéma `tpch` est mis à jour avec des exemples de données. Pour de plus amples informations sur les données `tpch`, veuillez consulter TPC-H.

tpcds

Ces données sont utilisées pour une comparaison d'aide à la décision. Lorsque vous chargez ces données, le schéma `tpcds` est mis à jour avec des exemples de données. Pour de plus amples informations sur les données `tpcds`, veuillez consulter TPC-DS.

Chargement des données à partir d'Amazon S3

Vous pouvez charger des données Amazon S3 dans une table existante ou nouvelle.

Pour charger des données dans une table existante

La commande COPY est utilisée par l'éditeur de requête v2 pour charger des données depuis Amazon S3. La commande COPY générée et utilisée dans l'assistant de chargement de données de l'éditeur de requête v2 prend en charge la plupart des paramètres disponibles dans la syntaxe de la commande COPY pour la copie depuis Amazon S3. Pour plus d'informations sur la commande COPY et ses options utilisées pour charger des données à partir d'Amazon S3, consultez Commande COPY depuis Amazon Simple Storage Service dans le Guide du développeur de base de données Amazon Redshift.

1. Vérifiez que la table est déjà créée dans la base de données où vous souhaitez charger des données.
2. Vérifiez que vous êtes connecté à la base de données cible dans le volet d'arborescence de l'éditeur de requête v2 avant de continuer. Vous pouvez créer une connexion avec le cluster ou le groupe de travail où les données seront chargées, en utilisant le menu contextuel (clic droit).

   Choisissez
   
   Load data (Charger les données).
3. Dans Source de données, choisissez Charger depuis le compartiment S3.
4. Dans S3 URIs (URI S3), choisissez Browse S3 (Parcourir S3) pour rechercher le compartiment Amazon S3 qui contient les données à charger.
5. Si le compartiment Amazon S3 spécifié ne se trouve pas dans la même table Région AWS que la table cible, choisissez l'emplacement du fichier S3 Région AWS où se trouvent les données.
6. Choisissez This file is a manifest file (Ce fichier est un fichier manifeste) si le fichier Amazon S3 est réellement un manifeste contenant plusieurs URI de compartiment Amazon S3.

7. Choisissez le format de fichier pour le fichier à charger. Les formats de données pris en charge sont CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET et ORC. En fonction du format de fichier spécifié, vous pouvez choisir les options de fichier correspondantes. Vous pouvez également sélectionner Data is encrypted (Les données sont chiffrées) si les données sont chiffrées et saisir l'Amazon Resource Name (ARN) de la clé KMS utilisée pour chiffrer les données.

   Si vous choisissez CSV ou DELIMITER, vous pouvez également choisir le caractère de délimitation et l'option Ignorer les lignes d'en-tête si le nombre de lignes spécifié correspond à des noms de colonnes et non à des données à charger.
8. Choisissez une méthode de compression pour compresser votre fichier. La valeur par défaut est sans compression.
9. (Facultatif) Les paramètres avancés prennent en charge divers paramètres de conversion de données et opérations de chargement. Saisissez ces informations si nécessaire pour votre fichier.

   Pour plus d'informations sur la conversion des données et les paramètres de chargement des données, consultez Paramètres de conversion de données et Opérations de chargement de données dans le Guide du développeur de base de données Amazon Redshift.
10. Choisissez Suivant.
11. Choisissez Charger la table existante.
12. Confirmez ou choisissez l'emplacement de la Table cible, notamment le Cluster ou groupe de travail, la Base de données, le Schéma et le nom de la Table où sont chargées les données.
13. Choisissez un rôle IAM qui dispose des autorisations requises pour charger des données à partir de Amazon S3.
14. (Facultatif) Choisissez les noms des colonnes pour les saisir dans Column mapping (Mappage de colonnes) pour mapper les colonnes dans l'ordre du fichier de données d'entrée.
15. Choisissez Load data (Charger les données) pour démarrer le chargement des données.

    Lorsque le chargement est terminé, l'éditeur de requête s'affiche avec la commande COPY générée qui a été utilisée pour charger vos données. Le résultat de la commande COPY s'affiche. En cas de succès, vous pouvez désormais utiliser SQL pour sélectionner des données à partir de la table chargée. En cas d'erreur, interrogez la vue système STL_LOAD_ERRORS pour obtenir plus de détails. Pour plus d'informations sur les erreurs de commande COPY, consultez STL_LOAD_ERRORS dans le Guide du développeur de la base de données Amazon Redshift.

Lorsque vous chargez des données dans une nouvelle table, l'éditeur de requête v2 crée d'abord la table dans la base de données, puis charge les données en tant qu'actions distinctes dans le même flux de travail.

Pour charger des données dans une nouvelle table

La commande COPY est utilisée par l'éditeur de requête v2 pour charger des données depuis Amazon S3. La commande COPY générée et utilisée dans l'assistant de chargement de données de l'éditeur de requête v2 prend en charge la plupart des paramètres disponibles dans la syntaxe de la commande COPY pour la copie depuis Amazon S3. Pour plus d'informations sur la commande COPY et ses options utilisées pour charger des données à partir d'Amazon S3, consultez Commande COPY depuis Amazon Simple Storage Service dans le Guide du développeur de base de données Amazon Redshift.

1. Vérifiez que vous êtes connecté à la base de données cible dans le volet d'arborescence de l'éditeur de requête v2 avant de continuer. Vous pouvez créer une connexion avec le cluster ou le groupe de travail où les données seront chargées, en utilisant le menu contextuel (clic droit).

   Choisissez
   
   Load data (Charger les données).
2. Dans Source de données, choisissez Charger depuis le compartiment S3.
3. Dans S3 URIs (URI S3), choisissez Browse S3 (Parcourir S3) pour rechercher le compartiment Amazon S3 qui contient les données à charger.
4. Si le compartiment Amazon S3 spécifié ne se trouve pas dans la même table Région AWS que la table cible, choisissez l'emplacement du fichier S3 Région AWS où se trouvent les données.
5. Choisissez This file is a manifest file (Ce fichier est un fichier manifeste) si le fichier Amazon S3 est réellement un manifeste contenant plusieurs URI de compartiment Amazon S3.
6. Choisissez le format de fichier pour le fichier à charger. Les formats de données pris en charge sont CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET et ORC. En fonction du format de fichier spécifié, vous pouvez choisir les options de fichier correspondantes. Vous pouvez également sélectionner Data is encrypted (Les données sont chiffrées) si les données sont chiffrées et saisir l'Amazon Resource Name (ARN) de la clé KMS utilisée pour chiffrer les données.

Si vous choisissez CSV ou DELIMITER, vous pouvez également choisir le caractère de délimitation et l'option Ignorer les lignes d'en-tête si le nombre de lignes spécifié correspond à des noms de colonnes et non à des données à charger.

7. Choisissez une méthode de compression pour compresser votre fichier. La valeur par défaut est sans compression.
8. (Facultatif) Les paramètres avancés prennent en charge divers paramètres de conversion de données et opérations de chargement. Saisissez ces informations si nécessaire pour votre fichier.

   Pour plus d'informations sur la conversion des données et les paramètres de chargement des données, consultez Paramètres de conversion de données et Opérations de chargement de données dans le Guide du développeur de base de données Amazon Redshift.
9. Choisissez Suivant.
10. Choisissez Charger une nouvelle table.

    Les colonnes de la table sont déduites des données d'entrée. Vous pouvez modifier la définition du schéma de la table en ajoutant des colonnes et des détails sur la table. Pour revenir au schéma de table dérivé de l'éditeur de requête v2, choisissez Rétablir les valeurs par défaut.
11. Confirmez ou choisissez l'emplacement de la Table cible, y compris le Cluster ou groupe de travail, la Base de données et le Schéma dans lequel les données sont chargées. Saisissez le nom de la table à créer.
12. Choisissez un rôle IAM qui dispose des autorisations requises pour charger des données à partir de Amazon S3.
13. Sélectionnez Créer une table pour créer la table à l'aide de la définition indiquée.

    Un résumé de la définition de la table s'affiche. La table est créée dans la base de données. Pour supprimer ultérieurement la table, exécutez la commande SQL DROP TABLE. Pour plus d'informations, consultez la section DROP TABLE dans le Guide du développeur de la base de données Amazon Redshift.
14. Choisissez Load data (Charger les données) pour démarrer le chargement des données.

    Lorsque le chargement est terminé, l'éditeur de requête s'affiche avec la commande COPY générée qui a été utilisée pour charger vos données. Le résultat de la commande COPY s'affiche. En cas de succès, vous pouvez désormais utiliser SQL pour sélectionner des données à partir de la table chargée. En cas d'erreur, interrogez la vue système STL_LOAD_ERRORS pour obtenir plus de détails. Pour plus d'informations sur les erreurs de commande COPY,

consultez STL_LOAD_ERRORS dans le Guide du développeur de la base de données Amazon Redshift.

Chargement de données à partir d'un fichier local : configuration et flux de travail

Vous pouvez charger des données d'un fichier local dans une table existante ou nouvelle.

Configuration administrateur pour charger des données à partir d'un fichier local

Votre administrateur de l'éditeur de requête v2 doit spécifier le compartiment Amazon S3 commun dans la fenêtre Account settings (Paramètres du compte). Les utilisateurs du compte doivent être configurés avec les autorisations appropriées.

- Autorisations IAM nécessaires – Les utilisateurs du chargement à partir du fichier local doivent disposer des autorisations `s3:ListBucket`, `s3:GetBucketLocation`, `s3:putObject`, `s3:getObject` et `s3:deleteObject`. Il *`optional-prefix`* peut être spécifié pour limiter l'utilisation de ce compartiment liée à l'éditeur de requêtes v2 aux objets portant ce préfixe. Vous pouvez utiliser cette option lorsque ce même compartiment Amazon S3 est utilisé dans d'autres contextes que l'éditeur de requête v2. Pour en savoir plus sur les compartiments et les préfixes, consultez Managing user access to specific folders (Gestion de l'accès des utilisateurs à des dossiers spécifiques) dans Amazon Simple Storage Service User Guide (Guide de l'utilisateur d'Amazon Simple Storage Service). Pour s'assurer que l'accès aux données entre utilisateurs n'est pas autorisé, nous recommandons à l'administrateur de l'éditeur de requête v2 d'utiliser une politique de compartiment Amazon S3 pour restreindre l'accès aux objets en fonction de `aws:userid`. L'exemple suivant autorise Amazon S3 à read/write accéder uniquement *`<staging-bucket-name>`* aux objets Amazon S3 dont le préfixe est `aws:userid` le.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::<staging-bucket-name>"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::<staging-bucket-name>[/<optional-prefix>]/
${aws:userid}/*"
            ]
        }
    ]
}
```

- Séparation des données – Nous déconseillons d'accorder aux utilisateurs un accès mutuel à leurs données respectives (même brièvement). Le chargement à partir d'un fichier local utilise le compartiment Amazon S3 intermédiaire configuré par l'administrateur de l'éditeur de requête v2. Configurez la politique de compartiment pour le compartiment intermédiaire afin d'assurer une séparation des données entre les utilisateurs. L'exemple suivant montre une politique de compartiment qui sépare les données entre les utilisateurs du*<staging-bucket-name>*.

  JSON

```
{
 "Version":"2012-10-17",
    "Statement": [
        {"Sid": "userIdPolicy",
            "Effect": "Deny",
            "Principal": "*",
            "Action": ["s3:PutObject",
                       "s3:GetObject",
                       "s3:DeleteObject"],
            "NotResource": [
                "arn:aws:s3:::<staging-bucket-name>[/<optional-prefix>]/
${aws:userid}/*"
            ]
         }
    ]
}
```

Chargement de données à partir d'un fichier local

Pour charger les données d'un fichier local dans une table existante

Votre administrateur de l'éditeur de requête v2 doit spécifier le compartiment Amazon S3 commun dans la fenêtre Paramètres du compte. L'éditeur de requête v2 charge automatiquement le fichier local dans un compartiment Amazon S3 commun utilisé par votre compte, puis utilise la commande COPY pour charger les données. La commande COPY générée et exécutée par la fenêtre de chargement de fichier local de l'éditeur de requête v2 prend en charge la plupart des paramètres disponibles dans la syntaxe de la commande COPY pour la copie depuis Amazon S3. Pour en savoir plus sur la commande COPY et ses options permettant de charger des données à partir d'Amazon S3, consultez Commande COPY depuis Amazon S3 dans le Guide du développeur de base de données Amazon Redshift.

1. Vérifiez que la table est déjà créée dans la base de données où vous souhaitez charger des données.
2. Vérifiez que vous êtes connecté à la base de données cible dans le volet d'arborescence de l'éditeur de requête v2. Vous pouvez créer une connexion avec le cluster ou le groupe de travail où les données seront chargées, en utilisant le menu contextuel (clic droit).
3. Choisissez  Load data (Charger les données).
4. Dans Data source (Source de données), choisissez Load from local file (Charger depuis un fichier local).
5. Choisissez Parcourir pour rechercher le fichier qui contient les données en question et sélectionnez Charger un fichier. Par défaut, les fichiers portant les extensions `.csv`, `.avro`, `.parquet` et `.orc` sont affichés, mais vous pouvez choisir d'autres types de fichiers. La taille maximale du fichier est de 100 Mo.
6. Choisissez le format de fichier pour le fichier à charger. Les formats de données pris en charge sont CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET et ORC. En fonction du format de fichier spécifié, vous pouvez choisir les options de fichier correspondantes. Vous pouvez également sélectionner Data is encrypted (Les données sont chiffrées) si les données sont chiffrées et saisir l'Amazon Resource Name (ARN) de la clé KMS utilisée pour chiffrer les données.

Si vous choisissez CSV ou DELIMITER, vous pouvez également choisir le caractère de délimitation et l'option Ignorer les lignes d'en-tête si le nombre de lignes spécifié correspond à des noms de colonnes et non à des données à charger.

7. (Facultatif) Les paramètres avancés prennent en charge divers paramètres de conversion de données et opérations de chargement. Saisissez ces informations si nécessaire pour votre fichier.

   Pour plus d'informations sur la conversion des données et les paramètres de chargement des données, consultez Paramètres de conversion de données et Opérations de chargement de données dans le Guide du développeur de base de données Amazon Redshift.

8. Choisissez Suivant.
9. Choisissez Charger la table existante.
10. Confirmez ou choisissez l'emplacement de la Table cible, notamment le Cluster ou groupe de travail, la Base de données, le Schéma et le nom de la Table où sont chargées les données.
11. (Facultatif) Vous pouvez choisir les noms de colonnes à saisir dans Column mapping (Mappage de colonnes) pour mapper les colonnes dans l'ordre du fichier de données d'entrée.
12. Choisissez Load data (Charger les données) pour démarrer le chargement des données.

    À l'issue du chargement, un message s'affiche indiquant si le chargement a abouti ou non. En cas de succès, vous pouvez désormais utiliser SQL pour sélectionner des données à partir de la table chargée. En cas d'erreur, interrogez la vue système STL_LOAD_ERRORS pour obtenir plus de détails. Pour plus d'informations sur les erreurs de commande COPY, consultez STL_LOAD_ERRORS dans le Guide du développeur de la base de données Amazon Redshift.

    Le modèle de commande COPY qui a servi à charger les données apparaît dans votre Query history (Historique des requêtes). Si ce modèle de commande COPY présente certains des paramètres utilisés, il ne peut pas être exécuté directement dans un onglet de l'éditeur. Pour en savoir plus sur l'historique des requêtes, consultez Afficher l'historique des requêtes et des onglets.

Lorsque vous chargez des données dans une nouvelle table, l'éditeur de requête v2 crée d'abord la table dans la base de données, puis charge les données en tant qu'actions distinctes dans le même flux de travail.

Pour charger les données d'un fichier local dans une nouvelle table

Votre administrateur de l’éditeur de requête v2 doit spécifier le compartiment Amazon S3 commun dans la fenêtre Account settings (Paramètres du compte). Le fichier local est automatiquement chargé dans un compartiment Amazon S3 commun utilisé par votre compte. La commande COPY est ensuite utilisée par l'éditeur de requête v2 pour charger les données. La commande COPY générée et exécutée par la fenêtre de chargement de fichier local de l'éditeur de requête v2 prend en charge la plupart des paramètres disponibles dans la syntaxe de la commande COPY pour la copie depuis Amazon S3. Pour en savoir plus sur la commande COPY et ses options permettant de charger des données à partir d’Amazon S3, consultez Commande COPY depuis Amazon S3 dans le Guide du développeur de base de données Amazon Redshift.

1. Vérifiez que vous êtes connecté à la base de données cible dans le volet d’arborescence de l’éditeur de requête v2. Vous pouvez créer une connexion avec le cluster ou le groupe de travail où les données seront chargées, en utilisant le menu contextuel (clic droit).
2. Choisissez  Load data (Charger les données).
3. Dans Data source (Source de données), choisissez Load from local file (Charger depuis un fichier local).
4. Choisissez Parcourir pour rechercher le fichier qui contient les données en question et sélectionnez Charger un fichier. Par défaut, les fichiers portant les extensions `.csv`, `.avro`, `.parquet` et `.orc` sont affichés, mais vous pouvez choisir d’autres types de fichiers. La taille maximale du fichier est de 100 Mo.
5. Choisissez le format de fichier pour le fichier à charger. Les formats de données pris en charge sont CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET et ORC. En fonction du format de fichier spécifié, vous pouvez choisir les options de fichier correspondantes. Vous pouvez également sélectionner Data is encrypted (Les données sont chiffrées) si les données sont chiffrées et saisir l’Amazon Resource Name (ARN) de la clé KMS utilisée pour chiffrer les données.

   Si vous choisissez CSV ou DELIMITER, vous pouvez également choisir le caractère de délimitation et l'option Ignorer les lignes d'en-tête si le nombre de lignes spécifié correspond à des noms de colonnes et non à des données à charger.

6. (Facultatif) Les paramètres avancés prennent en charge divers paramètres de conversion de données et opérations de chargement. Saisissez ces informations si nécessaire pour votre fichier.

   Pour plus d'informations sur la conversion des données et les paramètres de chargement des données, consultez Paramètres de conversion de données et Opérations de chargement de données dans le Guide du développeur de base de données Amazon Redshift.
7. Choisissez Suivant.
8. Choisissez Charger une nouvelle table.
9. Confirmez ou choisissez l'emplacement de la Table cible, y compris le Cluster ou groupe de travail, la Base de données et le Schéma dans lequel les données sont chargées. Saisissez le nom de la table à créer.
10. Sélectionnez Créer une table pour créer la table à l'aide de la définition indiquée.

    Un résumé de la définition de la table s'affiche. La table est créée dans la base de données. Pour supprimer ultérieurement la table, exécutez la commande SQL DROP TABLE. Pour plus d'informations, consultez la section DROP TABLE dans le Guide du développeur de la base de données Amazon Redshift.
11. Choisissez Load data (Charger les données) pour démarrer le chargement des données.

    Lorsque le chargement est terminé, un message s'affiche pour indiquer si le chargement a réussi ou non. En cas de succès, vous pouvez désormais utiliser SQL pour sélectionner des données à partir de la table chargée. En cas d'erreur, interrogez la vue système STL_LOAD_ERRORS pour obtenir plus de détails. Pour plus d'informations sur les erreurs de commande COPY, consultez STL_LOAD_ERRORS dans le Guide du développeur de la base de données Amazon Redshift.

    Le modèle de commande COPY qui a servi à charger les données apparaît dans votre Query history (Historique des requêtes). Si ce modèle de commande COPY présente certains des paramètres utilisés, il ne peut pas être exécuté directement dans un onglet de l'éditeur. Pour en savoir plus sur l'historique des requêtes, consultez Afficher l'historique des requêtes et des onglets.

Création de requêtes avec Amazon Redshift

Vous pouvez saisir une requête dans l'éditeur ou sélectionner une requête enregistrée dans la liste Queries (Requêtes) et choisir Run (Exécuter).

Par défaut, Limit 100 (Limite de 100) est défini pour limiter les résultats à 100 lignes. Vous pouvez désactiver cette option pour renvoyer un ensemble de résultats plus important. Si vous désactivez cette option, vous pouvez inclure l'option LIMIT dans votre instruction SQL, si vous souhaitez éviter des ensembles de résultats très volumineux. Pour plus d'informations, consultez ORDER BY clause (Clause ORDER BY) dans le Guide du développeur de bases de données Amazon Redshift.

Pour afficher un plan de requête dans la zone de résultats, activez Explain (Expliquer). Activez Explain graph (Graphique d'explication) pour que les résultats affichent également une représentation graphique du plan d'explication.

Pour enregistrer une requête dans le dossier Queries (Requêtes), choisissez Save (Enregistrer).

Dans le cas d'une requête réussie, un message de réussite s'affiche. Si la requête renvoie des informations, les résultats s'affichent dans la section Results (Résultats). Si le nombre de résultats dépasse la zone d'affichage, les chiffres apparaissent en haut de cette dernière. Vous pouvez choisir les chiffres pour afficher les pages de résultats successives.

Vous pouvez filtrer et trier Result (Résultat) pour chaque colonne. Pour entrer des critères de filtre dans l'en-tête de la colonne de résultats, survolez la colonne pour afficher un menu (☰) où vous pouvez saisir des critères pour filtrer la colonne.

Si la requête contient une erreur, l'éditeur de requête v2 affiche un message d'erreur dans la zone de résultats. Le message fournit des informations sur la façon de corriger la requête.

Vous pouvez exporter ou copier les résultats de votre requête en utilisant le menu contextuel (clic droit) dans la zone des résultats comme suit :

- Choisissez Copier vers et choisissez JSON ou CSV pour télécharger les lignes sélectionnées dans un fichier.
- Choisissez Copier les lignes pour copier les lignes sélectionnées dans le presse-papiers.
- Choisissez Copier les lignes avec les en-têtes pour copier les lignes sélectionnées avec les en-têtes de colonne dans le presse-papiers.

Vous pouvez aussi choisir Exporter dans la zone des résultats, puis choisir soit JSON soit CSV pour télécharger l'ensemble des résultats de lignes dans un fichier. Le nombre de lignes dans l'ensemble de résultats peut être limité par l'option Limit (Limiter) ou la clause SQL `limit` de la requête. La taille maximale de l'ensemble de résultats téléchargés est de 5 Mo.

Vous pouvez également utiliser le raccourci Ctrl+C sur Windows ou Cmd+C sur macOS pour copier les données de la page de résultats actuelle dans le presse-papiers. Si aucune ligne n'est sélectionnée, la cellule sur laquelle vous vous concentrez est copiée dans le presse-papiers. Si des lignes sont sélectionnées, alors les lignes sélectionnées sont copiées dans le presse-papiers.

Pour ajouter un nouvel onglet de requête, choisissez l'icône



,

puis Editor (Éditeur), qui apparaît sur la ligne avec les onglets de requête. L'onglet de requête utilise une `Isolated session` ou pas. Avec une session isolée, les résultats d'une commande SQL, telle que la création d'une table temporaire dans un onglet de l'éditeur, ne sont pas visibles dans un autre onglet de l'éditeur. Lorsque vous ouvrez un onglet d'éditeur dans l'éditeur de requête v2, l'option par défaut est une session isolée.

Pour exécuter une requête

1. Dans la zone de requête, effectuez l'une des actions suivantes :

   - Saisissez une requête.
   - Collez une requête que vous avez copiée.
   - Cliquez sur l'onglet Queries (Requêtes), ouvrez le menu contextuel (clic droit) d'une requête enregistrée et choisissez Open query (Ouvrir la requête).

2. Confirmez que vous avez choisi les valeurs Cluster ou Workgroup (Groupe de travail) et Database (Base de données) correctes du SQL que vous prévoyez d'exécuter.

   Pour commencer, vous pouvez choisir Cluster ou Workgroup (Groupe de travail) dans l'arborescence. Choisissez également votre Database (Base de données) dans l'arborescence.

   Vous pouvez modifier les paramètres Cluster ou Groupe de travail, et Base de données dans chaque onglet de l'éditeur avec la liste de contrôles déroulante située à côté de l'en-tête Session isolée de chaque onglet de l'éditeur.

   Pour chaque onglet de l'éditeur, vous choisissez d'exécuter ou non le code SQL dans une Isolated session (Session isolée). Une session isolée possède sa propre connexion à une base de données. Utilisez-la pour exécuter du code SQL isolé des autres sessions de l'éditeur de requête. Pour plus d'informations sur les connexions, consultez Ouverture de l'éditeur de requête v2.

3. Cliquez sur Exécuter.

La zone Result (Résultat) s'ouvre et affiche les résultats de la requête.

Pour afficher le plan d'explication d'une requête

1. Sélectionnez la requête.
2. Activez Explain (Expliquer).

   Par défaut, l'option Explain graph (Graphique d'explication) est également activée.
3. Cliquez sur Exécuter.

   La requête s'exécute et le plan d'explication s'affiche dans la zone Result (Résultat) de la requête.

L'éditeur de requête v2 prend en charge les fonctionnalités suivantes :

- Vous pouvez créer des requêtes avec plusieurs instructions SQL dans un onglet de requête. Les requêtes sont exécutées en série et plusieurs onglets de résultats s'ouvrent pour chaque requête.
- Vous pouvez créer des requêtes avec des variables de séance et des tables temporaires.
- Vous pouvez créer des requêtes avec des paramètres remplaçables désignés par `${parameter}`. Vous pouvez créer votre requête SQL avec plusieurs paramètres remplaçables et utiliser le même paramètre à plusieurs endroits de votre instruction SQL.

  Lorsque la requête s'exécute, une fenêtre s'affiche pour saisir la valeur du paramètre. Chaque fois que vous exécutez la requête, la fenêtre s'affiche pour entrer les valeurs de vos paramètres.

  Pour obtenir un exemple, consultez Exemple : ventes supérieures à un paramètre spécifique.
- Les requêtes sont versionnées automatiquement. Vous pouvez choisir une version antérieure d'une requête à exécuter.
- Vous n'avez pas besoin d'attendre la fin d'une requête avant de poursuivre votre flux de travail. Vos requêtes continuent de s'exécuter, même si vous fermez l'éditeur de requête.
- Lors de la création de requêtes, l'achèvement automatique des noms de schéma, de table et de colonne est pris en charge à l'aide d'un raccourci.

L'éditeur SQL prend en charge les fonctionnalités suivantes :

- Les crochets de début et de fin utilisés dans SQL ont des couleurs identiques. Des lignes verticales sont affichées dans l'éditeur pour vous aider à faire correspondre les crochets.
- Vous pouvez réduire et développer des sections de votre code SQL.
- Vous pouvez rechercher et remplacer du texte dans votre SQL.
- Vous pouvez utiliser les touches de raccourci pour plusieurs tâches d'édition courantes.
- Les erreurs SQL sont mises en surbrillance dans l'éditeur pour faciliter la localisation des zones problématiques.

Pour une démonstration des fonctionnalités d'édition, regardez la vidéo suivante : Une expérience d'édition nouvelle et améliorée dans Amazon Redshift Query Editor V2.

Exemples de requêtes

Vous trouverez ci-après les descriptions des différents types de requêtes que vous pouvez exécuter.

Les données utilisées dans bon nombre de ces requêtes proviennent de l'exemple de schéma `tickit`. Pour plus d'informations sur le chargement des exemples de données `tickit`, consultez Chargement de données dans une base de données. Pour plus d'informations sur les exemples de données `tickit`, consultez Exemple de base de données dans le Guide du développeur de base de données Amazon Redshift.

Lorsque vous exécutez ces exemples de requêtes, confirmez que vous choisissez la base de données appropriée dans l'éditeur, telle que `sample_data_dev`.

Rubriques

- Exemple : définition de variables de séance
- Exemple : événement le plus important par ventes totales
- Exemple : ventes supérieures à un paramètre spécifique
- Exemple : créer une table temporaire
- Exemple : sélection à partir d'une table temporaire

Exemple : définition de variables de séance

La commande suivante définit le paramètre de configuration du serveur `search_path` sur public pour la séance. Pour plus d'informations, consultez SET et search_path dans le Guide du développeur de bases de données Amazon Redshift.

```
set search_path to public;
```

Exemple : événement le plus important par ventes totales

La requête suivante recherche l'événement ayant le plus de ventes.

```
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
group by eventname
order by 3;
```

Voici une liste partielle des résultats.

```
eventname           totalorders       totalsales
White Christmas         20              9352
Joshua Radin            38             23469
Beach Boys              58             30383
Linda Ronstadt          56             35043
Rascal Flatts           76             38214
Billy Idol              67             40101
Stephenie Meyer         72             41509
Indigo Girls            57             45399
...
```

Exemple : ventes supérieures à un paramètre spécifique

La requête suivante recherche les ventes dont la quantité vendue est supérieure au paramètre spécifié par `${numberoforders}`. Lorsque la valeur du paramètre est 7, le résultat est de 60 lignes. Lorsque vous exécutez la requête, l'éditeur de requête v2 affiche une fenêtre Run query form (Exécuter un formulaire de requête) pour rassembler la valeur des paramètres dans l'instruction SQL.

```
select salesid, qtysold
from sales
where qtysold > ${numberoforders}
order by 2;
```

Voici une liste partielle des résultats.

```
salesid qtysold
```

```
20005 8
21279 8
130232 8
42737 8
74681 8
67103 8
105533 8
91620 8
121552 8
...
```

Exemple : créer une table temporaire

L'instruction suivante crée la table temporaire eventsalestemp en sélectionnant des informations dans les tables sales (ventes) et event (événement).

```
create temporary table eventsalestemp as
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
group by eventname;
```

Exemple : sélection à partir d'une table temporaire

L'instruction suivante sélectionne les événements, le total des commandes et le total des ventes à partir de la table temporaire eventsalestemp, ordonnés par nombre total de commandes.

```
select eventname,  totalorders,  totalsales
from eventsalestemp
order by 2;
```

Voici une liste partielle de résultats :

```
eventname          totalorders   totalsales
White Christmas         20          9352
Joshua Radin            38         23469
Martina McBride         50         52932
Linda Ronstadt          56         35043
Indigo Girls            57         45399
Beach Boys              58         30383
...
```

Blocs-notes dans Amazon Redshift

Vous pouvez utiliser des blocs-notes pour organiser, annoter et partager plusieurs requêtes SQL dans un même document. Vous pouvez ajouter plusieurs cellules Markdown et de requête SQL à un bloc-notes. Les blocs-notes permettent de regrouper des requêtes et des explications associées à une analyse de données dans un seul document à l'aide de plusieurs cellules de requête et Markdown. Vous pouvez ajouter du texte et mettre en forme l'apparence à l'aide de la syntaxe Markdown pour fournir du contexte et des informations supplémentaires pour vos tâches d'analyse de données. Vous pouvez partager vos blocs-notes avec les membres de l'équipe.

Pour utiliser des blocs-notes, vous devez ajouter une autorisation pour les blocs-notes à votre principal IAM (utilisateur IAM ou rôle IAM). Il est recommandé d'associer des politiques d'autorisation à un rôle IAM, puis de l'attribuer à des utilisateurs et à des groupes, le cas échéant. Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift. Vous pouvez ajouter l'autorisation à l'une des politiques gérées par l'éditeur de requêtes v2. Pour plus d'informations, consultez Accès à l'éditeur de requête v2.

Vous pouvez exécuter toutes les cellules d'un bloc-notes de manière séquentielle. La cellule de requête SQL d'un bloc-notes possède la plupart des mêmes fonctionnalités qu'un onglet d'éditeur de requêtes. Pour plus d'informations, consultez Création de requêtes avec Amazon Redshift. Voici les différences entre un onglet d'éditeur de requêtes et une cellule SQL dans un bloc-notes.

- Il n'existe aucun contrôle pour exécuter `Explain` sur une instruction SQL dans un bloc-notes.
- Vous ne pouvez créer qu'un seul graphique par cellule SQL dans un bloc-notes.

Vous pouvez exporter et importer des bloc-notes dans des fichiers créés avec l'éditeur de requête v2. L'extension de fichier est `.ipynb` et la taille du fichier peut atteindre 5 Mo au maximum. Les cellules SQL et Markdown sont stockées dans le fichier. Aucun cluster ou groupe de travail ni base de données ne sont stockés dans le bloc-notes exporté. Lorsque vous ouvrez un bloc-notes importé, vous choisissez le cluster ou le groupe de travail et la base de données dans laquelle l'exécuter. Après avoir exécuté des cellules SQL, vous pouvez choisir d'afficher ou non la page actuelle des résultats sous forme de graphique dans l'onglet des résultats. Le jeu de résultats d'une requête n'est pas stocké dans le bloc-notes.

Création d'un bloc-notes

Vous pouvez créer un bloc-notes pour organiser, annoter et partager plusieurs requêtes SQL dans un même document.

Pour créer un bloc-notes

1. Dans le menu du navigateur, choisissez l’icône Éditeur ().
2. Cliquez sur l’icône plus (), puis sur Bloc-notes.

   Par défaut, une cellule de requête SQL apparaît dans le bloc-notes.
3. Dans la cellule de requête SQL, effectuez l’une des actions suivantes :

   - Saisissez une requête.
   - Collez une requête que vous avez copiée.
4. (Facultatif) Choisissez l’icône plus (), puis Markdown pour ajouter une cellule Markdown dans laquelle vous pouvez fournir du texte descriptif ou explicatif à l’aide de la syntaxe Markdown standard.
5. (Facultatif) Choisissez l’icône plus (), puis SQL pour insérer une cellule SQL.

Vous pouvez renommer des blocs-notes à l’aide de l’icône crayon ().

Dans l’icône menu (), vous pouvez également effectuer les opérations suivantes sur un bloc-notes :

- 

  Share with my team (Partager avec mon équipe) : pour partager le bloc-notes avec votre équipe, tel que défini par des balises. Pour partager un bloc-notes avec votre équipe, assurez-vous que la balise principale `sqlworkbench-team` est définie sur la même valeur que les autres membres de votre équipe dans votre compte. Par exemple, un administrateur peut définir la valeur sur

`accounting-team` pour tous les membres du service comptable. Pour obtenir un exemple, consultez Autorisations requises pour utiliser l'éditeur de requête v2.

- 

  Export (Exporter) : pour exporter le bloc-notes vers un fichier local portant l'extension `.ipynb`.

- 

  Importer une requête : pour importer une requête depuis un fichier local dans une cellule du bloc-notes. Vous pouvez importer des fichiers avec des extensions `.sql` et `.txt`.

- 

  Save version (Enregistrer la version) : pour créer une version du bloc-notes. Pour voir les versions d'un bloc-notes, accédez à vos blocs-notes enregistrés et ouvrez Version history (Historique des versions).

- 

  Duplicate (Dupliquer) : pour créer une copie du bloc-notes et l'ouvrir dans un nouvel onglet de bloc-notes.

- 

  Shortcuts (Raccourcis) : pour afficher les raccourcis disponibles lors de la création d'un bloc-notes.

Importation dans des blocs-notes

Vous pouvez importer un bloc-notes complet ou des cellules SQL individuelles dans un bloc-notes de l'éditeur de requêtes v2.

Pour importer un bloc-notes complet à partir d'un fichier local dans Mes blocs-notes, choisissez 
Importer, puis Importer un bloc-notes. Accédez au fichier `.ipynb` contenant votre bloc-notes. Le bloc-notes est importé dans le dossier du bloc-notes actuellement ouvert. Vous pouvez ensuite ouvrir le bloc-notes dans l'éditeur de bloc-notes.

Pour importer une requête d'un fichier local dans une cellule SQL d'un bloc-notes, choisissez 
Importer, puis Importer une requête. Dans la fenêtre Importer une requête, suivez les instructions affichées à l'écran pour choisir les fichiers et les dossiers qui peuvent être importés sous forme de requête dans un nouveau bloc-notes ou un bloc-notes existant. Les fichiers doivent porter l'extension `.sql` ou`.txt`. Chaque requête peut aller jusqu'à 10 000 caractères. Lorsque vous ajoutez un bloc-

notes à un bloc-notes existant, vous choisissez quel bloc-notes parmi tous les blocs-notes de votre liste de blocs-notes enregistrés. Les requêtes importées sont ajoutées sous forme de cellules SQL à la fin du bloc-notes. Lorsque vous choisissez un nouveau bloc-notes, vous choisissez le nom du bloc-notes et celui-ci est créé dans le dossier des blocs-notes enregistrés actuellement ouvert.

> **Note**
>
> Lorsque vous créez `.sql` des fichiers sur macOS à l'aide de l' TextEditapplication, il se peut qu'une extension masquée supplémentaire soit ajoutée au fichier. Par exemple, un fichier nommé `Test.sql` créé dans TextEdit peut finir par être enregistré sous`Test.sql.rtf`. L'éditeur de requêtes v2 ne prend pas en charge les fichiers portant l'extension `.rtf`. Toutefois, si vous créez un `.sql` fichier à l'aide TextEdit d'un fichier texte brut et que vous l'enregistrez sous forme de fichier texte brut, le fichier possède une `.txt` extension masquée supplémentaire. Par exemple, un fichier nommé `Text.sql` peut être enregistré sous `Text.sql.txt`. Contrairement à l'extension `.rtf`, l'éditeur de requêtes v2 prend en charge les fichiers portant l'extension `.txt`. `Text.sql.txt` est donc pris en charge lors de l'importation de requêtes dans des blocs-notes.

Pour une démonstration des bloc-notes, regardez la vidéo suivante : Amazon Redshift SQL Notebooks in query editor v2 (Bloc-notes Amazon Redshift SQL dans l'éditeur de requête v2).

Interrogation du AWS Glue Data Catalog

Vous pouvez utiliser l'éditeur de requêtes v2 pour interroger les données cataloguées dans votre répertoire en AWS Glue Data Catalog utilisant des commandes SQL spécifiques et en accordant les autorisations décrites dans cette section. Par défaut, le AWS Glue Data Catalog est répertorié en tant que base de données de l'éditeur de requête v2 nommée`awsdatacatalog`. La fonctionnalité d'interrogation du AWS Glue Data Catalog n'est pas disponible dans toutes les Régions AWS Amazon Redshift. Pour savoir si elle est disponible, utilisez la commande SHOW. Pour plus d'informations AWS Glue, voir Qu'est-ce que c'est AWS Glue ? dans le Guide AWS Glue du développeur.

> **Note**
>
> L'interrogation n' AWS Glue Data Catalog est prise en charge que dans les clusters de type nœud Amazon Redshift RG ou RA3 et dans Amazon Redshift Serverless.

Vous pouvez configurer votre entrepôt de données et afficher les objets de AWS Glue base de données catalogués à l'aide des commandes SQL suivantes :

- SHOW – pour déterminer si le `awsdatacatalog` est monté pour l'entrepôt de données actuellement connecté. Par exemple, pour afficher la valeur du paramètre `data_catalog_auto_mount`, exécutez :

  ```
  SHOW data_catalog_auto_mount;
  ```

  Pour en savoir plus, consultez SHOW dans le Guide du développeur de base de données Amazon Redshift.

- ALTER SYSTEM – pour modifier la configuration au niveau du système de `data_catalog_auto_mount`. Par exemple, pour faire passer la valeur du paramètre `data_catalog_auto_mount` à on, exécutez :

  ```
  ALTER SYSTEM SET data_catalog_auto_mount = on;
  ```

  La modification prend effet lorsqu'un cluster provisionné est redémarré ou que l'activité d'un groupe de travail sans serveur est automatiquement suspendue puis reprise. Pour en savoir plus, consultez ALTER SYSTEM dans le Guide du développeur de base de données Amazon Redshift.

- SHOW SCHEMAS – affiche une liste de schémas. Les schémas de la base de données nommée `awsdatacatalog` représentent les AWS Glue bases de données cataloguées dans le. AWS Glue Data Catalog Par exemple, pour afficher ces schémas, exécutez :

  ```
  SHOW SCHEMAS FROM DATABASE awsdatacatalog;
  ```

  Pour en savoir plus, consultez SHOW SCHEMAS dans le Guide du développeur de base de données Amazon Redshift.

- SHOW TABLES – affiche la liste des tables d'un schéma. Par exemple, pour afficher les tables de la AWS Glue Data Catalog base de données nommée `awsdatacatalog` qui sont dans le schéma, `myglue` exécutez :

  ```
  SHOW TABLES FROM SCHEMA awsdatacatalog.myschema;
  ```

  Pour en savoir plus, consultez SHOW TABLES dans le Guide du développeur de base de données Amazon Redshift.

- SHOW COLUMNS – affiche la liste des colonnes d'une table. Par exemple, pour afficher les colonnes de la AWS Glue Data Catalog base de données nommée `awsdatacatalog` qui figurent dans le schéma `myglue` et la table, `mytable` exécutez :

  ```
  SHOW COLUMNS FROM TABLE awsdatacatalog.myglue.mytable;
  ```

  Pour en savoir plus, consultez SHOW COLUMNS dans le Guide du développeur de base de données Amazon Redshift.

Pour accorder à votre utilisateur ou rôle IAM l'autorisation d'interroger le AWS Glue Data Catalog,

1. Dans le volet d'arborescence, connectez-vous à votre base de données initiale dans votre cluster provisionné ou votre groupe de travail sans serveur en utilisant la méthode d'authentification Nom d'utilisateur et mot de passe de la base de données. Par exemple, connectez-vous à la base de données `dev` en utilisant le nom d'utilisateur et le mot de passe d'administrateur que vous avez utilisés au moment de créer le cluster ou le groupe de travail.
2. Dans un onglet de l'éditeur, exécutez l'instruction SQL suivante pour accorder à un utilisateur IAM l'accès au AWS Glue Data Catalog.

   ```
   GRANT USAGE ON DATABASE awsdatacatalog to "IAM:myIAMUser"
   ```

   Où se *`IAM:myIAMUser`* trouve un utilisateur IAM auquel vous souhaitez accorder des privilèges d'utilisation à. AWS Glue Data Catalog Vous pouvez également accorder un privilège d'utilisation *`IAMR:myIAMRole`* à un rôle IAM.
3. Dans le volet d'arborescence, modifiez ou supprimez la connexion au cluster ou groupe de travail que vous avez créé précédemment. Connectez-vous à votre cluster ou groupe de travail de l'une des manières suivantes :
   - Pour accéder à la base de données `awsdatacatalog` à partir d'un cluster, vous devez utiliser la méthode d'authentification Informations d'identification temporaires utilisant votre identité IAM. Pour en savoir plus sur cette méthode d’authentification, consultez Connexion à une base de données Amazon Redshift. Votre administrateur de l'éditeur de requête v2 devra peut-être configurer les Paramètres du compte pour que le compte affiche cette méthode d'authentification dans la fenêtre de connexion.
   - Pour accéder à la base de données `awsdatacatalog` à partir d'un groupe de travail, vous devez utiliser la méthode d'authentification Utilisateur fédéré. Pour en savoir plus sur cette méthode d’authentification, consultez Connexion à une base de données Amazon Redshift.

4. Avec le privilège accordé, vous pouvez utiliser votre identité IAM pour exécuter des requêtes SQL sur votre AWS Glue Data Catalog.

Après vous être connecté, vous pouvez utiliser l'éditeur de requête v2 pour interroger les données cataloguées dans AWS Glue Data Catalog. Dans le volet d'arborescence de l'éditeur de requête v2, choisissez le cluster ou le groupe de travail et la base de données `awsdatacatalog`. Dans le volet de l'éditeur ou du bloc-notes, vérifiez que le cluster ou le groupe de travail approprié est sélectionné. La base de données choisie doit être la base de données Amazon Redshift initiale, comme `dev`. Pour en savoir plus sur la création de requêtes, consultez Création de requêtes avec Amazon Redshift et Blocs-notes dans Amazon Redshift. La base de données nommée `awsdatacatalog` est réservée pour référencer la base de données du catalogue de données externe dans votre compte. Les requêtes exécutées sur la base de données `awsdatacatalog` peuvent être uniquement en lecture seule. Utilisez une notation en trois parties pour référencer la table dans votre instruction SELECT, Où la première partie est le nom de la base de données, la deuxième partie est le nom AWS Glue de la base de données et la troisième partie est le nom de la AWS Glue table.

```
SELECT * FROM awsdatacatalog.<aws-glue-db-name>.<aws-glue-table-name>;
```

Vous pouvez exécuter différents scénarios pour lire les AWS Glue Data Catalog données et remplir les tables Amazon Redshift.

L'exemple de code SQL suivant joint deux tables définies dans AWS Glue.

```
SELECT pn.emp_id, alias, role, project_name
FROM "awsdatacatalog"."empl_db"."project_name_table" pn,
"awsdatacatalog"."empl_db"."project_alias_table" pa
WHERE pn.emp_id = pa.emp_id;
```

L'exemple de code SQL suivant crée une table Amazon Redshift et la remplit avec les données d'une jointure de deux tables. AWS Glue

```
CREATE TABLE dev.public.glue AS
SELECT pn.emp_id, alias, role, project_name
FROM "awsdatacatalog"."empl_db"."project_name_table" pn,
"awsdatacatalog"."empl_db"."project_alias_table" pa
WHERE pn.emp_id = pa.emp_id;
```

Interrogation des tables Amazon S3 (version préliminaire)

Vous pouvez utiliser l'éditeur de requête v2 pour interroger les données contenues dans les catalogues Amazon S3 montés sur le AWS Glue Data Catalog. Les catalogues de tables Amazon S3 sont montés dès leur création et apparaissent automatiquement sous forme de bases de données externes sur tous les clusters provisionnés et les groupes de travail sans serveur au sein d'un même cluster Région AWS sous le même compte. AWS Glue Data Catalog Pour plus d'informations sur l'accès aux tables Amazon S3 avec Amazon Redshift, consultez Accès aux tables Amazon Redshift avec Amazon Redshift dans le Guide de l'utilisateur Amazon Simple Storage Service.

Interrogation d'un lac de données

Vous pouvez interroger des données dans un lac de données Amazon S3 en suivant l'ensemble des tâches décrites dans ce didacticiel. Tout d'abord, vous créez un schéma externe pour référencer la base de données externe dans le AWS Glue Data Catalog. Vous pouvez ensuite interroger des données dans le lac de données Amazon S3.

Démo : interroger un lac de données

Pour une démonstration de l'interrogation d'un lac de données, regardez la vidéo suivante. Interrogation de votre lac de données à partir de l'éditeur de requête v2 Amazon Redshift.

Conditions préalables

Avant d'utiliser votre lac de données dans l'éditeur de requête v2, confirmez que les éléments suivants ont été configurés dans votre environnement Amazon Redshift :

- Explorez vos données Amazon S3 en utilisant AWS Glue et activez votre catalogue de données pour AWS Lake Formation.
- Créez un rôle IAM pour Amazon Redshift à l'aide AWS Glue du catalogue de données activé pour. AWS Lake Formation Pour plus de détails sur cette procédure, consultez Pour créer un rôle IAM pour Amazon Redshift à l'aide AWS Glue Data Catalog d'un pour activé pour. AWS Lake Formation Pour plus d'informations sur l'utilisation de Redshift Spectrum et de Lake Formation, consultez la section Utilisation de Redshift Spectrum avec. AWS Lake Formation
- Vous accordez des autorisations SELECT sur la table à interroger dans la base de données Lake Formation. Pour plus de détails sur cette procédure, consultez Pour accorder les autorisations SELECT sur la table à interroger dans la base de données Lake Formation.

Vous pouvez vérifier dans la console Lake Formation (https://console.aws.amazon.com/lakeformation/), section Permissions, page des autorisations du Data Lake, que le rôle IAM, la AWS Glue base de données et les tables disposent des autorisations appropriées.

- Confirmez que votre utilisateur connecté dispose des autorisations nécessaires pour créer des schémas dans la base de données Amazon Redshift et accéder aux données de votre lac de données. Lorsque vous vous connectez à une base de données dans l'éditeur de requête v2, vous choisissez une méthode d'authentification qui inclut des informations d'identification, qui peuvent être un utilisateur de la base de données ou un utilisateur IAM. L'utilisateur connecté doit disposer des autorisations et des privilèges de base de données appropriés, tels qu'un `superuser`. L'utilisateur `admin` Amazon Redshift qui a créé le cluster ou le groupe de travail dispose de privilèges de `superuser` et peut créer des schémas et gérer la base de données Redshift. Pour plus d'informations sur la connexion à une base de données avec l'éditeur de requête v2, consultez Connexion à une base de données Amazon Redshift.

Création d'un schéma externe

Pour interroger les données d'un lac de données Amazon S3, commencez par créer un schéma externe. Le schéma externe référence la base de données externe dans le AWS Glue Data Catalog.

1. Dans la vue Éditeur de l'éditeur de requête v2, choisissez  Créer, puis Schéma.
2. Saisissez un nom de schéma.
3. Pour le Type de schéma, choisissez Externe.
4. Dans les détails du catalogue de données, la région correspond par défaut à l' Région AWS emplacement de votre base de données Redshift.
5. Choisissez la AWS Glue base de données à laquelle le schéma externe sera mappé et qui contient des références aux AWS Glue tables.
6. Choisissez un rôle IAM pour Amazon Redshift qui dispose des autorisations requises pour interroger des données sur Amazon S3.
7. Vous pouvez éventuellement choisir un rôle IAM autorisé à accéder au catalogue de données.
8. Choisissez Create schema (Créer un schéma).

   Le schéma apparaît sous votre base de données dans l'arborescence.

Lors de la création du schéma, si vous recevez une erreur d'autorisation refusée pour votre base de données, vérifiez si l'utilisateur connecté a le privilège de base de données pour créer un schéma.

Interrogation des données dans votre lac de données Amazon S3

Vous utilisez le schéma que vous avez créé dans la procédure précédente.

1. Dans le panneau de l'arborescence, sélectionnez le schéma.
2. Pour afficher une définition de tableau, choisissez un tableau. Les colonnes du tableau et les types de données s’affichent.
3. Pour interroger une table, sélectionnez la table et, dans le menu contextuel (clic droit), choisissez Sélectionner une table pour générer une requête.
4. Exécutez la requête dans l'éditeur.

   L'exemple de code SQL suivant a été généré par l'éditeur de requêtes v2 pour interroger toutes les lignes de la AWS Glue table nomméeflightscsv. Les colonnes et les lignes affichées dans le résultat sont tronquées par souci de simplicité.

```
SELECT * FROM "dev"."mydatalake_schema"."flightscsv";

year    quarter   month   dom  day_of_week   fl_date    unique_carrier  airline_id
  carrier   tail_num   fl_num
2016    4         10      19   3             10/19/16   OO              20304
  OO         N753SK    3086
2016    4         10      19   3             10/19/16   OO              20304
  OO         N753SK    3086
2016    4         10      19   3             10/19/16   OO              20304
  OO         N778SK    3087
2016 4         10      19   3             10/19/16   OO              20304
 OO         N778SK    3087
...
```

Unités de partage des données

Vous pouvez créer une unité de partage des données afin que les utilisateurs d’un autre cluster puissent interroger les données. Le cluster contenant les données que vous souhaitez partager s’appelle le cluster producteur. Vous créez une unité de partage des données sur le cluster producteur pour les objets de base de données que vous souhaitez partager. Vous pouvez partager des schémas, des tables, des vues et des fonctions définies par l’utilisateur (UDF) SQL. Le cluster

auquel vous souhaitez partager les données s'appelle le cluster consommateur. Sur le cluster consommateur, vous créez une base de données à partir de l'unité de partage des données. Les utilisateurs sur le cluster consommateur peuvent ensuite interroger les données. Pour plus d'informations, consultez Mise en route avec le partage de données dans le Guide du développeur de bases de données Amazon Redshift.

Création d'unités de partage des données

Vous créez une unité de partage des données sur le cluster que vous souhaitez utiliser en tant que cluster producteur. Pour plus d'informations sur les considérations relatives aux unités de partage des données, consultez Considérations relatives au partage des données dans Amazon Redshift dans le Guide du développeur de bases de données Amazon Redshift.

1. Choisissez la base de données sur le cluster producteur que vous souhaitez utiliser.
2. Créez l'unité de partage des données. Par exemple :

```
create datashare mysource;
```

3. Définissez des autorisations sur l'unité de partage des données. Par exemple :

```
grant alter, share on datashare mysource to admin;
```

4. Définissez des autorisations sur les objets de base de données que vous souhaitez partager. Par exemple :

```
alter datashare mysource add schema public;
```

```
alter datashare mysource add table public.event;
```

5. Définissez des autorisations sur l'espace de noms du cluster consommateur pour accéder à l'unité de partage des données. Par exemple :

```
grant usage on datashare mysource to namespace '2b12345-1234-5678-9012-
bb1234567890';
```

Affichage des unités de partage des données

Vous pouvez afficher les unités de partage des données que vous avez créées sur le cluster producteur.

1. Choisissez le cluster producteur.
2. Affichez les unités de partage des données. Par exemple :

```
show datashares;
```

```
share_name share_owner source_database  consumer_database share_type createdate
 is_publicaccessible share_acl producer_account producer_namespace
test_datashare 100  db_producer  NULL   OUTBOUND 2/15/2022  FALSE  admin
 123456789012  p1234567-8765-4321-p10987654321
```

Création de la base de données consommateur

Sur le cluster consommateur, vous créez une base de données à partir de l'unité de partage des données. Ces étapes décrivent comment partager des données entre deux clusters au sein d'un même compte. Pour plus d'informations sur le partage de données entre AWS comptes, consultez la section Partage de données entre AWS comptes dans le manuel Amazon Redshift Database Developer Guide.

Vous pouvez utiliser des commandes SQL ou le panneau d'arborescence de l'éditeur de requête v2 pour créer la base de données.

Pour utiliser SQL

1. Créez une base de données à partir de l'unité de partage des données pour votre compte et de l'espace de noms du cluster producteur. Par exemple :

```
create database share_db from datashare mysource of account '123456789012'
 namespace 'p1234567-8765-4321-p10987654321';
```

2. Définissez des autorisations pour que les utilisateurs puissent accéder à la base de données et au schéma. Par exemple :

```
grant usage on database share_db to usernames;
```

```
grant usage on schema public to usernames;
```

Pour utiliser le panneau d'arborescence de l'éditeur de requête v2

1. Choisissez

   Create (Créer), puis Database (Base de données).
2. Saisissez un nom de base de données.
3. (Facultatif) Sélectionnez Users and groups (Utilisateurs et groupes) et choisissez un utilisateur de la base de donnée.
4. Sélectionnez Créer à l'aide d'une unité de partage des données.
5. Sélectionnez l'unité de partage des données.
6. Choisissez Créer une base de données.

   La nouvelle base de données datashare (unité de partage des données)

   s'affiche dans le panneau d'arborescence de l'éditeur de requête v2.
7. Définissez des autorisations pour que les utilisateurs puissent accéder à la base de données et au schéma. Par exemple :

   ```
   grant usage on database share_db to usernames;
   ```

   ```
   grant usage on schema public to usernames;
   ```

Interrogation d'objets d'unité de partage des données

Sur le cluster consommateur, vous pouvez interroger des objets d'unité de partage des données en utilisant les noms d'objets complets exprimés avec la notation en trois parties : base de données, schéma et nom de l'objet.

1. Dans le panneau d'arborescence de l'éditeur de requête v2, choisissez le schéma.
2. Pour afficher une définition de tableau, choisissez un tableau.

Les colonnes du tableau et les types de données s'affichent.

3. Pour interroger un tableau, choisissez le tableau, puis utilisez le menu contextuel (clic droit) pour choisir Select table (Sélectionner un tableau).
4. Interrogez les tables à l'aide des commandes SELECT. Par exemple :

```
select top 10 * from test_db.public.event;
```

Interrogations planifiées avec l'éditeur de requête v2

Avec Amazon Redshift Query Editor V2, vous pouvez automatiser les requêtes SQL pour qu'elles s'exécutent selon un planning. Les requêtes planifiées sont des instructions SQL qui s'exécutent automatiquement à des moments ou à des intervalles spécifiés, ce qui vous permet de gérer efficacement les opérations de données et les tâches d'analyse récurrentes. Vous souhaiterez peut-être planifier des requêtes si vous souhaitez rationaliser le traitement par lots, générer des rapports réguliers ou gérer des pipelines de données au sein de leur environnement Amazon Redshift.

Les requêtes planifiées facilitent l'automatisation des flux de travail d'extraction, de transformation et de chargement (ETL), l'actualisation des tableaux de bord avec des informations actualisées et la mise en œuvre de diverses routines de gestion des données. Les pages suivantes décrivent en détail le processus de création, de configuration et de gestion des requêtes planifiées afin d'optimiser vos charges de travail Amazon Redshift.

Création d'une planification de requête avec l'éditeur de requête v2

Vous pouvez créer une planification en vue d'exécuter une instruction SQL avec l'éditeur de requête Amazon Redshift v2. La création d'une planification vise à exécuter l'instruction SQL aux périodes qui correspondent aux besoins de votre activité. Au moment de l'exécution de la requête planifiée, celle-ci est lancée par Amazon EventBridge et utilise l'API Amazon Redshift Data.

Pour créer une planification afin d'exécuter une instruction SQL

1. Dans la
   vue Éditeur 
   choisissez 
   créer une planification en vue d'exécuter une instruction SQL.

2. Lorsque vous définissez la planification, vous fournissez les informations suivantes.

   - Le rôle IAM qui prend les autorisations nécessaires pour exécuter la requête. Ce rôle IAM est également attaché à votre cluster ou groupe de travail.
   - Les valeurs d'authentification pour l'une AWS Secrets Manager ou l'autre des informations d'identification temporaires permettant d'autoriser l'accès à votre cluster ou groupe de travail. Ces méthodes d'authentification sont prises en charge par l'API de données. Pour plus d'informations, consultez Authentification d'une requête planifiée.
   - Le cluster ou le groupe de travail dans lequel réside votre base de données.
   - Le nom de la table de base de données qui contient les données à interroger.
   - Nom de la requête planifiée et sa description. L'éditeur de requête v2 ajoute le préfixe « QS2- » au nom de la requête planifiée que vous indiquez. L'éditeur de requête v1 ajoute le préfixe « QS- » aux noms de ses requêtes planifiées.
   - L'instruction SQL à exécuter selon la planification.
   - Les options de fréquence et de répétition de la planification ou une valeur au format cron qui définit la planification. Pour plus d'informations, consultez la section Cron Expressions dans le guide de l'utilisateur Amazon CloudWatch Events.
   - Si nécessaire, vous pouvez activer des notifications Amazon SNS standard pour surveiller la requête planifiée. Vous serez peut-être amené à confirmer l'adresse e-mail que vous avez fournie à la notification Amazon SNS. Vérifiez dans votre e-mail s'il existe un lien destiné à confirmer l'adresse e-mail pour la notification Amazon SNS. Pour en savoir plus, consultez Notifications par e-mail dans le Guide du développeur Amazon Simple Notification Service. Si votre requête est en cours d'exécution mais que vous ne voyez aucun message publié dans votre rubrique SNS, consultez Ma règle s'exécute, mais je ne vois aucun message publié dans ma rubrique Amazon SNS dans le guide de l'utilisateur EventBridge Amazon.

3. Choisissez Planifier une requête pour enregistrer et activer la planification et ajouter celle-ci à la liste des requêtes dans la vue Requêtes planifiées.

La vue Requêtes planifiées 
toutes les requêtes planifiées pour vos clusters et groupes de travail. Cette vue vous permet d'afficher les détails de la requête planifiée, d'activer ou de désactiver la planification, de modifier la planification et de supprimer la requête planifiée. Lorsque vous examinez les détails d'une requête, vous pouvez aussi consulter l'historique de ses exécutions dans le cadre de la planification.

> **Note**
>
> Une exécution de requête planifiée ne reste disponible dans la liste Historique de planification que 24 heures. Les requêtes qui s'exécutent selon une planification ne figurent pas dans la vue Historique des requêtes de l'éditeur de requête v2

Démonstration de la planification d'une requête

Pour une démonstration de la planification d'une requête, regardez la vidéo suivante.Vidéo de démonstration de la planification d'une requête.

Configuration des autorisations pour planifier une requête

Pour planifier des requêtes, l'utilisateur Gestion des identités et des accès AWS (IAM) qui définit le calendrier et le rôle IAM associé au calendrier doit être configuré avec les autorisations IAM pour utiliser Amazon et l'API Amazon EventBridge Redshift Data. Pour recevoir des e-mails des requêtes planifiées, la notification Amazon SNS que vous spécifiez éventuellement doit également être configurée.

Ce qui suit décrit les tâches liées à l'utilisation de politiques AWS gérées pour fournir des autorisations, mais en fonction de votre environnement, vous souhaiterez peut-être limiter les autorisations autorisées.

Pour l'utilisateur IAM connecté à l'éditeur de requêtes v2, modifiez l'utilisateur IAM à l'aide de la console IAM (). https://console.aws.amazon.com/iam/

- Outre les autorisations nécessaires pour exécuter les opérations Amazon Redshift et Query Editor v2, associez `AmazonEventBridgeFullAccess` les politiques `AmazonRedshiftDataFullAccess` AWS gérées à un utilisateur IAM.
- Vous pouvez également attribuer les autorisations à un rôle et attribuer le rôle à l'utilisateur.

  Attachez une politique qui accorde l'autorisation `sts:AssumeRole` à l'ARN de ressource du rôle IAM que vous spécifiez lors de la définition de la requête planifiée. Pour en savoir plus sur l'endossement de rôles, consultez Octroi d'autorisations à un utilisateur pour endosser un rôle dans le Guide de l'utilisateur IAM.

  L'exemple suivant illustre une politique d'autorisation qui endosse le rôle IAM `myRedshiftRole` dans le compte `123456789012`. Le rôle IAM `myRedshiftRole` est également le rôle IAM qui est attaché au cluster ou au groupe de travail où s'exécute la requête planifiée.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AssumeIAMRole",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::123456789012:role/myRedshiftRole"
            ]
        }
    ]
}
```

Mettez à jour la politique d'approbation du rôle IAM utilisé pour planifier la requête afin de permettre à l'utilisateur IAM de l'endosser.

```
{
            "Sid": "AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/myIAMusername"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Pour le rôle IAM que vous spécifiez pour autoriser l'exécution de la requête planifiée, modifiez le rôle IAM à l'aide de la console IAM (). https://console.aws.amazon.com/iam/

- Associez `AmazonRedshiftDataFullAccess` les politiques `AmazonEventBridgeFullAccess` AWS gérées au rôle IAM. La politique gérée `AmazonRedshiftDataFullAccess` accepte uniquement l'autorisation `redshift-serverless:GetCredentials` pour les groupes de travail Redshift sans serveur balisés avec la clé `RedshiftDataFullAccess`.

Authentification d’une requête planifiée

Lorsque vous planifiez une requête, vous utilisez l'une des méthodes d'authentification suivantes lors de l'exécution SQL. Les entrées à effectuer dans l'éditeur de requête v2 varient en fonction de la méthode utilisée. Ces méthodes d'authentification sont prises en charge par l'API de données utilisée pour exécuter vos instructions SQL.

L'utilisateur ou le rôle de base de données utilisé pour exécuter la requête doit disposer des privilèges de base de données nécessaires. Par exemple, pour accorder des privilèges `IAMR:MyRedshiftQEv2Scheduler` à la table `mytable`, exécutez la commande SQL suivante.

```
GRANT all ON TABLE mytable TO "IAMR:MyRedshiftQEv2Scheduler";
```

Pour afficher la liste des utilisateurs de base de données de votre cluster ou groupe de travail, interrogez la vue système `PG_USER_INFO`.

> **Note**
>
> Tout groupe de travail Redshift sans serveur pour lequel vous planifiez des requêtes doit être balisé avec la clé `RedshiftDataFullAccess`. Pour plus d’informations, consultez Autorisation de l’accès à l’API de données Amazon Redshift.
> Au lieu de baliser le groupe de travail, vous pouvez également ajouter une politique en ligne au rôle IAM (spécifié avec la planification) qui autorise `redshift-serverless:GetCredentials`. Par exemple :
>
> JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "UseTemporaryCredentialsForAllServerlessWorkgroups",
            "Effect": "Allow",
            "Action": "redshift-serverless:GetCredentials",
            "Resource": [
                "arn:aws:redshift-serverless:*:*:workgroup/*"
            ]
        }
```

```
    ]
}
```

AWS Secrets Manager

Avec cette méthode, fournissez une valeur secrète pour le paramètre secret-arn qui est stocké dans AWS Secrets Manager. Ce secret contient des informations d'identification pour vous connecter à votre base de données. Vous avez peut-être créé un secret avec les informations d'identification appropriées lorsque vous avez créé votre cluster ou votre groupe de travail. Le secret doit être étiqueté avec la clé `RedshiftDataFullAccess`. Si la clé de balise n'est pas déjà présente, utilisez la AWS Secrets Manager console pour l'ajouter. Pour plus d'informations sur la création d'un secret, consultez Création d'un secret pour les informations d'identification de connexion à une base de données.

Pour plus d'informations sur les autorisations minimales, consultez Création et gestion des secrets avec AWS Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager .

Informations d'identification temporaires

Avec cette méthode, indiquez le Nom de la base de données et l'Utilisateur de la base de données pour vous connecter à une base de données située dans un cluster. Vous devez simplement indiquer le Nom de la base de données au moment de vous connecter à une base de données d'un groupe de travail.

Lorsque vous vous connectez à un cluster, la politique `AmazonRedshiftDataFullAccess` accorde à l'utilisateur de base de données nommé `redshift_data_api_user` une autorisation pour `redshift:GetClusterCredentials`. Si vous souhaitez utiliser un autre utilisateur de base de données pour exécuter l'instruction SQL, ajoutez une politique au rôle IAM attaché à votre cluster pour autoriser `redshift:GetClusterCredentials`. L'exemple de stratégie suivant autorise les utilisateurs de base de données `awsuser` et `myuser`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "UseTemporaryCredentialsForAllDbUsers",
            "Effect": "Allow",
```

```
            "Action": "redshift:GetClusterCredentials",
            "Resource": [
                "arn:aws:redshift:*:*:dbuser:*/awsuser",
                "arn:aws:redshift:*:*:dbuser:*/myuser"
            ]
        }
    ]
}
```

Configuration d'autorisations pour consulter l'historique des requêtes planifiées

Pour permettre aux utilisateurs de consulter l'historique des requêtes planifiées, modifiez le rôle IAM (spécifié avec la planification) Relations d'approbation pour ajouter les autorisations.

Voici un exemple de politique de confiance dans un rôle IAM qui permet à l'utilisateur IAM de consulter l'historique *myIAMusername* des requêtes de planification. Au lieu d'accorder à un utilisateur IAM l'autorisation `sts:AssumeRole`, vous pouvez choisir d'accorder à un rôle IAM cette autorisation.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "redshift.amazonaws.com",
                    "redshift-serverless.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "events.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
```

```
        },
        {
            "Sid": "AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/myIAMusername"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Surveillance de la requête planifiée

Pour la rubrique Amazon SNS que vous spécifiez pour l'envoi de notifications par e-mail, créez la rubrique Amazon SNS à l'aide de l'éditeur de requête v2 en accédant à la section Notifications SNS, choisissez Activer pour la surveillance, puis créez la rubrique avec Créer une rubrique SNS. L'éditeur de requêtes v2 crée la rubrique Amazon SNS et ajoute un principal de service à la politique d'accès d'Amazon. EventBridge Voici un exemple de Statégie d'accès qui est créé dans la rubrique Amazon SNS. Dans l'exemple, les Région AWS *us-west-2* rubriques Compte AWS *123456789012*,, et Amazon SNS *select-version-pdx-testunload* sont utilisées.

JSON

```
{
  "Version":"2012-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "Allow_Publish_Events",
      "Effect": "Allow",
      "Principal": {
        "Service": "events.amazonaws.com"
      },
      "Action": "sns:Publish",
      "Resource": "arn:aws:sns:us-west-2:123456789012:select-version-pdx-
testunload"
    }
  ]
}
```

Lorsque la requête planifiée est exécutée, Amazon SNS envoie des e-mails de AWS notification. L'exemple suivant montre un e-mail envoyé à *myemail@example.com* pour une requête planifiée *QS2-may25a* qui s'est exécuté Région AWS *eu-north-1* dans le cadre de la Compte AWS *123456789012* rubrique de notification Amazon SNS. *may25a-SNS*

```
{"version":"0","id":"8e4323ec-5258-7138-181b-91290e30ff9b","detail-type":"Scheduled
 Event","source":"aws.events","account":"123456789012","time":"2023-05-25T15:22:00Z",
                    "region":"eu-north-1","resources":["arn:aws:events:eu-
north-1:123456789012:rule/QS2-may25a"],"detail":{}}

--
If you wish to stop receiving notifications from this topic, please click or visit the
 link below to unsubscribe:
https://sns.eu-north-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:eu-
north-1:123456789012:may25a-SNS:0c1a3d05-39c2-4507-
bc3d-47250513d7b0&Endpoint=myemail@example.com

Please do not reply directly to this email. If you have any questions or comments
 regarding this email, please contact us at https://aws.amazon.com/support
```

Résolution des problèmes liés à la configuration de la planification d'une requête

Si vous rencontrez des problèmes pour planifier une requête, tenez compte des points suivants.

Les requêtes ne s'exécutent pas

Vérifiez que le rôle IAM utilisé dans la planification est autorisé à obtenir les informations d'identification temporaires du cluster. L'autorisation pour les clusters provisionnés est `redshift:GetClusterCredentialsWithIAM`. L'autorisation pour les groupes de travail Redshift sans serveur est `redshift-serverless:GetCredentials`.

L'historique planifié ne s'affiche pas

L'utilisateur IAM ou le rôle IAM utilisé pour se connecter à la AWS console n'a pas été ajouté à la politique de confiance du rôle IAM utilisé pour planifier la requête.

Lors de l'utilisation AWS Secrets Manager de la requête planifiée pour se connecter, vérifiez que le secret est marqué avec la clé`RedshiftDataFullAccess`.

Si la requête planifiée utilise une AWS Secrets Manager connexion, le rôle IAM utilisé pour planifier la requête doit avoir l'équivalent d'une politique gérée `SecretsManagerReadWrite` attachée au rôle.

L'état de l'historique des requêtes est **`Failed`**

Consultez la vue système SYS_QUERY_HISTORY pour obtenir des détails sur les raisons de l'échec de la requête. Il est possible que l'utilisateur ou le rôle de base de données ayant servi à exécuter la requête ne disposait pas des privilèges nécessaires pour exécuter la requête SQL. Pour plus d'informations, consultez Authentification d'une requête planifiée.

Les requêtes SQL suivantes interrogent la vue SYS_QUERY_HISTORY pour renvoyer les requêtes ayant échoué.

```
SELECT user_id, query_id, transaction_id, session_id, database_name, query_type,
 status, error_message, query_text
FROM sys_query_history
WHERE status = 'failed';
```

Pour rechercher des informations à propos de l'échec d'une requête planifiée spécifique, consultez Afficher les résultats d'une requête planifiée avec AWS CloudShell.

Afficher les résultats d'une requête planifiée avec AWS CloudShell

Vous pouvez l'utiliser AWS CloudShell pour obtenir des informations sur une requête de planification. Vous devez disposer des autorisations appropriées pour exécuter les AWS CLI commandes indiquées dans la procédure suivante.

Pour afficher les résultats d'une requête planifiée

1. Sur la AWS console, ouvrez l'invite de AWS CloudShell commande. Pour plus d'informations AWS CloudShell, voir Contenu du guide AWS CloudShell de l'AWS CloudShell utilisateur.
2. Endossez le rôle IAM de la requête planifiée. Pour endosser le rôle, recherchez le rôle IAM associé à la requête planifiée dans l'éditeur de requête v2 et utilisez-le dans la commande de l' AWS CLI dans AWS CloudShell. Par exemple, pour le rôle `scheduler`, entrez une commande AWS STS pour endosser le rôle utilisé par la requête planifiée.

   ```
   aws sts assume-role --role-arn "arn:aws:iam::123456789012:role/scheduler" --role-
   session-name "scheduler-test"
   ```

   Les informations d'identification renvoyées se présentent comme suit.

   ```
   "Credentials": {
   ```

```
"AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
"SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
"SessionToken": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY...",
"Expiration": "2023-08-18T18:19:44+00:00"
},
"AssumedRoleUser": {
"AssumedRoleId": "AROA35B2NH6WBTP7ONL4E:scheduler-test",
"Arn": "arn:aws:sts::123456789012:assumed-role/scheduler/scheduler-test"
}
}
```

3. Créez des variables environnementales en AWS CLI utilisant les informations d'identification affichées lorsque vous assumez le rôle IAM. Vous devez utiliser ces jetons avant qu'ils n'arrivent à expiration. Par exemple, vous entrez ce qui suit dans AWS CloudShell.

```
export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
export AWS_SESSION_TOKEN=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY...
```

4. Pour voir l'erreur d'une requête ayant échoué, exécutez la AWS CLI commande pour décrire une instruction. L'ID de l'instruction SQL est tiré du champ ID figurant dans l'Historique de planification d'une requête planifiée dans l'éditeur de requête v2.

```
aws redshift-data describe-statement --id 130d2620-05d2-439c-b7cf-815d9767f513
```

Dans cet exemple, la requête SQL planifiée `select * from users limit 100` génère une erreur SQL indiquant que la table `users` n'existe pas.

```
{
"CreatedAt": "2023-08-18T17:39:15.563000+00:00",
"Duration": -1,
"Error": "ERROR: relation \"users\" does not exist",
"HasResultSet": false,
"Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
"QueryString": "select * from users limit 100\n—RequestID=a1b2c3d4-5678-90ab-cdef-
EXAMPLE22222; TraceID=1-633c5642-4039308d03f3a0ba53dbdf6f",
"RedshiftPid": 1073766651,
"RedshiftQueryId": 0,
"ResultRows": -1,
"ResultSize": -1,
"Status": "FAILED",
```

```
"UpdatedAt": "2023-08-18T17:39:16.116000+00:00",
"WorkgroupName": "default"
}
```

Visualisation des résultats de requêtes

Une fois que vous avez exécuté une requête et que les résultats sont affichés, vous pouvez activerChart (Graphique) pour afficher une visualisation graphique de la page actuelle des résultats. Vous pouvez utiliser les contrôles suivants pour définir le contenu, la structure et l'apparence de votre graphique :

Trace



Représente un ensemble de repères graphiques associés dans un graphique. Vous pouvez définir plusieurs traces dans un graphique.

Type

Vous pouvez définir le type de trace pour représenter les données comme l'une des options suivantes :

- Graphique à nuages de points pour un nuage de points ou un graphique à bulles.
- Graphique à barres pour représenter les catégories de données avec des barres verticales ou horizontales.
- Graphique en aires pour définir les zones remplies.
- Histogramme qui utilise des barres pour représenter la distribution des fréquences.
- Graphique en secteurs pour une représentation circulaire de données où chaque tranche représente un pourcentage de l'ensemble.
- Graphique en entonnoir ou en zone d'entonnoir pour représenter les données à travers les différentes étapes d'un processus.
- Le graphique OHLC (open-high-low-close) est souvent utilisé pour les données financières afin de représenter les valeurs d'ouverture, de maximum, de minimum et de clôture le long de l'axe des x, qui représente généralement des intervalles de temps.
- Graphique en chandelier pour représenter une plage de valeurs pour une catégorie sur une chronologie.

- Graphique en cascade pour représenter la façon dont une valeur initiale augmente ou diminue à travers une série de valeurs intermédiaires. Les valeurs peuvent représenter des intervalles de temps ou des catégories.
- Graphique en courbes pour représenter les changements de valeur au fil du temps.

Axe des X

Vous spécifiez une colonne de tableau qui contient des valeurs à tracer le long de l'axe des X. Les colonnes qui contiennent des valeurs descriptives représentent généralement des données dimensionnelles. Les colonnes qui contiennent des valeurs quantitatives représentent généralement des données factuelles.

Axe des Y

Vous spécifiez une colonne de tableau qui contient des valeurs à tracer le long de l'axe Y. Les colonnes qui contiennent des valeurs descriptives représentent généralement des données dimensionnelles. Les colonnes qui contiennent des valeurs quantitatives représentent généralement des données factuelles.

Sous-parcelles

Vous pouvez définir des présentations supplémentaires de données graphiques.

Transforme

Vous pouvez définir des transformations pour filtrer les données de trace. Vous utilisez une transformation fractionnée pour afficher plusieurs traces à partir d'une trace source unique. Vous utilisez une transformation agrégée pour présenter une trace sous forme de moyenne ou de minimum. Vous utilisez une transformation de tri pour trier une trace.

Apparence générale

Vous pouvez définir les valeurs par défaut pour la couleur d'arrière-plan, la couleur de la marge, les échelles de couleurs pour créer des palettes, le style et les tailles du texte, le style et la taille du titre et la barre de mode. Vous pouvez définir des interactions pour faire glisser, cliquer et survoler. Vous pouvez définir un métatexte. Vous pouvez définir des apparences par défaut pour les traces, les axes, les légendes et les annotations.

Pour créer un diagramme

1. Exécutez une requête et obtenez des résultats.
2. Activez Charts (Diagrammes).

3. Choisissez Trace (Suivi) et commencez à visualiser vos données.
4. Choisissez un style de diagramme parmi les options suivantes :
   - Scatter (À points)
   - Bar (À barres)
   - Area
   - Histogramme
   - Pie (À secteurs)
   - Funnel (Synthèse)
   - Entonnoir (Zone de synthèse)
   - OHLC (open-high-low-close)
   - Candlestick (Chandelier)
   - Waterfall (Cascade)
   - Line
5. Choisissez Style pour personnaliser l'apparence, y compris les couleurs, les axes, la légende et les annotations. Vous pouvez ajouter du texte, des formes et des images.
6. Choisissez Annotations pour ajouter du texte, des formes et des images.
7. Pour mettre à jour l'affichage du diagramme, choisissez Refresh (Actualiser). Choisissez Full screen (Plein écran) pour développer l'affichage du diagramme.

Exemple : créer un diagramme à secteurs pour visualiser les résultats de la requête

L'exemple suivant utilise la table Sales (Ventes) de l'exemple de base de données. Pour plus d'informations, consultez Exemple de base de données dans le Guide du développeur de base de données Amazon Redshift.

Voici la requête que vous exécutez pour fournir les données du diagramme à secteurs.

```
select top 5 eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid group by eventname
order by 3;
```

Pour créer un diagramme à secteurs pour l'événement le plus important en fonction des ventes totales

1. Exécutez la requête.
2. Dans la zone de résultats de la requête, activez Chart (Diagramme).
3. Sélectionnez Trace (Suivi).
4. Pour Type, choisissez Pie (À secteurs).
5. Pour Values (Valeurs), choisissez totalsales.
6. Pour Labels (Étiquettes), choisissez eventname.
7. Choisissez Style, puis General (Général).
8. Sous Colorscales, choisissez Categorical (catégorie), puis Pastel 2.



Exemple : créer un graphique combiné pour comparer le chiffre d'affaires et les ventes

Effectuez les étapes de cet exemple pour créer un graphique qui combine un graphique à barres pour les données de chiffre d'affaires et un graphique linéaire pour les données de vente. L'exemple suivant utilise le tableau Sales (Ventes) de l'exemple de base de données tickit. Pour plus d'informations, consultez Exemple de base de données dans le Guide du développeur de base de données Amazon Redshift.

Voici la requête que vous exécutez pour fournir les données du graphique.

```
select eventname, total_price, total_qty_sold
from  (select eventid, total_price, total_qty_sold, ntile(1000) over(order by
 total_price desc) as percentile
       from (select eventid, sum(pricepaid) total_price, sum(qtysold) total_qty_sold
```

```
            from   tickit.sales
            group by eventid)) Q, tickit.event E
       where Q.eventid = E.eventid
       and percentile = 1
order by total_price desc;
```

Pour créer un graphique combiné permettant de comparer le chiffre d'affaires et les ventes

1. Exécutez la requête.
2. Dans la zone de résultats de la requête, activez Chart (Diagramme).
3. Sous trace o, pour Type, choisissez Barres.
4. Pour X, choisissez eventname.
5. Pour Y, choisissez total_price.

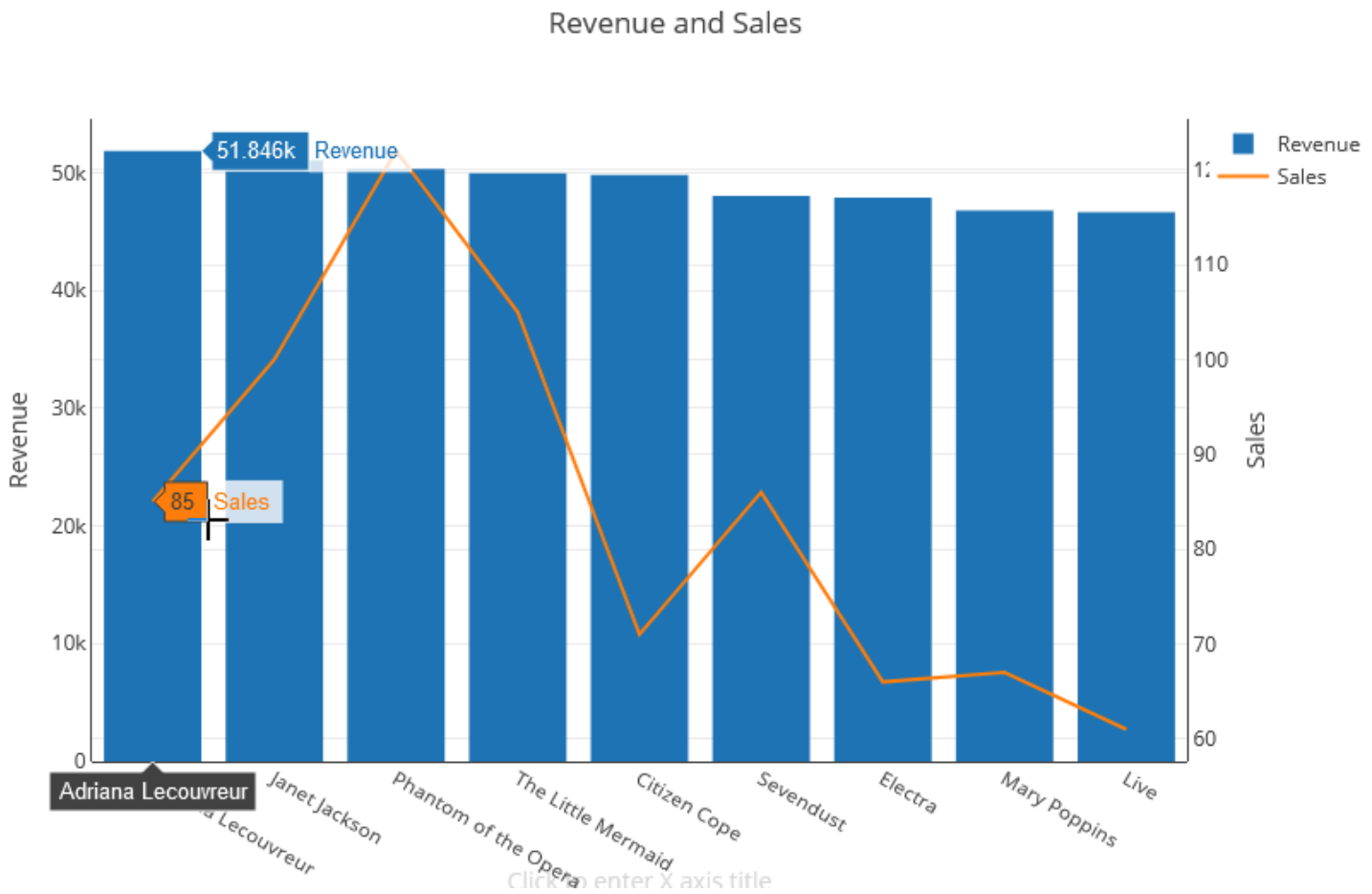
   Le graphique à barres s'affiche avec des noms d'événements le long de l'axe des X.
6. Sous Style, choisissez Traces.
7. Pour Name (Nom), saisissez Revenue (Chiffre d'affaires).
8. Sous Style, choisissez Axes.
9. Pour Titres, choisissez Y, puis saisissez Chiffre d'affaires.

   L'étiquette Chiffre d'affaires s'affiche sur l'axe Y gauche.
10. Sous Structure, choisissez Traces.
11. Choisissez
    +
    Trace.

    Les options de la trace 1 s'affichent.
12. Pour Type, choisissez Ligne.
13. Pour X, choisissez eventname.
14. Pour Y, choisissez total_qty_sold.
15. Sous Axes à utiliser, pour Axe des Y choisissez
    +
    .

    L'Axe des Y affiche Y2.
16. Sous Style, choisissez Axes.

17. Sous Titres, choisissez Y2.
18. Pour Nom, saisissez Ventes.
19. Sous Lignes, choisissez Y:Sales.
20. Sous Ligne d'axe, choisissez Afficher, puis pour Position, choisissez Droite.



Démo : créez des visualisations à l'aide de Amazon Redshift Query Editor V2

Pour une démonstration de création de visualisations, regardez la vidéo suivante. Créer des visualisations à l'aide de l'éditeur de requête v2 Amazon Redshift.

Collaborer et partager en équipe

Vous pouvez partager des requêtes avec votre équipe.

Une équipe est définie pour un ensemble d'utilisateurs qui collaborent et partagent des ressources de l'éditeur de requête v2. Un administrateur peut créer une équipe en ajoutant une balise à un rôle IAM. Pour plus d'informations, consultez Autorisations requises pour utiliser l'éditeur de requête v2.

Sauvegarde et navigation pour les requêtes

Avant de pouvoir partager votre requête avec votre équipe, enregistrez votre requête. Vous pouvez afficher et supprimer les requêtes enregistrées.

Pour enregistrer une requête

1. Préparez votre requête et choisissez Save (Enregistrer).
2. Saisissez un titre pour votre requête.
3. Choisissez Enregistrer.

Pour rechercher les requêtes enregistrées

1. Dans le panneau de navigation, choisissez Queries (Requêtes).
2. Vous pouvez afficher les requêtes My queries (Mes requêtes), Shared by me (Partagé par moi) ou Shared to my team (Partagé avec mon équipe). Ces requêtes peuvent apparaître sous forme de requêtes individuelles ou dans des dossiers que vous avez créés.

Partage d'une requête

Vous pouvez partager vos requêtes avec votre équipe. Vous pouvez également afficher l'historique des requêtes enregistrées et gérer les versions des requêtes.

Pour partager une requête avec votre équipe, assurez-vous que la balise principale `sqlworkbench-team` est définie sur la même valeur que les autres membres de votre équipe dans votre compte. Par exemple, un administrateur peut définir la valeur sur `accounting-team` pour tous les membres du service comptable. Pour obtenir un exemple, consultez Autorisations requises pour utiliser l'éditeur de requête v2.

Pour partager une requête avec une équipe

1. Dans le panneau de navigation, choisissez Queries (Requêtes).
2. Ouvrez le menu contextuel (clic droit) de la requête que vous souhaitez partager et choisissez Share with my team (Partager avec mon équipe).
3. Choisissez la ou les équipes avec lesquelles vous souhaitez partager la requête, puis choisissez Save sharing options (Enregistrer les options de partage).

Gestion des versions des requêtes

Chaque fois que vous enregistrez une requête SQL, l'éditeur de requête v2 l'enregistre en tant que nouvelle version. Vous pouvez parcourir les versions antérieures des requêtes, enregistrer une copie d'une requête ou restaurer une requête.

Pour gérer les versions des requêtes

1. Dans le panneau de navigation, choisissez Queries (Requêtes).
2. Ouvrez le menu contextuel (clic droit) de la requête que vous souhaitez utiliser.
3. Choisissez Version history (Historique des versions) pour ouvrir une liste de versions de la requête.
4. Sur la page Version history (Historique des versions), vous pouvez effectuer les actions suivantes :
   - Revert to selected (Restaurer la sélection) – Revenez à la version sélectionnée et continuez à utiliser cette version.
   - Save selected as (Enregistrer la sélection sous) – Créez une requête dans l'éditeur.

Interrogation d'une base de données à l'aide de l'éditeur de requêtes Amazon Redshift v1

Utiliser l'éditeur de requête est la façon la plus simple d'exécuter des requêtes sur les bases de données hébergées par votre cluster Amazon Redshift. Après avoir créé votre cluster, vous pouvez exécuter immédiatement des requêtes en utilisant l'éditeur de requête dans la console Amazon Redshift.

> **Note**
>
> Vous ne pouvez pas interroger des données dans Amazon Redshift sans serveur à l'aide de cet éditeur de requêtes original. Utilisez plutôt l'Éditeur de requêtes v2 Amazon Redshift.

En février 2021, un éditeur de requête mis à jour a été déployé et les autorisations d'utilisation de l'éditeur de requête ont été modifiées. Le nouvel éditeur de requêtes utilise l'API Amazon Redshift Data pour exécuter des requêtes. La `AmazonRedshiftQueryEditor` politique, qui est une

politique AWS gérée Gestion des identités et des accès AWS (IAM), a été mise à jour pour inclure les autorisations nécessaires. Si vous avez une politique IAM personnalisée, assurez-vous de la mettre à jour. Utilisez `AmazonRedshiftQueryEditor` comme guide. Les modifications apportées à `AmazonRedshiftQueryEditor` sont les suivantes :

- L'autorisation de gérer les résultats de l'instruction de l'éditeur de requête nécessite l'utilisateur propriétaire de l'instruction.
- L'autorisation d'utiliser Secrets Manager pour se connecter à une base de données a été ajoutée.

Pour plus d'informations, consultez Autorisations requises pour utiliser l'éditeur de requêtes de la console Amazon Redshift.

Lorsque vous vous connectez à votre cluster à partir du nouvel éditeur de requêtes, vous pouvez utiliser l'une des deux méthodes d'authentification.

L'éditeur de requête vous permet d'effectuer les opérations suivantes :

- Exécutez des requêtes d'instruction SQL unique.
- Téléchargez des jeux de résultats pouvant atteindre 100 Mo dans un fichier de valeurs séparées par des virgules (CSV).
- Enregistrez les requêtes dans le but de les réutiliser. Vous ne pouvez pas enregistrer les requêtes dans les régions Europe (Paris), Asie-Pacifique (Osaka), Asie-Pacifique (Hong Kong) ou Moyen-Orient (Bahreïn).
- Affichez les détails d'exécution de requête pour les tables définies par l'utilisateur.
- Planifiez l'exécution des requêtes à un moment ultérieur.
- Affichez un historique des requêtes que vous avez créées dans l'éditeur de requêtes.
- Exécutez des requêtes sur des clusters à l'aide du routage VPC amélioré.

Considérations relatives à l'éditeur de requête

Considérez ce qui suit sur l'utilisation des requêtes lorsque vous utilisez l'éditeur de requête :

- La durée maximale d'une requête est de 24 heures.
- La taille maximale du résultat de requête est de 100 Mo. Si un appel renvoie plus de 100 Mo de données de réponse, l'appel est arrêté.

- La durée maximale de conservation des résultats de la requête est de 24 heures.
- La taille maximale de l'instruction de requête est de 100 Ko.
- Le cluster doit être créé dans un cloud privé virtuel (VPC) basé sur le service Amazon VPC.
- Vous ne pouvez pas utiliser les transactions dans l'éditeur de requête. Pour plus d'informations sur les transactions, consultez BEGIN dans le Manuel du développeur de base de données Amazon Redshift.
- Vous pouvez enregistrer une requête de 3 000 caractères maximum.

En vous connectant à un entrepôt de données Amazon Redshift à l'aide des outils client SQL

Vous pouvez vous connecter aux entrepôts de données Amazon Redshift depuis les outils clients SQL via des connexions Java Database Connectivity (JDBC), Python et Open Database Connectivity (ODBC). Amazon Redshift ne fournit et n'installe pas de bibliothèques ou d'outils clients SQL. Pour utiliser ces outils ou bibliothèques afin de travailler avec les données de vos entrepôts de données, installez-les sur votre ordinateur client ou votre instance Amazon EC2. Vous pouvez utiliser la plupart des outils clients SQL qui prennent en charge les pilotes ODBC, Python ou JDBC.

Consultez la liste des sections à la fin de cette rubrique pour parcourir le processus de configuration de votre ordinateur client ou de votre instance Amazon EC2 afin de lui faire utiliser une connexion JDBC, Python ou ODBC. Les rubriques discutent également des options de sécurité associées pour la connexion du client au serveur. Par ailleurs, vous trouverez des informations sur la configuration et la connexion à partir d'outils clients SQL, tels que Amazon Redshift RSQL. Vous pouvez essayer ces outils si vous n'avez pas encore d'outil de Business Intelligence à utiliser. Vous pouvez également utiliser cette section pour en savoir plus sur la connexion à vos données. Enfin, si vous rencontrez des problèmes lorsque vous essayez de vous connecter à votre entrepôt de données, vous pouvez consulter les informations sur la résolution des problèmes afin d'identifier les solutions.

Recommandations pour la connexion avec des outils clients

Si vous vous connectez à votre cluster Redshift à l'aide d'une adresse IP, cela peut entraîner des durées d'indisponibilité supplémentaires en cas de panne ou de perte de connexion, et le cluster est mis en ligne dans une nouvelle zone de disponibilité (AZ). Toutefois, si vous souhaitez toujours que votre application se connecte à Redshift à l'aide d'une adresse IP, utilisez l'adresse IP privée attachée au point de terminaison du cloud privé virtuel (VPC) du cluster. Vous pouvez le trouver dans les détails du cluster, dans Réseau et sécurité, sous l'onglet Propriétés.

> **Note**
>
> Si votre application utilise l'adresse IP du nœud principal pour accéder au cluster Redshift, il est recommandé de la modifier pour utiliser l'URL du point de terminaison du cluster. Pour plus d'informations, consultez Configuration des connexions dans Amazon Redshift.

Rubriques

- Configuration des connexions dans Amazon Redshift
- Bonnes pratiques pour découvrir les métadonnées
- Configuration des options de sécurité des connexions
- Connexion à partir d'outils et de codes clients
- Utilisation d'un profil d'authentification pour se connecter à Amazon Redshift
- Résolution des problèmes de connexion dans Amazon Redshift

Configuration des connexions dans Amazon Redshift

Dans la section suivante, découvrez comment configurer les connexions JDBC, Python et ODBC afin de vous connecter à votre cluster à partir d'outils clients SQL. Cette section décrit comment configurer les connexions JDBC, Python et ODBC. Elle décrit également comment utiliser Secure Sockets Layer (SSL) et les certificats de serveur pour chiffrer la communication entre le client et le serveur.

Pilotes JDBC, Python et ODBC pour Amazon Redshift

Pour utiliser les données de votre cluster, vous devez disposer de pilotes JDBC, Python ou ODBC pour la connectivité à partir de votre ordinateur client ou instance. Codez vos applications afin d'utiliser des opérations d'API d'accès aux données JDBC, Python ou ODBC et utilisez des outils client SQL qui prennent en charge JDBC, Python ou ODBC.

Amazon Redshift propose des pilotes JDBC, Python et ODBC à télécharger. Ces pilotes sont pris en charge par Support. Les pilotes PostgreSQL ne sont pas testés et ne sont pas pris en charge par l'équipe Amazon Redshift. Utilisez les pilotes spécifiques à Amazon RedShift lorsque vous vous connectez à un cluster Amazon Redshift. Les pilotes Amazon Redshift présentent les avantages suivants :

- Prise en charge de l'authentification IAM, SSO et fédérée.
- Prise en charge des nouveaux types de données Amazon Redshift.
- Prise en charge des profils d'authentification.
- Performances améliorées en conjonction avec les améliorations d'Amazon Redshift.

Pour plus d'informations sur le téléchargement des pilotes JDBC et ODBC et la configuration des connexions à votre cluster, consultez Configuration d'une connexion pour la version 2.x du pilote JDBC pour Amazon Redshift, Connecteur Amazon Redshift Python et Configuration d'une connexion pour le pilote ODBC version 2.x pour Amazon Redshift.

Pour plus d'informations sur la gestion des identités IAM, y compris les bonnes pratiques pour les rôles IAM, consultez Identity and Access Management dans Amazon Redshift.

Recherche de votre chaîne de connexion au cluster

Pour vous connecter à votre cluster avec votre outil client SQL, vous devez disposer de la chaîne de connexion au cluster. Vous pouvez trouver la chaîne de connexion du cluster dans la console Amazon Redshift, sur la page de détails d'un cluster.

Pour rechercher la chaîne de connexion d'un cluster

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters, puis choisissez le nom du cluster dans la liste pour ouvrir ses détails.
3. Les chaînes de connexion JDBC URL et ODBC URL sont disponibles, ainsi que des détails supplémentaires dans la section Informations générales. Chaque chaîne est basée sur la AWS région dans laquelle le cluster s'exécute. Cliquez sur l'icône en regard de la chaîne de connexion appropriée pour copier celle-ci.

Pour vous connecter à un point de terminaison de cluster, vous pouvez utiliser l'URL du point de terminaison du cluster provenant d'une demande d'DescribeClusters API. Voici un exemple d'URL de point de terminaison d'un cluster.

```
mycluster.cmeaswqeuae.us-east-2.redshift.amazonaws.com
```

Si vous avez configuré un nom de domaine personnalisé pour votre cluster, vous pouvez également vous en servir pour vous connecter à votre cluster. Pour en savoir plus sur la création d'un nom de domaine personnalisé, consultez Configuration d'un nom de domaine personnalisé.

> **Note**
>
> Lorsque vous vous connectez, n'utilisez pas l'adresse IP d'un nœud de cluster ou l'adresse IP du point de terminaison d'un VPC. Utilisez toujours le point de terminaison Redshift pour éviter une panne inutile. La seule exception à l'utilisation de l'URL du point de terminaison est lorsque vous utilisez un nom de domaine personnalisé. Pour plus d'informations, consultez Utilisation d'un nom de domaine personnalisé pour les connexions client.

Configuration d'une connexion pour la version 2.x du pilote JDBC pour Amazon Redshift

Vous pouvez utiliser une connexion au pilote JDBC version 2.x pour vous connecter à votre cluster Amazon Redshift à partir de nombreux outils clients SQL tiers. Le connecteur Amazon Redshift JDBC fournit une solution open source. Vous pouvez parcourir le code source, demander des améliorations, signaler des problèmes et apporter des contributions.

Pour obtenir les dernières informations sur les modifications du pilote JDBC, consulter le journal des modifications.

Par défaut, le pilote JDBC d'Amazon Redshift est configuré pour utiliser les keepalives TCP afin d'empêcher les connexions de s'interrompre. Vous pouvez spécifier le moment où le pilote commence à envoyer des paquets keepalive ou désactiver la fonction en définissant les propriétés pertinentes dans l'URL de la connexion. Pour plus d'informations sur la syntaxe de l'URL de connexion, consultez Création de l'URL de connexion.

Propriété	Description
`TCPKeepAlive`	Pour désactiver les keepalives TCP, définissez cette propriété sur `FALSE`.

Rubriques

- Téléchargez le pilote Amazon Redshift JDBC, version 2.x

- Installation du pilote Amazon Redshift JDBC, version 2.x
- Obtention de l'URL JDBC
- Création de l'URL de connexion
- Configuration d'une connexion JDBC avec Apache Maven
- Configuration de l'authentification et du protocole SSL
- Configuration de la journalisation
- Conversions du type de données
- Utilisation du support d'instructions préparées
- Différences entre les versions 2.x et 1.x du pilote JDBC
- Création de fichiers d'initialisation (.ini) pour le pilote JDBC version 2.x
- Options de configuration du pilote JDBC version 2.x
- Versions précédentes du pilote JDBC version 2.x

Téléchargez le pilote Amazon Redshift JDBC, version 2.x

> **Note**
>
> Le pilote Amazon Redshift JDBC 2.x n'est pas conçu pour être thread-safe. Deux threads ou plus qui tentent simultanément d'utiliser la même connexion peuvent entraîner des blocages, des erreurs, des résultats incorrects ou d'autres comportements inattendus.
> Si vous avez une application multithread, nous vous recommandons de synchroniser l'accès au pilote pour éviter les accès simultanés.

Amazon Redshift propose des pilotes pour les outils qui sont compatibles avec l'API JDBC 4.2. Le nom de la classe de ce pilote est `com.amazon.redshift.Driver`.

Pour obtenir des informations détaillées sur la manière d'installer le pilote JDBC, de référencer les bibliothèques du pilote JDBC et d'enregistrer la classe du pilote, consultez les rubriques suivantes.

Pour chaque ordinateur où vous utilisez le pilote JDBC Amazon Redshift version 2.x, assurez-vous que l'Environnement d'exécution Java (JRE) (JRE) 8.0 est installé.

Si vous utilisez le pilote Amazon Redshift JDBC pour l'authentification de base de données, assurez-vous que le chemin de classe Java contient la version AWS SDK pour Java 2.40.5 ou ultérieure. Si

ce n'est pas le cas AWS SDK pour Java , téléchargez le fichier ZIP contenant le pilote compatible avec JDBC 4.2 et les bibliothèques dépendantes du pilote pour le SDK : AWS

- Version 2.x du pilote compatible JDBC 4.2 et bibliothèques AWS dépendantes du pilote du SDK Dans la région de Chine (Pékin), cliquez sur le lien suivant : pilote compatible JDBC pilote du SDK AWS

  Ce fichier ZIP contient la version 2.x du pilote compatible JDBC 4.2 et les fichiers de bibliothèque dépendants du pilote SDK for AWS Java 2.x. Décompressez les fichiers jar dépendants au même emplacement que le pilote JDBC. Seul le pilote JDBC doit être dans CLASSPATH.

  Ce fichier ZIP n'inclut pas le AWS SDK complet pour Java 2.x. Toutefois, il inclut les bibliothèques dépendantes du pilote AWS SDK for Java 2.x requises pour l'authentification (IAM) des bases Gestion des identités et des accès AWS de données.

  Utilisez ce pilote Amazon Redshift JDBC avec le AWS SDK requis pour l'authentification de base de données IAM.

  Pour installer le AWS SDK complet pour Java 2.x, AWS consultez la section SDK pour JavaAWS SDK pour Java 2.x dans le manuel du développeur.
- Version 2.x du pilote compatible JDBC 4.2 (sans le AWS SDK) Dans la région de Chine (Pékin) SDK) AWS

Examinez la licence logicielle du pilote JDBC version 2.x et modifiez le fichier journal :

- Licence du pilote JDBC version 2.x
- Journal des modifications du pilote JDBC version 2.x

Les pilotes JDBC version 1.2.27.1051 et ultérieures prennent en charge les procédures stockées Amazon Redshift. Pour plus d'informations, consultez Création de procédures stockées dans Amazon Redshift dans le Guide du développeur de base de données Amazon Redshift.

Installation du pilote Amazon Redshift JDBC, version 2.x

Pour installer la version 2.x du pilote compatible avec Amazon Redshift JDBC 4.2 et les bibliothèques dépendantes du pilote pour le AWS SDK, extrayez les fichiers de l'archive ZIP dans le répertoire de votre choix.

Pour installer la version 2.x du pilote compatible Amazon Redshift JDBC 4.2 (sans le kit SDK AWS), copiez le fichier JAR dans le répertoire de votre choix.

Pour accéder à un magasin de données Amazon Redshift à l'aide du pilote JDBC Amazon Redshift, vous devez définir la configuration comme décrit ci-dessous.

Rubriques

- Référencement des bibliothèques de pilotes JDBC
- Enregistrement de la classe de pilote

Référencement des bibliothèques de pilotes JDBC

L'application JDBC ou le code Java que vous utilisez pour vous connecter à vos données doit accéder aux fichiers JAR du pilote. Dans l'application ou le code, spécifiez tous les fichiers JAR que vous avez extraits de l'archive ZIP.

Utilisation du pilote dans une application JDBC

Les applications JDBC fournissent généralement un ensemble d'options de configuration pour ajouter une liste de fichiers de bibliothèque de pilotes. Utilisez les options disponibles pour inclure tous les fichiers JAR de l'archive ZIP comme partie intégrante de la configuration du pilote dans l'application. Pour plus d'informations, consultez la documentation de votre application JDBC.

Utilisation du pilote dans le code Java

Vous devez inclure tous les fichiers de la bibliothèque de pilotes dans le chemin d'accès de la classe. Il s'agit du chemin d'accès grâce auquel l'environnement d'exécution Java recherche les classes et autres fichiers de ressources. Pour plus d'informations, consultez la documentation Java SE appropriée pour définir le chemin d'accès de classe pour votre système d'exploitation.

- Windows: https://docs.oracle.com/javase/7/docs/technotes/tools/windows/classpath.html
- Linux et Solaris : https://docs.oracle.com/javase/7/docs/technotes/tools/solaris/classpath.html
- macOS : le chemin de classe macOS par défaut est le répertoire dans lequel le pilote JDBC est installé.

Enregistrement de la classe de pilote

Assurez-vous d’enregistrer la classe appropriée pour votre application. Vous utilisez les classes suivantes pour connecter le pilote JDBC Amazon Redshift aux magasins de données Amazon Redshift :

- Les classes `Driver` étendent `java.sql.Driver`.
- Les classes `DataSource` incluent également `javax.sql.DataSource` et `javax.sql.ConnectionPoolDataSource`.

Le pilote prend en charge les noms de classe complets suivants qui sont indépendants de la version JDBC :

- `com.amazon.redshift.jdbc.Driver`
- `com.amazon.redshift.jdbc.DataSource`

L'exemple suivant montre comment utiliser la DriverManager classe pour établir une connexion pour JDBC 4.2.

```
            private static Connection connectViaDM() throws Exception
{
Connection connection = null;
connection = DriverManager.getConnection(CONNECTION_URL);
return connection;
}
```

L’exemple suivant montre comment utiliser la classe `DataSource` pour établir une connexion.

```
 private static Connection connectViaDS() throws Exception
{
Connection connection = null;
11
Amazon Redshift JDBC Driver Installation and Configuration Guide
DataSource ds = new com.amazon.redshift.jdbc.DataSource
();
ds.setURL(CONNECTION_URL);
```

```
connection = ds.getConnection();
return connection;
}
```

Obtention de l'URL JDBC

Avant de pouvoir vous connecter à votre cluster Amazon Redshift à partir d'un outil client SQL, vous devez connaître l'URL JDBC de votre cluster. L'URL JDBC a le format suivant : `jdbc:redshift://endpoint:port/database`.

Les champs du format indiqué ci-dessus ont les valeurs suivantes.

Champ	Value
`jdbc`	Protocole de la connexion.
`redshift`	Le sous-protocole qui spécifie l'utilisation du pilote Amazon Redshift pour se connecter à la base de données.
endpoint	Le point de terminaison du cluster Amazon Redshift.
port	Numéro du port que vous avez spécifié lorsque vous avez lancé le cluster. Si vous avez un pare-feu, assurez-vous que ce port est ouvert pour que vous l'utilisiez.
database	Base de données que vous avez créée pour votre cluster.

Voici un exemple d'URL JDBC : `jdbc:redshift://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/dev`

Si vos valeurs d'URL contiennent l'un des caractères réservés d'URI suivants, les valeurs doivent être codées en URL :

- ;
- +
- {
- }

- [
-]
- &
- =
- ?
- un espace vide

Par exemple, si votre valeur `PWD` est `password:password`, une URL de connexion utilisant cette valeur ressemblera à ce qui suit :

```
jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/
dev;UID=amazon;PWD=password%3Apassword
```

Pour plus d'informations sur la création d'une connexion, consultez Recherche de votre chaîne de connexion au cluster.

Si l'ordinateur client ne peut pas se connecter à la base de données, il se peut que vous deviez résoudre d'éventuels problèmes. Pour plus d'informations, consultez Résolution des problèmes de connexion dans Amazon Redshift.

Création de l'URL de connexion

Utilisez l'URL de connexion pour fournir des informations de connexion au magasin de données auquel vous accédez. Voici le format de l'URL de connexion pour le pilote Amazon Redshift JDBC version 2.x. Ici, [Host] le point de terminaison du serveur Amazon Redshift et [Port] est le numéro du port TCP (Transmission Control Protocol) que le serveur utilise pour écouter les demandes des clients.

```
jdbc:redshift://[Host]:[Port]
```

Voici le format d'une URL de connexion qui spécifie certains paramètres facultatifs.

```
jdbc:redshift://[Host]:[Port]/[database];[Property1]=[Value];
[Property2]=[Value];
```

Si vos valeurs d'URL contiennent l'un des caractères réservés d'URI suivants, les valeurs doivent être codées en URL :

- ;
- +
- {
- }
- [
-]
- &
- =
- ?
- un espace vide

Par exemple, si votre valeur PWD est `password:password`, une URL de connexion utilisant cette valeur ressemblera à ce qui suit :

```
jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/
dev;UID=amazon;PWD=password%3Apassword
```

Par exemple, supposons que vous voulez vous connecter au port 9000 sur un cluster Amazon Redshift dans la région USA Ouest (Californie du Nord) sur AWS. Vous souhaitez également accéder à la base de données nommée dev et authentifier la connexion à l'aide d'un nom d'utilisateur et d'un mot de passe de base de données. Dans ce cas, vous pouvez également utiliser l'URL de connexion suivante.

```
jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/
dev;UID=amazon;PWD=amazon
```

Vous pouvez utiliser les caractères suivants pour séparer les options de configuration du reste de la chaîne d'URL :

- ;
- ?

Par exemple, les chaînes d'URL suivantes sont équivalentes :

```
jdbc:redshift://my_host:5439/dev;ssl=true;defaultRowFetchSize=100
```

```
jdbc:redshift://my_host:5439/dev?ssl=true;defaultRowFetchSize=100
```

Vous pouvez utiliser les caractères suivants pour séparer les options de configuration dans la chaîne d'URL :

- ;
- &

Par exemple, les chaînes d'URL suivantes sont équivalentes :

```
jdbc:redshift://my_host:5439/dev;ssl=true;defaultRowFetchSize=100
```

```
jdbc:redshift://my_host:5439/dev;ssl=true&defaultRowFetchSize=100
```

L'exemple d'URL suivant indique le niveau de journal 6 et le chemin d'accès des journaux.

```
jdbc:redshift://redshift.amazonaws.com:5439/dev;DSILogLevel=6;LogPath=/home/user/logs;
```

Ne dupliquez pas les propriétés de l'URL de connexion.

Pour connaître la liste complète des options de configuration que vous pouvez spécifier, consultez Options de configuration du pilote JDBC version 2.x.

> **Note**
>
> Lorsque vous vous connectez, n'utilisez pas l'adresse IP d'un nœud de cluster ou l'adresse IP du point de terminaison d'un VPC. Utilisez toujours le point de terminaison Redshift pour éviter une panne inutile. La seule exception à l'utilisation de l'URL du point de terminaison est lorsque vous utilisez un nom de domaine personnalisé. Pour plus d'informations, consultez Utilisation d'un nom de domaine personnalisé pour les connexions client.

Configuration d'une connexion JDBC avec Apache Maven

Apache Maven est un outil de gestion et de compréhension de projets logiciels. AWS SDK pour Java prend en charge les projets Apache Maven. Pour plus d'informations, consultez Utilisation du kit SDK avec Apache Maven dans le Guide du développeur AWS SDK pour Java .

Si vous utilisez Apache Maven, vous pouvez configurer et construire vos projets pour utiliser un pilote JDBC Amazon Redshift afin de vous connecter à votre cluster Amazon Redshift. Pour ce faire, ajoutez le pilote JDBC en tant que dépendance dans le fichier `pom.xml` de votre projet. Si vous utilisez Maven pour créer votre projet et que vous souhaitez faire appel à une connexion JDBC, suivez les étapes décrites dans cette section

Pour configurer le pilote JDBC en tant que dépendance Maven

1. Ajoutez le référentiel Amazon ou Maven Central dans la section des référentiels de votre fichier `pom.xml`.

   > **Note**
   >
   > L'URL dans le code suivant renvoie un exemple d'erreur si elle est utilisée dans un navigateur. Utilisez cette URL uniquement dans le contexte d'un projet Maven.

   Pour vous connecter à l'aide du protocole SSL, ajoutez le référentiel suivant à votre fichier `pom.xml`.

   ```
   <repositories>
       <repository>
         <id>redshift</id>
         <url>https://s3.amazonaws.com/redshift-maven-repository/release</url>
       </repository>
   </repositories>
   ```

   Pour un référentiel Maven Central, ajoutez ce qui suit à votre fichier `pom.xml`.

   ```
   <repositories>
       <repository>
         <id>redshift</id>
         <url>https://repo1.maven.org/maven2</url>
       </repository>
   </repositories>
   ```

2. Déclarez la version du pilote à utiliser dans la section des dépendances de votre fichier `pom.xml`.

Amazon Redshift propose des pilotes pour les outils qui sont compatibles avec l'API JDBC 4.2. Pour plus d'informations sur les fonctionnalités prises en charge par ces pilotes, consultez Téléchargez le pilote Amazon Redshift JDBC, version 2.x.

Remplacez *driver-version* dans l'exemple suivant avec votre version de pilote, par exemple, `2.1.0.1`. Pour un pilote compatible JDBC 4.2, utilisez ce qui suit.

```
<dependency>
   <groupId>com.amazon.redshift</groupId>
   <artifactId>redshift-jdbc42</artifactId>
   <version>driver-version</version>
</dependency>
```

Le nom de la classe de ce pilote est `com.amazon.redshift.Driver`.

Les pilotes Amazon Redshift Maven ont besoin des dépendances facultatives suivantes lorsque vous utilisez l'authentification de base de données IAM.

```
<dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-java-sdk-core</artifactId>
      <version>1.12.23</version>
      <scope>runtime</scope>
      <optional>true</optional>
</dependency>
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-java-sdk-redshift</artifactId>
      <version>1.12.23</version>
      <scope>runtime</scope>
      <optional>true</optional>
</dependency>
<dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-java-sdk-sts</artifactId>
      <version>1.12.23</version>
      <scope>runtime</scope>
      <optional>true</optional>
</dependency>
```

Pour mettre à niveau ou modifier le pilote JDBC Amazon Redshift vers la dernière version, modifiez d'abord la section version de la dépendance vers la dernière version du pilote. Ensuite, nettoyez le projet avec le plugin Maven Clean, comme indiqué ci-après.

```
mvn clean
```

Configuration de l'authentification et du protocole SSL

Pour protéger les données contre les accès non autorisés, les magasins de données Amazon Redshift exigent que toutes les connexions soient authentifiées à l'aide des informations d'identification de l'utilisateur. Certains magasins de données exigent également que les connexions soient établies via le protocole SSL, avec ou sans authentification unidirectionnelle.

Le pilote Amazon Redshift JDBC version 2.x fournit une prise en charge complète de ces protocoles d'authentification.

La version SSL prise en charge par le pilote dépend de la version JVM que vous utilisez. Pour plus d'informations sur les versions SSL prises en charge par chaque version de Java, consultez Diagnosing TLS, SSL, and HTTPS sur le blog Java Platform Group Product Management.

La version SSL utilisée pour la connexion est la version la plus élevée prise en charge par le pilote et le serveur, qui est déterminée au moment de la connexion.

Configurez le pilote JDBC Amazon Redshift version 2.x pour authentifier votre connexion conformément aux exigences de sécurité du serveur Redshift auquel vous vous connectez.

Vous devez toujours fournir votre nom d'utilisateur et votre mot de passe Redshift pour authentifier la connexion. Selon que SSL est activé et requis sur le serveur, vous devrez peut-être également configurer le pilote pour qu'il se connecte via SSL. Vous pouvez également utiliser l'authentification SSL à sens unique afin que le client (le pilote lui-même) vérifie l'identité du serveur.

Vous fournissez les informations de configuration au pilote dans l'URL de connexion. Pour plus d'informations sur la syntaxe de l'URL de connexion, consultez Création de l'URL de connexion.

Le protocole SSL indique TLS/SSL à la fois la sécurité de la couche transport et la couche des sockets sécurisés. Le pilote prend en charge les versions standard de. TLS/SSL

Configuration de l'authentification IAM

Si vous vous connectez à un serveur Amazon Redshift à l'aide de l'authentification IAM, définissez les propriétés suivantes dans le cadre de votre chaîne de connexion à la source de données.

Pour plus d'informations sur l'authentification IAM, consultez Identity and Access Management dans Amazon Redshift.

Pour utiliser l'authentification IAM, utilisez l'un des formats de chaîne de connexion suivants :

Chaîne de connexion	Description
`jdbc:redshift:iam:// [host]:[port]/[db]`	Chaîne de connexion régulière. Le pilote déduit les valeurs de ClusterID et Region de l'hôte.
`jdbc:redshift:iam:// [cluster-id]: [region]/[db]`	Le pilote récupère les informations sur l'hôte, en fonction des valeurs de ClusterID et Region.
`jdbc:redshift:iam:// [host]/[db]`	Le pilote utilise par défaut le port 5439 et déduit les valeurs de ClusterID et Region de l'hôte. En fonction du port que vous avez sélectionné lors de la création, de la modification ou de la migration du cluster, autorisez l'accès au port sélectionné.

Spécification des profils

Si vous utilisez l'authentification IAM, vous pouvez spécifier des propriétés de connexion supplémentaires obligatoires ou facultatives sous un nom de profil. Ce faisant, vous pouvez éviter de mettre certaines informations directement dans la chaîne de connexion. Vous spécifiez le nom du profil dans votre chaîne de connexion à l'aide de la propriété Profile.

Les profils peuvent être ajoutés au fichier AWS d'informations d'identification. L'emplacement par défaut de ce fichier est : `~/.aws/credentials`

Vous pouvez modifier la valeur par défaut en définissant le chemin d'accès dans la variable d'environnement suivante : `AWS_CREDENTIAL_PROFILES_FILE`

Pour plus d'informations sur les profils, consultez Utilisation d'informations d'identification AWS dans le AWS SDK pour Java.

Utilisation des informations d'identification du profil d'instance

Si vous exécutez une application sur une instance Amazon EC2 associée à un rôle IAM, vous pouvez vous connecter à l'aide des informations d'identification du profil d'instance.

Pour ce faire, utilisez l'un des formats de chaîne de connexion IAM du tableau précédent et définissez la propriété de connexion dbuser sur le nom d'utilisateur Amazon Redshift sous lequel vous vous connectez.

Pour plus d'informations sur les profils d'instance, consultez Gestion des accès dans le Guide de l'utilisateur IAM.

Utilisation des fournisseurs d'informations d'identification

Le pilote prend également en charge les plugins du fournisseur d'informations d'identification des services suivants :

- AWS Centre d'identité IAM
- Active Directory Federation Service (ADFS)
- Service de jetons web JSON (JWT)
- Services Microsoft Azure Active Directory (AD) et navigateur Microsoft Azure Active Directory (AD)
- Service Okta
- PingFederate Service
- Navigateur SAML pour les services SAML tels qu'Okta, Ping ou ADFS

Si vous utilisez l'un de ces services, l'URL de connexion doit spécifier les propriétés suivantes :

- Plugin_Name— Le chemin de classe complet pour la classe de plugin de votre fournisseur d'informations d'identification.
- IdP_Host : hôte du service que vous utilisez pour vous authentifier dans Amazon Redshift.
- IdP_Port : port sur lequel l'hôte du service d'authentification écoute. Non requis pour Okta.
- Utilisateur : nom d'utilisateur du serveur idp_host.
- Mot de passe : mot de passe associé au nom d'utilisateur idp_host.
- DbUser— Le nom d'utilisateur Amazon Redshift sous lequel vous vous connectez.
- SSL_Insecure : indique si le certificat du serveur IDP doit être vérifié.
- Client_ID— L'ID client associé au nom d'utilisateur dans le portail Azure AD. Utilisé uniquement pour Azure AD.
- Client_Secret— Le secret client associé à l'ID client dans le portail Azure AD. Utilisé uniquement pour Azure AD.

- IdP_Tenant : ID de locataire Azure AD pour votre application Amazon Redshift. Utilisé uniquement pour Azure AD.
- App_ID— L'ID d'application Okta pour votre application Amazon Redshift. Utilisé uniquement pour Okta.
- App_Name— Le nom d'application Okta facultatif pour votre application Amazon Redshift. Utilisé uniquement pour Okta.
- Partner_SPID— La valeur SPID (identifiant du fournisseur de services) optionnelle du partenaire. Utilisé uniquement pour PingFederate.
- Idc_Region— L' Région AWS emplacement de l'instance AWS IAM Identity Center. Utilisé uniquement pour AWS IAM Identity Center.
- Issuer_Url— Le point de terminaison de l'instance du serveur AWS IAM Identity Center. Utilisé uniquement pour AWS IAM Identity Center.

Si vous utilisez un plugin de navigateur pour l’un de ces services, l’URL de connexion peut également inclure les éléments suivants :

- Login_URL: l'URL de la ressource sur le site Web du fournisseur d'identité lorsque vous utilisez le langage SAML (Security Assertion Markup Language) ou les services Azure AD via un plug-in de navigateur. Ce paramètre est obligatoire si vous utilisez un plugin de navigateur.

- Listen_Port— Port utilisé par le pilote pour obtenir la réponse SAML du fournisseur d'identité lorsqu'il utilise les services SAML, Azure AD ou AWS IAM Identity Center via un plug-in de navigateur.

- IdP_ Response_Timeout — Durée, en secondes, pendant laquelle le pilote attend la réponse SAML du fournisseur d'identité lorsqu'il utilise les services SAML, Azure AD ou AWS IAM Identity Center via un plug-in de navigateur.

Pour plus d’informations sur les propriétés supplémentaires de la chaîne de connexion, consultez Options de configuration du pilote JDBC version 2.x.

Utilisation du nom d’utilisateur et du mot de passe uniquement

Si le serveur auquel vous vous connectez n’utilise pas SSL, il vous suffit de fournir votre nom d’utilisateur et votre mot de passe Redshift pour authentifier la connexion.

Pour configurer l’authentification en utilisant uniquement votre nom d’utilisateur et votre mot de passe Redshift

1. Définissez la propriété `UID` sur votre nom d’utilisateur Redshift pour accéder au serveur Amazon Redshift.
2. Définissez la propriété PWD avec le mot de passe correspondant à votre nom d’utilisateur Redshift.

Utilisation de SSL sans vérification d’identité

Si le serveur auquel vous vous connectez utilise SSL, mais ne nécessite pas de vérification d’identité, vous pouvez configurer le pilote pour qu’il utilise une fabrique SSL non validante.

Pour configurer une connexion SSL sans vérification d’identité

1. Définissez la propriété `UID` sur votre nom d’utilisateur Redshift pour accéder au serveur Amazon Redshift.
2. Définissez la propriété `PWD` avec le mot de passe correspondant à votre nom d’utilisateur Redshift.
3. Définition de la propriété `SSLFactory` à `com.amazon.redshift.ssl.NonValidatingFactory`.

Utilisation de l’authentification SSL unidirectionnelle

Si le serveur auquel vous vous connectez utilise SSL et dispose d’un certificat, vous pouvez configurer le pilote pour vérifier l’identité du serveur à l’aide de l’authentification unidirectionnelle.

One-way l'authentification nécessite un certificat SSL approuvé signé pour vérifier l'identité du serveur. Vous pouvez configurer le pilote pour utiliser un certificat spécifique ou accéder à un certificat TrustStore contenant le certificat approprié. Si vous ne spécifiez pas de certificat ou TrustStore, le pilote utilise le langage Java par défaut TrustStore (généralement l'un `jssecacerts` ou l'autre`cacerts`).

Pour configurer l’authentification SSL unidirectionnelle

1. Définissez la propriété UID sur votre nom d’utilisateur Redshift pour accéder au serveur Amazon Redshift.

2. Définissez la propriété PWD avec le mot de passe correspondant à votre nom d'utilisateur Redshift.
3. Définissez la propriété SSL sur true (vrai).
4. Définissez la SSLRootCert propriété sur l'emplacement de votre certificat CA racine.
5. Si vous n'utilisez pas l'une des versions Java par défaut TrustStores, effectuez l'une des opérations suivantes :
   - Pour spécifier un certificat de serveur, définissez la SSLRootCert propriété sur le chemin complet du certificat.
   - Pour spécifier un TrustStore, procédez comme suit :
     a. Utilisez le programme keytool pour ajouter le certificat de serveur à celui TrustStore que vous souhaitez utiliser.
     b. Spécifiez le mot de passe TrustStore et à utiliser lors du démarrage de l'application Java à l'aide du pilote. Par exemple :

```
-Djavax.net.ssl.trustStore=[TrustStoreName]
-Djavax.net.ssl.trustStorePassword=[TrustStorePassword]
-Djavax.net.ssl.trustStoreType=[TrustStoreType]
```

6. Choisissez-en une :
   - Pour valider le certificat, définissez la propriété SSLMode sur verify-ca.
   - Pour valider le certificat et vérifier le nom d'hôte dans le certificat, définissez la propriété SSLMode sur verify-full.

Configuration de la journalisation

Vous pouvez activer la journalisation dans le pilote pour aider à diagnostiquer les problèmes.

Vous pouvez consigner les informations relatives au pilote en utilisant les méthodes suivantes :

- Pour enregistrer les informations consignées dans des fichiers .log, consultezUtilisation des fichiers journaux.
- Pour envoyer les informations enregistrées au LogStream ou LogWriter spécifiées dans le DriverManager, voirEn utilisant LogStream ou LogWriter.

Vous fournissez les informations de configuration au pilote dans l'URL de connexion. Pour plus d'informations sur la syntaxe de l'URL de connexion, consultez Création de l'URL de connexion.

Utilisation des fichiers journaux

N'activez la journalisation que le temps de capturer un problème. La journalisation diminue performances et peut consommer une grande quantité d'espace disque.

Définissez la LogLevel clé dans votre URL de connexion pour activer la journalisation et spécifiez la quantité de détails inclus dans les fichiers journaux. Le tableau suivant répertorie les niveaux de journalisation fournis par le pilote JDBC Amazon Redshift version 2.x, dans l'ordre du moins verbeux au plus verbeux.

LogLevel valeur	Description
1	Journalisation des événements d'erreurs graves qui conduiront le pilote à l'abandon.
2	Journalisation des événements d'erreur qui pourraient permettre au pilote de continuer à fonctionner.
3	Journalisation des événements qui peuvent entraîner une erreur si aucune action n'est entreprise. Ce niveau de journalisation et les niveaux de journalisation supérieurs à ce niveau enregistrent également les requêtes de l'utilisateur.
4	Journalisation d'informations générales qui décrivent la progression du pilote.
5	Journalisation d'informations détaillées qui sont utiles pour le débogage du pilote.
6	Journalisation de toutes les activités du pilote.

Pour configurer la journalisation qui utilise des fichiers journaux

1. Définissez la LogLevel propriété sur le niveau d'informations souhaité à inclure dans les fichiers journaux.
2. Définissez la LogPath propriété sur le chemin complet du dossier dans lequel vous souhaitez enregistrer les fichiers journaux.

   Par exemple, l'URL de connexion suivante active le niveau 3 de journalisation et enregistre les fichiers journaux dans le dossier C:\temp : `jdbc:redshift://redshift.company.us-west- 1.redshift.amazonaws.com:9000/Default;DSILogLevel=3;LogPath=C:\temp`
3. Pour vous assurer que les nouveaux paramètres prennent effet, redémarrez votre application JDBC et reconnectez-vous au serveur.

   Le pilote Amazon Redshift JDBC produit les fichiers journaux suivants à l'emplacement spécifié dans la propriété : LogPath

   - redshift_jdbc.log qui enregistre l'activité du pilote qui n'est pas spécifique à une connexion.
   - redshift_jdbc_connection_[Number].log pour chaque connexion établie à la base de données, où [Number] est un numéro qui identifie chaque fichier journal. Ce fichier enregistre l'activité du pilote spécifique à la connexion.

Si la LogPath valeur n'est pas valide, le pilote envoie les informations enregistrées au flux de sortie standard (`System.out`)

En utilisant LogStream ou LogWriter

N'activez la journalisation que le temps de capturer un problème. La journalisation diminue performances et peut consommer une grande quantité d'espace disque.

Définissez la LogLevel clé dans votre URL de connexion pour activer la journalisation et spécifiez la quantité de détails envoyés au LogStream ou LogWriter spécifiée dans le DriverManager.

Pour activer la journalisation qui utilise le LogStream ou LogWriter :

1. Pour configurer le pilote afin de consigner des informations générales décrivant la progression du pilote, définissez la LogLevel propriété sur 1 ou INFO.
2. Pour vous assurer que les nouveaux paramètres prennent effet, redémarrez votre application JDBC et reconnectez-vous au serveur.

Conversions du type de données

Le pilote Amazon Redshift JDBC version 2.x prend en charge de nombreux formats de données courants, la conversion entre les types de données Amazon Redshift, SQL et Java.

Le tableau suivant répertorie les mappages de types de données pris en charge.

Type Amazon Redshift	Type SQL	Type Java
BIGINT	SQL_BIGINT	Long
BOOLEAN	SQL_BIT	Booléen
CHAR	SQL_CHAR	Chaîne
DATE	SQL_TYPE_DATE	java.sql.Date
DECIMAL	SQL_NUMERIC	BigDecimal
DOUBLE PRECISION	SQL_DOUBLE	Double
GEOMETRY	SQL_ LONGVARBINARY	byte[]
INTEGER	SQL_INTEGER	Entier
OID	SQL_BIGINT	Long
SUPER	SQL_LONGVARCHAR	Chaîne
REAL	SQL_REAL	Float
SMALLINT	SQL_SMALLINT	Court
TEXT	SQL_VARCHAR	Chaîne
TIME	SQL_TYPE_TIME	java.sql.Time
TIMETZ	SQL_TYPE_TIME	java.sql.Time
TIMESTAMP	SQL_TYPE_ TIMESTAMP	java.sql.Timestamp
TIMESTAMPTZ	SQL_TYPE_ TIMESTAMP	java.sql.Timestamp

Type Amazon Redshift	Type SQL	Type Java
VARCHAR	SQL_VARCHAR	Chaîne

Utilisation du support d’instructions préparées

Le pilote JDBC Amazon Redshift prend en charge les instructions préparées. Vous pouvez utiliser des instructions préparées pour améliorer les performances des requêtes paramétrées qui doivent être exécutées plusieurs fois au cours de la même connexion.

Une instruction préparée est une instruction SQL compilée côté serveur, mais pas exécutée immédiatement. La déclaration compilée est stockée sur le serveur sous forme d' PreparedStatement objet jusqu'à ce que vous fermiez l'objet ou la connexion. Tant que cet objet existe, vous pouvez exécuter l’instruction préparée autant de fois que nécessaire en utilisant différentes valeurs de paramètre, sans avoir à compiler à nouveau l’instruction. Ce surcoût réduit permet à l’ensemble de requêtes d’être exécuté plus rapidement.

Pour plus d’informations sur les instructions préparées, consultez « Utilisation des instructions préparées » dans le didacticiel JDBC Basics d’Oracle.

Vous pouvez préparer une instruction contenant plusieurs requêtes. Par exemple, l’instruction préparée suivante contient deux requêtes INSERT :

```
PreparedStatement pstmt = conn.prepareStatement("INSERT INTO
MyTable VALUES (1, 'abc'); INSERT INTO CompanyTable VALUES
(1, 'abc');");
```

Veillez à ce que ces requêtes ne dépendent pas des résultats d’autres requêtes spécifiées dans la même instruction préparée. Étant donné que les requêtes ne s’exécutent pas pendant l’étape de préparation, les résultats n’ont pas encore été renvoyés et ne sont pas disponibles pour d’autres requêtes dans la même instruction préparée.

Par exemple, l’instruction préparée suivante, qui crée une table puis insère des valeurs dans cette table qui vient d’être créée, n’est pas autorisée :

```
PreparedStatement pstmt = conn.prepareStatement("CREATE
TABLE MyTable(col1 int, col2 varchar); INSERT INTO myTable
VALUES (1, 'abc');");
```

Si vous essayez de préparer cette instruction, le serveur renvoie une erreur indiquant que la table de destination (myTable) n'existe pas encore. La requête CREATE doit être exécutée avant que la requête INSERT puisse être préparée.

Différences entre les versions 2.x et 1.x du pilote JDBC

Cette section décrit les différences dans les informations renvoyées par les versions 2.x et 1.x du pilote JDBC. Le pilote JDBC version 1.x est interrompu.

Le tableau suivant répertorie les DatabaseMetadata informations renvoyées par les fonctions get DatabaseProductName () et get DatabaseProductVersion () pour chaque version du pilote JDBC. Le pilote JDBC version 2.x obtient les valeurs lorsque la connexion est établie. Le pilote JDBC version 1.x obtient les valeurs à la suite d'une requête.

Version du pilote JDBC	résultat get DatabaseProductName ()	résultat get DatabaseProductVersion ()
2.x	Redshift	8,0.2
1.x	PostgreSQL	08,00.0002

Le tableau suivant répertorie les DatabaseMetadata informations renvoyées par la TypeInfo fonction get pour chaque version du pilote JDBC.

Version du pilote JDBC	obtenir le TypeInfo résultat
2.x	Compatible avec les types de données Redshift
1.x	Compatible avec les types de données PostgreSQL

Création de fichiers d'initialisation (.ini) pour le pilote JDBC version 2.x

En utilisant des fichiers d'initialisation (.ini) pour le pilote JDBC Amazon Redshift version 2.x, vous pouvez spécifier des paramètres de configuration au niveau du système. Par exemple, les paramètres d'authentification de fournisseur d'identité fédéré peuvent varier pour chaque application. Le fichier .ini fournit un emplacement commun aux clients SQL pour obtenir les paramètres de configuration requis.

Vous pouvez créer un fichier d'initialisation (.ini) du pilote JDBC version 2.x qui contient des options de configuration pour les clients SQL. Le nom par défaut du fichier est `rsjdbc.ini`. Le pilote JDBC version 2.x recherche le fichier .ini aux emplacements suivants, répertoriés par ordre de priorité :

- Le paramètre `IniFile` dans l'URL de connexion ou dans la boîte de dialogue des propriétés de connexion du client SQL. Assurez-vous que le paramètre `IniFile` contient le chemin d'accès complet au fichier .ini, y compris le nom du fichier. Pour plus d'informations sur le paramètre `IniFile`, consultez IniFile. Si le paramètre `IniFile` spécifie de manière incorrecte l'emplacement du fichier .ini, une erreur s'affiche.
- Variables d'environnement telles que AMAZON_REDSHIFT_JDBC_INI_FILE avec le chemin complet, y compris le nom du fichier. Vous pouvez utiliser `rsjdbc.ini` ou spécifier un nom de fichier. Si la variable d'environnement AMAZON_REDSHIFT_JDBC_INI_FILE spécifie de manière incorrecte l'emplacement du fichier .ini, une erreur s'affiche.
- Répertoire dans lequel se trouve le fichier JAR du pilote.
- Répertoire de base de l'utilisateur.
- Répertoire temporaire du système.

Vous pouvez organiser le fichier .ini en sections, par exemple, [DRIVER]. Chaque section contient des paires clé-valeur qui spécifient divers paramètres de connexion. Vous pouvez utiliser le paramètre `IniSection` pour spécifier une section dans le fichier .ini. Pour plus d'informations sur le paramètre `IniSection`, consultez IniSection.

Voici un exemple de format de fichier .ini, avec des sections pour [DRIVER], [DEV], [QA] et [PROD]. La section [DRIVER] peut s'appliquer à n'importe quelle connexion.

```
[DRIVER]
key1=val1
key2=val2

[DEV]
key1=val1
key2=val2

[QA]
key1=val1
key2=val2

[PROD]
```

```
key1=val1
key2=val2
```

Le pilote JDBC version 2.x charge les paramètres de configuration à partir des emplacements suivants, répertoriés par ordre de priorité :

- Paramètres de configuration par défaut dans le code de l'application.
- Propriétés de la section [DRIVER] du fichier .ini, si inclus.
- Paramètres de configuration de la section personnalisée, si l'option `IniSection` est fournie dans l'URL de connexion ou dans la boîte de dialogue des propriétés de connexion du client SQL.
- Propriétés de l'objet de propriété de connexion spécifié dans l'appel `getConnection`.
- Paramètres de configuration spécifiés dans l'URL de connexion.

Options de configuration du pilote JDBC version 2.x

Vous trouverez ci-dessous des descriptions des options que vous pouvez spécifier pour la version 2.x du pilote Amazon Redshift JDBC. Les options de configuration ne sont pas sensibles à la casse.

Vous pouvez définir les propriétés de configuration à l'aide de l'URL de connexion. Pour plus d'informations, consultez Création de l'URL de connexion.

Rubriques

- AccessKeyID
- AllowDBUserOverride
- App_ID
- App_Name
- ApplicationName
- AuthProfile
- AutoCreate
- Client_ID
- Client_Secret
- ClusterID
- Compression
- connectTimeout

- connectionTimezone
- base de données MetadataCurrentDbOnly
- DbUser
- DbGroups
- DBNAME
- par défaut RowFetchSize
- DisableIsValidQuery
- activer FetchRingBuffer
- activer MultiSqlSupport
- EnableTableTypes
- aller chercher RingBufferSize
- ForceLowercase
- groupFederation
- HOST
- IAMDisableCache
- IAMDuration
- Idc_Client_Display_Name
- Idc_Region
- IdP_Host
- IdP_Partition
- IdP_Port
- IdP_Tenant
- IdP_ Response_Timeout
- IniFile
- IniSection
- isServerless
- Issuer_Url
- Listen_Port
- Login_URL

- loginTimeout
- se connecter ToRp
- LogLevel
- LogPath
- OverrideSchemaPatternType
- Partner_SPID
- Mot de passe
- Plugin_Name
- PORT
- Préférez PQ
- Preferred_Role
- Profil
- PWD
- queryGroup
- readOnly
- Région
- re WriteBatchedInserts
- re WriteBatchedInsertsSize
- roleArn
- rôle SessionName
- scope
- SecretAccessKey
- SessionToken
- sans serveur AcctId
- sans serveur WorkGroup
- socketFactory
- socketTimeout
- SSL
- SSL_Insecure

- SSLCert
- SSLFactory
- SSLKey
- SSLMode
- SSLPassword
- SSLRootCert
- StsEndpointUrl
- tcp KeepAlive
- jeton
- token_type
- UID
- Utilisateur
- web IdentityToken

AccessKeyID

- Valeur par défaut – Aucune
- Types de données – Chaîne

Vous pouvez spécifier ce paramètre pour entrer la clé d'accès IAM pour l'utilisateur ou le rôle. Vous pouvez généralement localiser la clé en consultant une chaîne ou un profil utilisateur existant. Si vous spécifiez ce paramètre, vous devez également spécifier le paramètre `SecretAccessKey`. S'il est transmis dans l'URL JDBC, l' AccessKeyID doit être codé en URL.

Ce paramètre est facultatif.

AllowDBUserOverride

- Valeur par défaut : 0
- Types de données – Chaîne

Cette option spécifie si le pilote utilise la valeur de l'assertion SAML ou la valeur `DbUser` spécifiée dans la propriété de connexion `DbUser` dans l'URL de connexion.

Ce paramètre est facultatif.

1

Le pilote utilise la valeur `DbUser` de l'assertion SAML.

Si l'assertion SAML ne spécifie pas de valeur pour `DBUser`, le pilote utilise la valeur spécifiée dans la propriété de connexion `DBUser`. Si la propriété de connexion ne spécifie pas non plus de valeur, le pilote utilise la valeur spécifiée dans le profil de connexion.

0

Le pilote utilise la valeur `DBUser` spécifiée dans la propriété de connexion `DBUser`.

Si la propriété de connexion `DBUser` ne spécifie pas de valeur, le pilote utilise la valeur spécifiée dans le profil de connexion. Si le profil de connexion ne spécifie pas non plus de valeur, le pilote utilise la valeur de l'assertion SAML.

App_ID

- Valeur par défaut – Aucune
- Types de données – Chaîne

L'identifiant Okta-provided unique associé à votre application Amazon Redshift.

Ce paramètre est obligatoire si vous vous authentifiez via le service Okta.

App_Name

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le nom de l'application Okta que vous utilisez pour authentifier la connexion à Amazon Redshift.

Ce paramètre est facultatif.

ApplicationName

- Valeur par défaut – null

- Types de données – Chaîne

Nom de l'application à transmettre à Amazon Redshift à des fins d'audit.

Ce paramètre est facultatif.

AuthProfile

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le nom du profil d'authentification à utiliser pour la connexion à Amazon Redshift.

Ce paramètre est facultatif.

AutoCreate

- Valeur par défaut — false
- Types de données – Booléen

Cette option spécifie si le pilote provoque la création d'un nouvel utilisateur lorsque l'utilisateur spécifié n'existe pas.

Ce paramètre est facultatif.

true

Si l'utilisateur spécifié par `DBUser` ou l'ID unique (UID) n'existe pas, un nouvel utilisateur portant ce nom est créé.

false

Le pilote ne crée pas de nouveaux utilisateurs. Si l'utilisateur spécifié n'existe pas, l'authentification échoue.

Client_ID

- Valeur par défaut – Aucune
- Types de données – Chaîne

L'ID client à utiliser lors de l'authentification de la connexion à l'aide du service Azure AD.

Ce paramètre est obligatoire si vous vous authentifiez via le service Azure AD.

Client_Secret

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le secret client à utiliser lors de l'authentification de la connexion à l'aide du service Azure AD.

Ce paramètre est obligatoire si vous vous authentifiez via le service Azure AD.

ClusterID

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le nom du cluster Amazon Redshift auquel vous souhaitez vous connecter. Le pilote tente de détecter ce paramètre à partir de l'hôte donné. Si vous utilisez un Network Load Balancer (NLB) et que vous vous connectez via IAM, le pilote ne le détectera pas. Vous pouvez donc le définir à l'aide de cette option de connexion.

Ce paramètre est facultatif.

Compression

- Valeur par défaut : désactivé
- Types de données – Chaîne

Méthode de compression utilisée pour les communications par protocole filaire entre le serveur Amazon Redshift et le client ou le pilote.

Ce paramètre est facultatif.

Vous pouvez spécifier les valeurs suivantes :

- lz4

Définit la méthode de compression utilisée pour les communications par protocole filaire avec Amazon Redshift sur lz4.

- off

N’utilise pas la compression pour les communications par protocole filaire avec Amazon Redshift.

connectTimeout

- Valeur par défaut – 10
- Type de données – Entier

Valeur de délai d’expiration à utiliser pour les opérations de connexion de socket. Si le temps nécessaire à l’établissement d’une connexion Amazon Redshift dépasse cette valeur, la connexion est considérée comme non disponible. Le délai d’expiration est spécifié en secondes. Une valeur de 0 signifie qu’aucun délai d’expiration n’est spécifié.

Ce paramètre est facultatif.

connectionTimezone

- Valeur par défaut : LOCAL
- Types de données – Chaîne

Fuseau horaire au niveau de la session.

Ce paramètre est facultatif.

Vous pouvez spécifier les valeurs suivantes :

LOCAL

Configure le fuseau horaire au niveau de la session sur le fuseau horaire de la JVM LOCAL.

SERVER

Configure le fuseau horaire au niveau de la session sur le fuseau horaire défini pour l’utilisateur sur le serveur Amazon Redshift. Vous pouvez configurer les fuseaux horaires au niveau de la session pour les utilisateurs à l’aide de la commande suivante :

```
ALTER USER
[...]
SET TIMEZONE TO [...];
```

base de données MetadataCurrentDbOnly

- Valeur par défaut – true
- Types de données – Booléen

Cette option spécifie si l'API de métadonnées récupère les données de toutes les bases de données accessibles ou uniquement de la base de données connectée.

Ce paramètre est facultatif.

Vous pouvez spécifier les valeurs suivantes :

true

L'application récupère les métadonnées d'une seule base de données.

false

L'application récupère les métadonnées de toutes les bases de données accessibles.

DbUser

- Valeur par défaut – Aucune
- Types de données – Chaîne

L'ID utilisateur à utiliser avec votre compte Amazon Redshift. Vous pouvez utiliser un identifiant qui n'existe pas actuellement si vous avez activé la AutoCreate propriété.

Ce paramètre est facultatif.

DbGroups

- Valeur par défaut – PUBLIC
- Types de données – Chaîne

Une liste séparée par des virgules des noms de groupes de bases de données existants auxquels `DBUser` se joint pour la séance en cours.

Ce paramètre est facultatif.

DBNAME

- Valeur par défaut – null
- Types de données – Chaîne

Le nom de la base de données à laquelle se connecter. Vous pouvez utiliser cette option pour spécifier le nom de la base de données dans l'URL de connexion JDBC.

Ce paramètre est obligatoire. Vous devez spécifier le nom de la base de données, soit dans l'URL de connexion, soit dans les propriétés de connexion de l'application cliente.

par défaut RowFetchSize

- Valeur par défaut : 0
- Type de données – Entier

Cette option spécifie une valeur par défaut pour getFetchSize.

Ce paramètre est facultatif.

Vous pouvez spécifier les valeurs suivantes :

0

Récupérez toutes les lignes en une seule opération.

Nombre entier positif

Nombre de lignes à extraire de la base de données pour chaque itération de récupération du. ResultSet

DisableIsValidQuery

- Valeur par défaut – False

- Types de données – Booléen

Cette option indique si le pilote envoie une nouvelle requête de base de données lorsqu'il utilise la méthode Connection.isValid () pour déterminer si la connexion à la base de données est active.

Ce paramètre est facultatif.

true

Le pilote ne soumet pas de requête lorsqu'il utilise Connection.isValid () pour déterminer si la connexion à la base de données est active. Cela peut amener le pilote à identifier de manière incorrecte la connexion à la base de données comme étant active si le serveur de base de données s'est arrêté de manière inattendue.

false

Le pilote envoie une requête lorsqu'il utilise Connection.isValid () pour déterminer si la connexion à la base de données est active.

activer FetchRingBuffer

- Valeur par défaut – true
- Types de données – Booléen

Cette option spécifie que le pilote récupère les lignes à l'aide d'un tampon en anneau sur un thread séparé. Le RingBufferSize paramètre fetch spécifie la taille de la mémoire tampon en anneau.

La mémoire tampon en anneau implémente la gestion automatique de la mémoire dans JDBC afin d'éviter les erreurs de mémoire insuffisante (OOM) lors des opérations de récupération de données. La mémoire tampon surveille la taille réelle des données mises en mémoire tampon en temps réel, garantissant ainsi que l'utilisation totale de la mémoire par le pilote reste dans les limites définies. Lorsque la capacité de la mémoire tampon est atteinte, le pilote interrompt les opérations de récupération des données, empêchant ainsi le débordement de mémoire sans intervention manuelle. Cette protection intégrée élimine automatiquement les erreurs OOM, sans qu'aucune configuration ne soit requise de la part des utilisateurs.

Si une transaction détecte une instruction contenant plusieurs commandes SQL séparées par des points-virgules, la mémoire tampon de l'anneau de récupération pour cette transaction est définie sur false. La valeur de enable ne change pas. FetchRingBuffer

Ce paramètre est facultatif.

> **Note**
>
> Lorsque la mémoire tampon est désactivée et que la taille de lecture n'est pas correctement configurée, des problèmes de mémoire insuffisante (OOM) peuvent survenir. Pour plus d'informations sur la configuration de la taille de lecture, cliquez ici.

activer MultiSqlSupport

- Valeur par défaut – true
- Types de données – Booléen

Cette option spécifie s'il faut traiter plusieurs commandes SQL séparées par des points-virgules dans une instruction.

Ce paramètre est facultatif.

Vous pouvez spécifier les valeurs suivantes :

true

Le pilote traite plusieurs commandes SQL, séparées par des points-virgules, dans un objet Statement.

false

Le pilote renvoie une erreur pour plusieurs commandes SQL dans une seule instruction.

EnableTableTypes

- Valeur par défaut – true
- Types de données – Booléen

Cette option indique si le pilote reconnaît les informations détaillées sur le type de table provenant de la source de données dans les résultats des `getTableTypes` `DatabaseMetaData` méthodes `getTables` et. Par défaut, le pilote reconnaît les types de tables détaillés.

Ce paramètre est facultatif. Il est disponible dans les versions 2.2.8 et ultérieures du pilote.

true

Le pilote reconnaît les types de tables suivants : TABLE, VIEW, SYSTEM TABLE, SYSTEM VIEW, EXTERNAL TABLE et LOCAL TEMPORARY.

false

Le pilote normalise les informations détaillées sur les types de table dans les types de table génériques TABLE et VIEW.

aller chercher RingBufferSize

- Valeur par défaut – 1G
- Types de données – Chaîne

Cette option spécifie la taille de la mémoire tampon en anneau utilisée lors de la récupération du jeu de résultats. Vous pouvez spécifier une taille en octets, par exemple 1K pour 1 Ko, 5000 pour 5 000 octets, 1M pour 1 Mo, 1G pour 1 Go, etc. Vous pouvez également spécifier un pourcentage de mémoire de segment. Le pilote arrête de récupérer les lignes lorsqu'il atteint la limite. L'extraction reprend lorsque l'application lit les lignes et libère de l'espace dans la mémoire tampon en anneau.

Ce paramètre est facultatif.

ForceLowercase

- Valeur par défaut — false
- Types de données – Booléen

Cette option indique si le pilote met en minuscules tous les groupes de bases de données (DbGroups) envoyés par le fournisseur d'identité à Amazon Redshift lors de l'utilisation de l'authentification unique.

Ce paramètre est facultatif.

true

Le pilote met en minuscules tous les groupes de bases de données envoyés par le fournisseur d'identité.

false

Le pilote ne modifie pas les groupes de bases de données.

groupFederation

- Valeur par défaut — false
- Types de données – Booléen

Cette option spécifie si les groupes d'IDP Amazon Redshift doivent être utilisés. Ceci est pris en charge par l' GetClusterCredentialsV2 API.

Ce paramètre est facultatif.

true

Utilisez les groupes Amazon Redshift Identity Provider (IDP).

false

Utilisez l'API STS et GetClusterCredentials pour la fédération d'utilisateurs et spécifiez DbGroups explicitement la connexion.

HOST

- Valeur par défaut – null
- Types de données – Chaîne

Le nom d'hôte du serveur Amazon Redshift auquel se connecter. Vous pouvez utiliser cette option pour spécifier le nom d'hôte dans l'URL de connexion JDBC.

Ce paramètre est obligatoire. Vous devez spécifier le nom d'hôte, soit dans l'URL de connexion, soit dans les propriétés de connexion de l'application cliente.

IAMDisableCache

- Valeur par défaut — false
- Types de données – Booléen

Cette option spécifie si les informations d’identification IAM sont mises en cache.

Ce paramètre est facultatif.

true

Les informations d’identification IAM ne sont pas mises en cache.

false

Les informations d’identification IAM sont mises en cache. Cela améliore les performances lorsque les demandes envoyées à API Gateway sont limitées, par exemple.

IAMDuration

- Valeur par défaut – 900
- Type de données – Entier

La durée, en secondes, jusqu’au moment de l’expiration des informations d’identification IAM temporaires.

- Valeur minimale – 900
- Valeur maximale – 3 600

Ce paramètre est facultatif.

Idc_Client_Display_Name

- Valeur par défaut : pilote JDBC Amazon Redshift
- Types de données – Chaîne

Le nom d'affichage à utiliser pour le client qui l'utilise BrowserIdcAuthPlugin.

Ce paramètre est facultatif.

Idc_Region

- Valeur par défaut – Aucune
- Types de données – Chaîne

AWS Région dans laquelle se trouve l'instance IAM Identity Center.

Ce paramètre est requis uniquement lors de l’authentification à l’aide de `BrowserIdcAuthPlugin` dans l’option de configuration plugin_name.

IdP_Host

- Valeur par défaut – Aucune
- Types de données – Chaîne

L’hôte IdP (fournisseur d’identité) que vous utilisez pour vous authentifier dans Amazon Redshift. Cela peut être spécifié dans la chaîne de connexion ou dans un profil.

Ce paramètre est facultatif.

IdP_Partition

- Valeur par défaut – Aucune
- Types de données – Chaîne

Spécifie la partition cloud sur laquelle votre fournisseur d'identité (IdP) est configuré. Cela détermine le point de terminaison d'authentification IdP auquel le pilote se connecte.

Si ce paramètre est laissé vide, le pilote utilise par défaut la partition commerciale. Les valeurs possibles sont :

- `us-gov`: utilisez cette valeur si votre IdP est configuré dans Azure Government. Par exemple, Azure AD Government utilise le point de terminaison`login.microsoftonline.us`.
- `cn`: Utilisez cette valeur si votre IdP est configuré dans la partition cloud de Chine. Par exemple, Azure AD Chine utilise le point de terminaison`login.chinacloudapi.cn`.

Ce paramètre est facultatif.

IdP_Port

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le port utilisé par un IdP (fournisseur d'identité). Vous pouvez spécifier le port soit dans la chaîne de connexion, soit dans un profil. La valeur par défaut du port est 5439. En fonction du port que vous avez sélectionné lors de la création, de la modification ou de la migration du cluster, autorisez l'accès au port sélectionné.

Ce paramètre est facultatif.

IdP_Tenant

- Valeur par défaut – Aucune
- Types de données – Chaîne

ID de locataire Azure AD pour votre application Amazon Redshift.

Ce paramètre est obligatoire si vous vous authentifiez via le service Azure AD.

IdP_ Response_Timeout

- Valeur par défaut – 120
- Type de données – Entier

La durée, en secondes, pendant laquelle le pilote attend la réponse SAML du fournisseur d'identité lors de l'utilisation des services SAML ou Azure AD via un plugin de navigateur.

Ce paramètre est facultatif.

IniFile

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le chemin complet du fichier .ini, y compris le nom du fichier. Par exemple :

```
IniFile="C:\tools\rsjdbc.ini"
```

Pour plus d'informations concernant le fichier .ini, consultez Création de fichiers d'initialisation (.ini) pour le pilote JDBC version 2.x.

Ce paramètre est facultatif.

IniSection

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le nom d'une section du fichier .ini contenant les options de configuration. Pour plus d'informations concernant le fichier .ini, consultez Création de fichiers d'initialisation (.ini) pour le pilote JDBC version 2.x.

L'exemple suivant spécifie la section [Prod] du fichier .ini :

```
IniSection="Prod"
```

Ce paramètre est facultatif.

isServerless

- Valeur par défaut — false
- Types de données – Booléen

Cette option indique si l'hôte du point de terminaison Amazon Redshift est une instance sans serveur. Le pilote tente de détecter ce paramètre à partir de l'hôte donné. Si vous utilisez un Network Load Balancer (NLB), le pilote ne le détectera pas. Vous pouvez donc le définir ici.

Ce paramètre est facultatif.

true

L'hôte du point de terminaison Amazon Redshift est une instance sans serveur.

false

L'hôte du point de terminaison Amazon Redshift est un cluster provisionné.

Issuer_Url

- Valeur par défaut – Aucune
- Types de données – Chaîne

Pointe vers le point de terminaison de l'instance du serveur AWS IAM Identity Center.

Ce paramètre est requis uniquement lors de l’authentification à l’aide de `BrowserIdcAuthPlugin` dans l’option de configuration plugin_name.

Listen_Port

- Valeur par défaut : 7890
- Type de données – Entier

Port utilisé par le pilote pour recevoir la réponse SAML du fournisseur d'identité ou le code d'autorisation lors de l'utilisation des services SAML, Azure AD ou AWS Identity Center via un plug-in de navigateur.

Ce paramètre est facultatif.

Login_URL

- Valeur par défaut – Aucune
- Types de données – Chaîne

L’URL de la ressource sur le site Web du fournisseur d’identité lors de l’utilisation des services SAML ou Azure AD via un plugin de navigateur.

Ce paramètre est requis si vous vous authentifiez avec les services SAML ou Azure AD via un plugin de navigateur.

loginTimeout

- Valeur par défaut : 0
- Type de données – Entier

Le nombre de secondes à attendre avant d’interrompre la connexion et l’authentification au serveur. Si l’établissement de la connexion dépasse ce seuil, la connexion est abandonnée.

Lorsque cette propriété est définie sur 0, les connexions ne sont pas interrompues.

Ce paramètre est facultatif.

se connecter ToRp

- Valeur par défaut : `urn:amazon:webservices`
- Types de données – Chaîne

L'approbation des parties utilisatrices que vous souhaitez utiliser pour le type d'authentification AD FS.

Ce paramètre est facultatif.

LogLevel

- Valeur par défaut : 0
- Type de données – Entier

Utilisez cette propriété pour activer ou désactiver la journalisation dans le pilote et pour spécifier la quantité de détails inclus dans les fichiers journaux.

Activez la journalisation juste assez longtemps pour capturer un problème. La journalisation diminue performances et peut consommer une grande quantité d'espace disque.

Ce paramètre est facultatif.

Définissez le paramètre sur l'une des valeurs suivantes :

0

Désactiver toute la journalisation.

1

Activez la journalisation au niveau FATAL, qui enregistre les événements d'erreur très graves qui conduiront le pilote à abandonner les opérations.

2

Activez la journalisation au niveau ERROR, qui consigne les événements d'erreur qui peuvent tout de même permettre au pilote de poursuivre son exécution.

3

Activez la journalisation au niveau WARNING, qui consigne les événements susceptibles d'entraîner une erreur si aucune action n'est entreprise.

4

Activez la journalisation au niveau INFO, qui consigne les informations générales décrivant la progression du pilote.

5

Activez la journalisation au niveau DEBUG, qui enregistre des informations détaillées utiles pour le débogage du pilote.

6

Activez la journalisation au niveau TRACE, qui enregistre toute l'activité du pilote.

Lorsque la journalisation est activée, le pilote produit les fichiers journaux suivants à l'emplacement spécifié dans la propriété `LogPath` :

- **`redshift_jdbc.log`** : fichier qui enregistre l'activité du pilote qui n'est pas spécifique à une connexion.
- **`redshift_jdbc_connection_[Number].log`** : – Fichier pour chaque connexion établie à la base de données, où`[Number]` est un numéro qui distingue chaque fichier journal des autres. Ce fichier enregistre l'activité du pilote spécifique à la connexion.

Si la LogPath valeur n'est pas valide, le pilote envoie les informations enregistrées au flux de sortie standard,`System.out`.

LogPath

- Valeur par défaut – Le répertoire de travail actuel.
- Types de données – Chaîne

Le chemin complet du dossier dans lequel le pilote enregistre les fichiers journaux lorsque la DSILogLevel propriété est activée.

Pour avoir la garantie que l'URL de connexion est compatible avec toutes les applications JDBC, nous vous recommandons de traiter les barres obliques inverses (\) dans le chemin d'accès de votre fichier en saisissant une autre barre oblique inverse.

Ce paramètre est facultatif.

OverrideSchemaPatternType

- Valeur par défaut – null
- Type de données – Entier

Cette option indique si le type de requête utilisé dans les appels getTables doit être remplacé.

0

Requête universelle sans schéma

1

Requête à schéma local

2

Requête à schéma externe

Ce paramètre est facultatif.

Partner_SPID

- Valeur par défaut – Aucune
- Types de données – Chaîne

La valeur SPID (ID du fournisseur de services) du partenaire à utiliser lors de l'authentification de la connexion à l'aide du PingFederate service.

Ce paramètre est facultatif.

Mot de passe

- Valeur par défaut – Aucune
- Types de données – Chaîne

Lors de la connexion à l’aide de l’authentification IAM via un fournisseur d’identité, il s’agit du mot de passe du serveur IDP_Host. Lors de l’utilisation de l’authentification standard, celle-ci peut être utilisée pour le mot de passe de la base de données Amazon Redshift au lieu de PWD.

Ce paramètre est facultatif.

Plugin_Name

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le nom de classe entièrement qualifié pour mettre en œuvre un plugin de fournisseur d'informations d'identification spécifique.

Ce paramètre est facultatif.

Les options de fournisseur suivantes sont prises en charge :

- **`AdfsCredentialsProvider`** – Active Directory Federation Service.
- **`AzureCredentialsProvider`** : service Microsoft Azure Active Directory (AD).
- **`BasicJwtCredentialsProvider`** : service de jetons web JSON (JWT).
- **`BasicSamlCredentialsProvider`** – informations d'identification SAML (Security Assertion Markup Language) que vous pouvez utiliser avec de nombreux fournisseurs de services SAML.
- **`BrowserAzureCredentialsProvider`** : service Microsoft Azure Active Directory (AD) du navigateur.
- **`BrowserAzureOAuth2CredentialsProvider`** : service Microsoft Azure Active Directory (AD) du navigateur pour l'authentification native.
- **`BrowserIdcAuthPlugin`**— Un plugin d'autorisation utilisant AWS IAM Identity Center.
- **`BrowserSamlCredentialsProvider`** : navigateur SAML pour les services SAML tels qu'Okta, Ping ou ADFS.
- **`IdpTokenAuthPlugin`**— Un plugin d'autorisation qui accepte un jeton AWS IAM Identity Center ou des jetons d'identité (JWT) OpenID Connect (JSON-based OIDC) provenant de n'importe quel fournisseur d'identité Web AWS lié à IAM Identity Center.
- **`OktaCredentialsProvider`** : service Okta.
- **`PingCredentialsProvider`**— PingFederate Un service.

PORT

- Valeur par défaut – null
- Type de données – Entier

Le port du serveur Amazon Redshift auquel se connecter. Vous pouvez utiliser cette option pour spécifier le port dans l'URL de connexion JDBC.

Ce paramètre est facultatif.

Préférez PQ

- Valeur par défaut – true
- Types de données – Booléen

Cette option contrôle si le pilote annonce des groupes d'échange de clés hybrides post-quantiques dans le TLS 1.3. ClientHello Lorsque des groupes post-quantiques sont proposés et que le serveur les prend également en charge, le serveur en sélectionne un. Sinon, la poignée de main revient à un échange de clés classique de manière transparente.

Ce paramètre est facultatif. Il est disponible dans les versions 2.2.8 et ultérieures du pilote.

true

Le pilote annonce les groupes d'échange de clés TLS hybrides post-quantiques lorsqu'ils sont pris en charge par le moteur d'exécution.

false

Le pilote ne fait pas de publicité pour les groupes post-quantiques. Utilisez ce paramètre si un boîtier intermédiaire réseau bloque les poignées de main TLS parce qu'il ne reconnaît pas les groupes d'échange de clés post-quantiques proposés par le pilote.

Preferred_Role

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le rôle IAM que vous souhaitez endosser lors de la connexion à Amazon Redshift.

Ce paramètre est facultatif.

Profil

- Valeur par défaut – Aucune

- Types de données – Chaîne

Le nom du profil à utiliser pour l'authentification IAM. Ce profil contient toutes les propriétés de connexion supplémentaires non spécifiées dans la chaîne de connexion.

Ce paramètre est facultatif.

PWD

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le mot de passe correspondant au nom d'utilisateur Amazon Redshift que vous avez fourni à l'aide de l'UID de propriété.

Ce paramètre est facultatif.

queryGroup

- Valeur par défaut – null
- Types de données – Chaîne

Cette option permet d'affecter une requête à une file d'attente au moment de l'exécution en assignant votre requête au groupe de requêtes approprié. Le groupe de requêtes est défini pour la séance. Toutes les requêtes qui s'exécutent sur la connexion appartiennent à ce groupe de requêtes.

Ce paramètre est facultatif.

readOnly

- Valeur par défaut — false
- Types de données – Booléen

Cette propriété spécifie si le pilote est en mode lecture seule.

Ce paramètre est facultatif.

true

La connexion est en mode lecture seule et ne peut pas écrire dans le magasin de données.

false

La connexion n’est pas en mode lecture seule et peut écrire dans le magasin de données.

Région

- Valeur par défaut – null
- Types de données – Chaîne

Cette option indique la AWS région dans laquelle se trouve le cluster. Si vous spécifiez l' StsEndPoint option, l'option Région est ignorée. L’opération de l’API `GetClusterCredentials` Redshift utilise également l’option Region.

Ce paramètre est facultatif.

re WriteBatchedInserts

- Valeur par défaut — false
- Types de données – Booléen

Cette option permet d’optimiser la réécriture et la combinaison des instructions INSERT compatibles en lots.

Ce paramètre est facultatif.

re WriteBatchedInsertsSize

- Valeur par défaut – 128
- Type de données – Entier

Cette option permet d’optimiser la réécriture et la combinaison des instructions INSERT compatibles en lots. Cette valeur doit augmenter de façon exponentielle par puissance 2.

Ce paramètre est facultatif.

roleArn

- Valeur par défaut – Aucune
- Types de données – Chaîne

Amazon Resource Name (ARN) du rôle. Assurez-vous de spécifier ce paramètre lorsque vous spécifiez BasicJwtCredentialsProvider l' Plugin_Name option. Spécifiez l'ARN au format suivant :

`arn:partition:service:region:account-id:resource-id`

Ce paramètre est obligatoire si vous spécifiez BasicJwtCredentialsProvider l' Plugin_Name option.

rôle SessionName

- Valeur par défaut : jwt_redshift_session
- Types de données – Chaîne

Un identifiant pour la séance de rôle assumé. En règle générale, vous transmettez le nom ou l'identifiant associé à l'utilisateur de votre application. Les informations d'identification de sécurité temporaires utilisées par votre application sont associées à cet utilisateur. Vous pouvez spécifier ce paramètre lorsque vous spécifiez BasicJwtCredentialsProvider l' Plugin_Name option.

Ce paramètre est facultatif.

scope

- Valeur par défaut – Aucune
- Types de données – Chaîne

Une liste des portées, séparées par des espaces, auxquels l'utilisateur peut consentir. Vous spécifiez ce paramètre afin que votre application Microsoft Azure puisse obtenir le consentement des API que vous souhaitez appeler. Vous pouvez spécifier ce paramètre lorsque vous spécifiez BrowserAzureOAuth2CredentialsProvider l' Plugin_Name option.

Ce paramètre est obligatoire pour le BrowserAzureOAuth2CredentialsProvider plug-in.

SecretAccessKey

- Valeur par défaut – Aucune
- Types de données – Chaîne

La clé d'accès IAM pour l'utilisateur ou le rôle. Si cela est spécifié, l' AccessKeyID doit également être spécifié. Si l'URL JDBC est transmise, elle SecretAccessKey doit être codée en URL.

Ce paramètre est facultatif.

SessionToken

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le jeton de séance IAM temporaire associé au rôle IAM que vous utilisez pour vous authentifier. S'il est transmis dans l'URL JDBC, le jeton de session IAM temporaire doit être encodé en URL.

Ce paramètre est facultatif.

sans serveur AcctId

- Valeur par défaut – null
- Types de données – Chaîne

ID du compte Amazon Redshift sans serveur. Le pilote tente de détecter ce paramètre à partir de l'hôte donné. Si vous utilisez un Network Load Balancer (NLB), le pilote ne le détectera pas. Vous pouvez donc le définir ici.

Ce paramètre est facultatif.

sans serveur WorkGroup

- Valeur par défaut – null
- Types de données – Chaîne

Nom du groupe de travail Amazon Redshift sans serveur. Le pilote tente de détecter ce paramètre à partir de l'hôte donné. Si vous utilisez un Network Load Balancer (NLB), le pilote ne le détectera pas. Vous pouvez donc le définir ici.

Ce paramètre est facultatif.

socketFactory

- Valeur par défaut – null
- Types de données – Chaîne

Cette option spécifie une fabrique de sockets pour la création de sockets.

Ce paramètre est facultatif.

socketTimeout

- Valeur par défaut : 0
- Type de données – Entier

Nombre de secondes à attendre pendant les opérations de lecture de socket avant expiration. Si l'opération prend plus de temps que ce seuil, alors la connexion est fermée. Lorsque cette propriété est définie sur 0, la connexion ne s'interrompt pas.

Ce paramètre est facultatif.

SSL

- Valeur par défaut – TRUE
- Types de données – Chaîne

Utilisez cette propriété pour activer ou désactiver SSL pour la connexion.

Ce paramètre est facultatif.

Vous pouvez spécifier les valeurs suivantes :

TRUE

Le pilote se connecte au serveur via SSL.

FALSE

Le pilote se connecte au serveur sans utiliser SSL. Cette option n'est pas prise en charge avec l'authentification IAM.

Vous pouvez également configurer la AuthMech propriété.

SSL_Insecure

- Valeur par défaut – true

- Types de données – Chaîne

Cette propriété indique si le certificat du serveur des hôtes IdP doit être vérifié.

Ce paramètre est facultatif.

Vous pouvez spécifier les valeurs suivantes :

true

Le pilote ne vérifie pas l'authenticité du certificat du serveur IdP.

false

Le pilote vérifie l'authenticité du certificat du serveur IdP.

SSLCert

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le chemin d'accès complet d'un fichier .pem ou .crt contenant des certificats d'autorité de certification approuvés supplémentaires pour vérifier l'instance de serveur Amazon Redshift lors de l'utilisation de SSL.

Ce paramètre est requis si SSLKey est spécifié.

SSLFactory

- Valeur par défaut – Aucune
- Types de données – Chaîne

La fabrique SSL à utiliser lors de la connexion au serveur TLS/SSL sans utiliser de certificat de serveur.

SSLKey

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le chemin d'accès complet du fichier .der contenant le fichier de clé PKCS8 pour vérifier les certificats spécifiés dans SSLCert.

Ce paramètre est requis si SSLCert est spécifié.

SSLMode

- Valeur par défaut : verify-ca
- Types de données – Chaîne

Utilisez cette propriété pour spécifier la manière dont le pilote valide les certificats lorsque cette option TLS/SSL est activée.

Ce paramètre est facultatif.

Vous pouvez spécifier les valeurs suivantes :

verify-ca

Le pilote vérifie que le certificat provient d'une autorité de certification approuvée.

verify-full

Le pilote vérifie que le certificat provient d'une autorité de certification approuvée et que le nom d'hôte dans le certificat correspond à celui spécifié dans l'URL de connexion.

> **Note**
>
> Nous vous recommandons d'utiliser `verify-full` des connexions SSL dans la mesure du possible.

SSLPassword

- Valeur par défaut : 0
- Types de données – Chaîne

Le mot de passe du fichier de clé crypté spécifié dans SSLKey.

Ce paramètre est obligatoire si SSLKey est spécifié et que le fichier de clé est chiffré.

SSLRootCert

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le chemin complet d'un fichier .pem ou .crt contenant le certificat d'autorité de certification racine (root CA certificate) pour vérifier l'instance Amazon Redshift Server lors de l'utilisation de SSL.

StsEndpointUrl

- Valeur par défaut – null
- Types de données – Chaîne

Vous pouvez spécifier un point de terminaison AWS Security Token Service (AWS STS). Si vous spécifiez cette option, l’option Region est ignorée. Vous pouvez uniquement spécifier un protocole sécurisé (HTTPS) pour ce point de terminaison.

tcp KeepAlive

- Valeur par défaut – TRUE
- Types de données – Chaîne

Utilisez cette propriété pour activer ou désactiver les keepalives TCP.

Ce paramètre est facultatif.

Vous pouvez spécifier les valeurs suivantes :

TRUE

Le pilote utilise les keepalives TCP pour empêcher les connexions de s’interrompre.

FALSE

Le pilote n’utilise pas les keepalives TCP.

jeton

- Valeur par défaut – Aucune
- Types de données – Chaîne

Un jeton d'accès fourni par AWS IAM Identity Center ou un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d'identité Web AWS lié à IAM Identity Center. Votre application doit générer ce jeton en authentifiant l'utilisateur de votre application auprès d' AWS IAM Identity Center ou d'un fournisseur d'identité lié à AWS IAM Identity Center.

Ce paramètre fonctionne avec `IdpTokenAuthPlugin`.

token_type

- Valeur par défaut – Aucune
- Types de données – Chaîne

Type de jeton utilisé dans `IdpTokenAuthPlugin`.

Vous pouvez spécifier les valeurs suivantes :

ACCESS_TOKEN

Entrez cette valeur si vous utilisez un jeton d'accès fourni par AWS IAM Identity Center.

EXT_JWT

Entrez cette valeur si vous utilisez un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d’identité Web intégré à AWS IAM Identity Center.

Ce paramètre fonctionne avec `IdpTokenAuthPlugin`.

UID

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le nom d’utilisateur de base de données que vous utilisez pour accéder à la base de données.

Ce paramètre est obligatoire.

Utilisateur

- Valeur par défaut – Aucune
- Types de données – Chaîne

Lors de la connexion à l'aide de l'authentification IAM via un IdP, il s'agit du nom d'utilisateur du serveur idp_host. Lors de l'utilisation de l'authentification standard, celui-ci peut être utilisé comme nom d'utilisateur de la base de données Amazon Redshift.

Ce paramètre est facultatif.

web IdentityToken

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le jeton d'accès OAuth 2.1 ou le jeton d'identification OpenID Connect qui est fourni par le fournisseur d'identité. Votre application doit obtenir ce jeton en authentifiant l'utilisateur de votre application auprès d'un fournisseur d'identité web. Assurez-vous de spécifier ce paramètre lorsque vous spécifiez BasicJwtCredentialsProvider l' Plugin_Name option.

Ce paramètre est obligatoire si vous spécifiez BasicJwtCredentialsProvider l' Plugin_Name option.

Versions précédentes du pilote JDBC version 2.x

Ne téléchargez une version antérieure du pilote JDBC Amazon Redshift version 2.x que si votre outil nécessite une version spécifique du pilote.

Il s'agit des anciens pilotes JDBC 4.2 compatibles avec la version 2.x des pilotes JDBC :

- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.2.8/redshift-jdbc42-2.2.8.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.2.7/redshift-jdbc42-2.2.7.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.2.6/redshift-jdbc42-2.2.6.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.2.5/redshift-jdbc42-2.2.5.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.2.4/redshift-jdbc42-2.2.4.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.2.3/redshift-jdbc42-2.2.3.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.2.2/redshift-jdbc42-2.2.2.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.2.1/redshift-jdbc42-2.2.1.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.2.0/redshift-jdbc42-2.2.0.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.34/redshift-jdbc42-2.1.0.34.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.33/redshift-jdbc42-2.1.0.33.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.32/redshift-jdbc42-2.1.0.32.zip

- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.30/redshift-jdbc42-2.1.0.30.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.29/redshift-jdbc42-2.1.0.29.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.28/redshift-jdbc42-2.1.0.28.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.26/redshift-jdbc42-2.1.0.26.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.25/redshift-jdbc42-2.1.0.25.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.24/redshift-jdbc42-2.1.0.24.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.23/redshift-jdbc42-2.1.0.23.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.22/redshift-jdbc42-2.1.0.22.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.21/redshift-jdbc42-2.1.0.21.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.20/redshift-jdbc42-2.1.0.20.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.19/redshift-jdbc42-2.1.0.19.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.18/redshift-jdbc42-2.1.0.18.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.17/redshift-jdbc42-2.1.0.17.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.16/redshift-jdbc42-2.1.0.16.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.15/redshift-jdbc42-2.1.0.15.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.14/redshift-jdbc42-2.1.0.14.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.13/redshift-jdbc42-2.1.0.13.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.12/redshift-jdbc42-2.1.0.12.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.11/redshift-jdbc42-2.1.0.11.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.10/redshift-jdbc42-2.1.0.10.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.9/redshift-jdbc42-2.1.0.9.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.8/redshift-jdbc42-2.1.0.8.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.7/redshift-jdbc42-2.1.0.7.zip

Connecteur Amazon Redshift Python

En utilisant le connecteur Amazon Redshift pour Python, vous pouvez intégrer le travail au AWS SDK pour Python (Boto3), ainsi qu'à Pandas et à Numerical Python (). NumPy Pour plus d'informations sur les pandas, consultez le référentiel des pandas GitHub . Pour plus d'informations NumPy, consultez le NumPy GitHubréférentiel.

Le connecteur Amazon Redshift Python fournit une solution open source. Vous pouvez parcourir le code source, demander des améliorations, signaler des problèmes et apporter des contributions.

Pour utiliser le connecteur Amazon Redshift Python, assurez-vous que vous disposez de Python version 3.6 ou ultérieure. Pour plus d'informations, consultez le Contrat de licence du pilote Amazon Redshift Python.

Le connecteur Amazon Redshift Python fournit les éléments suivants :

- Gestion des identités et des accès AWS Authentification (IAM). Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift.
- Authentification du fournisseur d'identité utilisant l'accès à l'API fédérée. L'accès à l'API fédéré est pris en charge par les fournisseurs d'identité d'entreprise tels que les suivants :
  - Azure AD. Pour plus d'informations, consultez le billet de blog AWS Big Data Federate Amazon Redshift access with Microsoft Azure AD single sign-on.
  - Active Directory Federation Services. Pour plus d'informations, consultez le billet de blog AWS Big Data Fédérer l'accès à votre cluster Amazon Redshift avec Active Directory Federation Services (AD FS) : Partie 1.
  - Okta. Pour plus d'informations, consultez le billet de blog consacré au AWS Big Data Federate Amazon Redshift access with Okta as an identity provider.
  - PingFederate. Pour plus d'informations, consultez le PingFederate site.
  - JumpCloud. Pour plus d'informations, consultez le JumpCloud site.
- Types de données Amazon Redshift.

Le connecteur Amazon Redshift Python implémente la spécification 2.0 de l'API de base de données Python. Pour plus d'informations, consultez PEP 249 : spécification de l'API de base de données Python v2.0 sur le site web de Python.

Rubriques

- Installation du connecteur Amazon Redshift Python
- Options de configuration du connecteur Amazon Redshift Python
- Importation du connecteur Python
- Intégration du connecteur Python avec NumPy
- Intégration du connecteur Python à pandas
- Utilisation des plugins de fournisseur d'identité
- Exemples d'utilisation du connecteur Amazon Redshift Python
- Référence d'API pour le connecteur Amazon Redshift Python

Installation du connecteur Amazon Redshift Python

Vous pouvez utiliser l'une des méthodes suivantes pour installer le connecteur Amazon Redshift Python :

- Python Package Index (PyPI)
- Conda
- Clonage du référentiel GitHub

Installation du connecteur Python depuis PyPI

Pour installer le connecteur Python à partir de l'index Python Package Index (PyPI), vous pouvez utiliser pip. Pour ce faire, exécutez la commande suivante.

```
>>> pip install redshift_connector
```

Vous pouvez installer le connecteur dans un environnement virtuel. Pour ce faire, exécutez la commande suivante.

```
>>> pip install redshift_connector
```

En option, vous pouvez installer des pandas et NumPy utiliser le connecteur.

```
>>> pip install 'redshift_connector[full]'
```

Pour plus d'informations sur pip, consultez le site web de pip.

Installation du connecteur Python depuis Conda

Vous pouvez installer le connecteur Python depuis Anaconda.org.

```
>>>conda install -c conda-forge redshift_connector
```

Installation du connecteur Python en clonant le GitHub dépôt depuis AWS

Pour installer le connecteur Python depuis la source, clonez le GitHub dépôt depuis AWS. Après avoir installé Python et virtualenv, configurez votre environnement et installez les dépendances requises en exécutant les commandes suivantes.

```
$ git clone https://github.com/aws/amazon-redshift-python-driver.git
$ cd amazon-redshift-python-driver
$ virtualenv venv
$ . venv/bin/activate
$ python -m pip install -r requirements.txt
$ python -m pip install -e .
$ python -m pip install redshift_connector
```

Options de configuration du connecteur Amazon Redshift Python

Vous trouverez ci-dessous des descriptions des options que vous pouvez spécifier pour le connecteur Amazon Redshift Python. Les options ci-dessous s'appliquent à la dernière version de connecteur disponible, sauf indication contraire.

access_key_id

- Valeur par défaut – Aucune
- Types de données – Chaîne

ID de clé d'accès pour l'utilisateur ou le rôle IAM configuré pour l'authentification de base de données IAM.

Ce paramètre est facultatif.

allow_db_user_override

- Valeur par défaut – False
- Types de données – Booléen

True

Spécifie que le connecteur utilise la valeur `DbUser` de l'assertion SAML (Security Assertion Markup Language).

False

Spécifie que la valeur du paramètre de connexion `DbUser` est utilisée.

Ce paramètre est facultatif.

app_name

- Valeur par défaut – Aucune
- Types de données – Chaîne

Nom de l'application fournisseur d'identité (IdP) utilisée pour l'authentification.

Ce paramètre est facultatif.

application_name

- Valeur par défaut – Aucune
- Type de données : chaîne

Nom de l’application client à transmettre à Amazon Redshift à des fins d’audit. Le nom de l’application que vous fournissez apparaît dans la colonne « application_name » de la table SYS_CONNECTION_LOG. Cela permet de suivre et de dépanner les sources de connexion lors des problèmes de débogage.

Ce paramètre est facultatif.

auth_profile

- Valeur par défaut – Aucune
- Types de données – Chaîne

Nom d'un profil d'authentification Amazon Redshift ayant des propriétés de connexion JSON. Pour plus d'informations sur l'attribution de noms aux paramètres de connexion, consultez la classe `RedshiftProperty`. La classe `RedshiftProperty` stocke les paramètres de connexion fournis par l'utilisateur final et, le cas échéant, générés pendant le processus d'authentification IAM (par exemple, les informations d'identification IAM temporaires). Pour plus d'informations, consultez le RedshiftProperty cours.

Ce paramètre est facultatif.

auto_create

- Valeur par défaut – False
- Types de données – Booléen

Valeur qui indique si l'utilisateur doit être créé s'il n'existe pas.

Ce paramètre est facultatif.

client_id

- Valeur par défaut – Aucune
- Types de données – Chaîne

ID client d'Azure IdP.

Ce paramètre est facultatif.

client_secret

- Valeur par défaut – Aucune
- Types de données – Chaîne

Secret client d'Azure IdP.

Ce paramètre est facultatif.

cluster_identifier

- Valeur par défaut – Aucune
- Types de données – Chaîne

Identifiant du cluster Amazon Redshift.

Ce paramètre est facultatif.

credentials_provider

- Valeur par défaut – Aucune
- Types de données – Chaîne

IdP utilisé pour s'authentifier auprès d'Amazon Redshift. Voici les valeurs valides :

- `AdfsCredentialsProvider`
- `AzureCredentialsProvider`

- `BrowserAzureCredentialsProvider`
- `BrowserAzureOAuth2CredentialsProvider`
- `BrowserIdcAuthPlugin` : un plugin d’autorisation utilisant AWS IAM Identity Center.
- `BrowserSamlCredentialsProvider`
- `IdpTokenAuthPlugin`— Un plugin d'autorisation qui accepte un jeton AWS IAM Identity Center ou des jetons d'identité (JWT) OpenID Connect (JSON-based OIDC) provenant de n'importe quel fournisseur d'identité Web lié AWS à l'IAM Identity Center.
- `PingCredentialsProvider`
- `OktaCredentialsProvider`

Ce paramètre est facultatif.

database

- Valeur par défaut – Aucune
- Types de données – Chaîne

Nom de la base de données à laquelle vous souhaitez vous connecter.

Ce paramètre est obligatoire.

database_metadata_current_db_only

- Valeur par défaut – True
- Types de données – Booléen

Valeur qui indique si une application prend en charge les catalogues d'unités de partage des données de plusieurs bases de données. La valeur par défaut True indique que l'application ne prend pas en charge les catalogues d'unités de partage des données de plusieurs bases de données pour des raisons de compatibilité ascendante.

Ce paramètre est facultatif.

db_groups

- Valeur par défaut – Aucune
- Type de données : chaîne

Liste séparée par des virgules des noms de groupes de base de données existants que l'utilisateur a indiqués par des DbUser jointures pour la session en cours.

Ce paramètre est facultatif.

db_user

- Valeur par défaut – Aucune
- Types de données – Chaîne

L'ID utilisateur à utiliser avec Amazon Redshift.

Ce paramètre est facultatif.

activer_types_tables

- Valeur par défaut – True
- Types de données – Booléen

Spécifie si le connecteur reconnaît les informations détaillées sur le type de table provenant de la source de données dans les résultats des méthodes `get_tables` et `get_table_types` des métadonnées. Par défaut, le connecteur reconnaît les types de tables détaillés.

- Vrai : le connecteur reconnaît les types de tables suivants : TABLE, VIEW, SYSTEM TABLE, SYSTEM VIEW, EXTERNAL TABLE et LOCAL TEMPORARY.
- Faux : le connecteur normalise les informations détaillées sur le type de table dans les types de table génériques TABLE et VIEW.

Ce paramètre est facultatif. Il est disponible dans les versions de connecteur 2.1.16 et ultérieures.

endpoint_url

- Valeur par défaut – Aucune
- Types de données – Chaîne

URL du point de terminaison Amazon Redshift. Cette option est réservée à un usage AWS interne.

Ce paramètre est facultatif.

group_federation

- Valeur par défaut – False
- Types de données – Booléen

Cette option spécifie si les groupes d'IDP Amazon Redshift doivent être utilisés.

Ce paramètre est facultatif.

true

Utilisez les groupes Amazon Redshift Identity Provider (IDP).

false

Utilisez l'API STS et GetClusterCredentials pour la fédération d'utilisateurs et spécifiez db_groups pour la connexion.

hôte

- Valeur par défaut – Aucune
- Types de données – Chaîne

Nom d'hôte du cluster Amazon Redshift.

Ce paramètre est facultatif.

iam

- Valeur par défaut – False
- Types de données – Booléen

L'authentification IAM est activée.

Ce paramètre est obligatoire.

iam_disable_cache

- Valeur par défaut – False
- Types de données – Booléen

Cette option spécifie si les informations d’identification IAM sont mises en cache. Par défaut, les informations d'identification IAM sont mises en cache. Cela améliore les performances lorsque les demandes envoyées à API Gateway sont limitées.

Ce paramètre est facultatif.

idc_client_display_name

- Valeur par défaut : connecteur Amazon Redshift Python
- Types de données – Chaîne

Le nom d'affichage à utiliser pour le client qui l'utilise BrowserIdcAuthPlugin.

Ce paramètre est facultatif.

idc_region

- Valeur par défaut – Aucune
- Types de données – Chaîne

AWS Région dans laquelle se trouve l'instance AWS IAM Identity Center.

Ce paramètre est requis uniquement lors de l’authentification à l’aide de `BrowserIdcAuthPlugin` dans l’option de configuration credentials_provider.

idp_partition

- Valeur par défaut – Aucune
- Types de données – Chaîne

Spécifie la partition cloud sur laquelle votre fournisseur d'identité (IdP) est configuré. Cela détermine le point de terminaison d'authentification IdP auquel le pilote se connecte.

Si ce paramètre est laissé vide, le pilote utilise par défaut la partition commerciale. Les valeurs possibles sont :

- `us-gov`: utilisez cette valeur si votre IdP est configuré dans Azure Government. Par exemple, Azure AD Government utilise le point de terminaison`login.microsoftonline.us`.

- `cn`: Utilisez cette valeur si votre IdP est configuré dans la partition cloud de Chine. Par exemple, Azure AD Chine utilise le point de terminaison`login.chinacloudapi.cn`.

Ce paramètre est facultatif.

idpPort

- Valeur par défaut – 7890
- Type de données – Entier

Port d'écoute auquel IdP envoie l'assertion SAML.

Ce paramètre est obligatoire.

idp_response_timeout

- Valeur par défaut – 120
- Type de données – Entier

Délai d'expiration de la récupération de l'assertion SAML à partir de l'IdP.

Ce paramètre est obligatoire.

idp_tenant

- Valeur par défaut – Aucune
- Types de données – Chaîne

Locataire IdP.

Ce paramètre est facultatif.

issuer_url

- Valeur par défaut – Aucune
- Types de données – Chaîne

Pointe vers le point de terminaison de l'instance du serveur AWS IAM Identity Center.

Ce paramètre est requis uniquement lors de l'authentification à l'aide de `BrowserIdcAuthPlugin` dans l'option de configuration credentials_provider.

listen_port

- Valeur par défaut – 7890
- Type de données – Entier

Port utilisé par le pilote pour recevoir la réponse SAML du fournisseur d'identité ou le code d'autorisation lors de l'utilisation des services SAML, Azure AD ou AWS IAM Identity Center via un plug-in de navigateur.

Ce paramètre est facultatif.

login_url

- Valeur par défaut – Aucune
- Type de données : chaîne

URL d'authentification unique pour le fournisseur d'identité.

Ce paramètre est facultatif.

max_prepared_statements

- Valeur par défaut : 1 000
- Type de données – Entier

Nombre maximal d'instructions préparées qui seront mises en cache par connexion. Le réglage de ce paramètre sur 0 désactive le mécanisme de mise en cache. La saisie d'un nombre négatif pour ce paramètre lui donne la valeur par défaut.

Ce paramètre est facultatif.

numeric_to_float

- Valeur par défaut – False
- Types de données – Booléen

Cette option spécifie si le connecteur convertit les valeurs de type de données numériques du format « décimal.Décimal » au format flottant. Par défaut, le connecteur reçoit les valeurs de type numérique en tant que format « décimal.Décimal » et ne les convertit pas.

Nous ne recommandons pas d'activer l'option numeric_to_float pour les cas d'utilisation qui exigent de la précision, car les résultats peuvent être arrondis.

Pour plus d'informations sur le format « décimal.Décimal » et les compromis entre celui-ci et le format flottant, consultez la section decimal — Decimal fixed point and floating point arithmetic (Arithmétique à virgule fixe de type décimal — Décimal et à virgule flottante) sur le site Web de Python.

Ce paramètre est facultatif.

partner_sp_id

- Valeur par défaut – Aucune
- Types de données – Chaîne

ID SP partenaire utilisé pour l'authentification avec Ping.

Ce paramètre est facultatif.

mot de passe

- Valeur par défaut – Aucune
- Types de données – Chaîne

Mot de passe à utiliser pour l'authentification.

Ce paramètre est facultatif.

port

- Valeur par défaut : 5439
- Type de données – Entier

Numéro de port du cluster Amazon Redshift.

Ce paramètre est obligatoire.

preferred_role

- Valeur par défaut – Aucune
- Types de données – Chaîne

Rôle IAM préféré pour la connexion actuelle.

Ce paramètre est facultatif.

principal_arn

- Valeur par défaut – Aucune
- Type de données : chaîne

L'Amazon Resource Name (ARN) de l'utilisateur ou du rôle IAM pour lequel vous générez une politique. Il est recommandé d'attacher une politique à un rôle, puis d'attacher le rôle à votre utilisateur, pour y accéder.

Ce paramètre est facultatif.

profile

- Valeur par défaut – Aucune
- Type de données : chaîne

Nom d'un profil dans un fichier d' AWS informations d'identification contenant des AWS informations d'identification.

Ce paramètre est facultatif.

provider_name

- Valeur par défaut – Aucune
- Type de données : chaîne

Nom du fournisseur d'authentification native Redshift.

Ce paramètre est facultatif.

region

- Valeur par défaut – Aucune
- Type de données : chaîne

L' Région AWS endroit où se trouve le cluster.

Ce paramètre est facultatif.

role_arn

- Valeur par défaut – Aucune
- Types de données – Chaîne

Amazon Resource Name (ARN) du rôle que l'appelant doit assumer. Ce paramètre est utilisé par le fournisseur indiqué par `JwtCredentialsProvider`.

Pour le `JwtCredentialsProvider`, ce paramètre est obligatoire. Sinon, ce paramètre est facultatif.

role_session_name

- Valeur par défaut – jwt_redshift_session
- Types de données – Chaîne

Un identifiant pour la séance de rôle assumé. En règle générale, vous transmettez le nom ou l'identifiant associé à l'utilisateur qui utilise votre application. Les informations d’identification de sécurité temporaires utilisées par votre application sont associées à cet utilisateur. Ce paramètre est utilisé par le fournisseur indiqué par `JwtCredentialsProvider`.

Ce paramètre est facultatif.

scope

- Valeur par défaut – Aucune
- Type de données : chaîne

Liste des portées, séparées par des espaces, auxquelles l'utilisateur peut consentir. Vous spécifiez ce paramètre afin que votre application puisse obtenir le consentement des API que vous souhaitez appeler. Vous pouvez spécifier ce paramètre lorsque vous spécifiez BrowserAzureOAuth2CredentialsProvider l'option credentials_provider.

Ce paramètre est obligatoire pour le BrowserAzureOAuth2CredentialsProvider plug-in.

secret_access_key_id

- Valeur par défaut – Aucune
- Types de données – Chaîne

Clé d'accès secrète pour l'utilisateur ou le rôle IAM configuré pour l'authentification de base de données IAM.

Ce paramètre est facultatif.

session_token

- Valeur par défaut – Aucune
- Types de données – Chaîne

ID de clé d’accès pour l’utilisateur ou le rôle IAM configuré pour l’authentification de base de données IAM. Ce paramètre est obligatoire si des AWS informations d'identification temporaires sont utilisées.

Ce paramètre est facultatif.

serverless_acct_id

- Valeur par défaut – Aucune
- Type de données : chaîne

ID du compte Amazon Redshift Serverless.

Ce paramètre est facultatif.

serverless_work_group

- Valeur par défaut – Aucune

- Type de données : chaîne

Nom du groupe de travail Amazon Redshift Serverless.

Ce paramètre est facultatif.

ssl

- Valeur par défaut – True
- Types de données – Booléen

Le protocole SSL est activé.

Ce paramètre est obligatoire.

ssl_insecure

- Valeur par défaut – False
- Types de données – Booléen

Valeur qui indique si la vérification du certificat de serveur d'hôtes IdP doit être désactivée. La définition de ce paramètre sur True désactivera la vérification du certificat SSL du serveur d'hôtes IdP. Nous vous recommandons de conserver la valeur par défaut de False dans les environnements de production.

Ce paramètre est facultatif.

sslmode

- Valeur par défaut – verify-ca
- Types de données – Chaîne

Sécurité de la connexion à Amazon Redshift. Vous pouvez spécifier chacune des valeurs suivantes :

- verify-ca
- verify-full

> **Note**
>
> Nous vous recommandons d'utiliser `verify-full` des connexions SSL dans la mesure du possible.

Ce paramètre est obligatoire.

tcp_keepalive

- Valeur par défaut – True
- Types de données – Booléen

S’il faut utiliser les keepalives TCP pour empêcher les connexions de s’interrompre. Vous pouvez spécifier les valeurs suivantes :

- True : le pilote utilisera les keepalives TCP pour empêcher les connexions de s’interrompre.
- False : le pilote n’utilisera pas les keepalives TCP.

Ce paramètre est facultatif.

tcp_keepalive_count

- Valeur par défaut – Aucune
- Type de données – Entier

Le nombre de sondes non reconnues à envoyer avant de considérer la connexion comme inactive. Par exemple, définir la valeur sur 3 signifie que le pilote enverra 3 paquets keepalive sans réponse avant de déterminer que la connexion n’est plus active.

Si ce paramètre n’est pas spécifié, Amazon Redshift utilise la valeur par défaut du système.

Ce paramètre est facultatif.

tcp_keepalive_interval

- Valeur par défaut – Aucune
- Type de données – Entier

Intervalle, en secondes, entre les sondes keepalive suivantes si le pilote n’a pas reçu d’accusé de réception pour la sonde précédente. Si vous spécifiez ce paramètre, il doit s’agir d’un nombre entier positif.

Si ce paramètre n’est pas spécifié, Amazon Redshift utilise la valeur par défaut du système.

Ce paramètre est facultatif.

tcp_keepalive_idle

- Valeur par défaut – Aucune
- Type de données – Entier

Durée d’inactivité, en secondes, après laquelle le pilote envoie la première sonde keepalive. Par exemple, si vous définissez la valeur sur 120, le pilote attendra 2 minutes d’inactivité avant d’envoyer le premier paquet keepalive. Si vous spécifiez ce paramètre, il doit s’agir d’un nombre entier positif.

Si ce paramètre n’est pas spécifié, Amazon Redshift utilise la valeur par défaut du système.

Ce paramètre est facultatif.

timeout

- Valeur par défaut – Aucune
- Type de données – Entier

Le nombre de secondes avant que la connexion au serveur ne soit interrompue.

Ce paramètre est facultatif.

jeton

- Valeur par défaut – Aucune
- Types de données – Chaîne

Un jeton d'accès fourni par AWS IAM Identity Center ou un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d'identité Web AWS lié à IAM Identity Center. Votre application doit générer ce jeton en authentifiant l'utilisateur de votre application auprès d' AWS IAM Identity Center ou d'un fournisseur d'identité lié à AWS IAM Identity Center.

Ce paramètre fonctionne avec `IdpTokenAuthPlugin`.

token_type

- Valeur par défaut – Aucune
- Types de données – Chaîne

Type de jeton utilisé dans `IdpTokenAuthPlugin`.

Vous pouvez spécifier les valeurs suivantes :

ACCESS_TOKEN

Entrez cette valeur si vous utilisez un jeton d'accès fourni par AWS IAM Identity Center.

EXT_JWT

Entrez cette valeur si vous utilisez un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d’identité Web intégré à AWS IAM Identity Center.

Ce paramètre fonctionne avec `IdpTokenAuthPlugin`.

user

- Valeur par défaut – Aucune
- Types de données – Chaîne

Nom d'utilisateur à utiliser pour l'authentification.

Ce paramètre est facultatif.

web_identity_token

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le jeton d'accès OAuth 2.0 ou le jeton d'identification OpenID Connect qui est fourni par le fournisseur d'identité. Assurez-vous que votre application obtient ce jeton en authentifiant l'utilisateur de votre application auprès d'un fournisseur d'identité web. Ce paramètre est utilisé par le fournisseur indiqué par `JwtCredentialsProvider`.

Pour le `JwtCredentialsProvider`, ce paramètre est obligatoire. Sinon, ce paramètre est facultatif.

Importation du connecteur Python

Pour importer le connecteur Python, exécutez la commande suivante.

```
>>> import redshift_connector
```

Pour vous connecter à un cluster Amazon Redshift à l'aide AWS d'informations d'identification, exécutez la commande suivante.

```
conn = redshift_connector.connect(
    host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
    port=5439,
    database='dev',
    user='awsuser',
    password='my_password'
 )
```

Intégration du connecteur Python avec NumPy

Voici un exemple d'intégration du connecteur Python avec NumPy.

```
>>>  import numpy
#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(
     host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
     port=5439,
     database='dev',
     user='awsuser',
     password='my_password'
  )

# Create a Cursor object
>>> cursor = conn.cursor()

# Query and receive result set
cursor.execute("select * from book")

result: numpy.ndarray = cursor.fetch_numpy_array()
```

```
print(result)
```

Voici les résultats.

```
[['One Hundred Years of Solitude' 'Gabriel García Márquez']
['A Brief History of Time' 'Stephen Hawking']]
```

Intégration du connecteur Python à pandas

Voici un exemple d'intégration du connecteur Python à pandas.

```
>>> import pandas

#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(
     host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
     port=5439,
     database='dev',
     user='awsuser',
     password='my_password'
  )

# Create a Cursor object
>>> cursor = conn.cursor()

# Query and receive result set
cursor.execute("select * from book")
result: pandas.DataFrame = cursor.fetch_dataframe()
print(result)
```

Utilisation des plugins de fournisseur d'identité

Pour des informations générales sur l'utilisation des plugins de fournisseur d'identité, veuillez consulter Options visant à fournir des informations d'identification IAM. Pour plus d'informations sur la gestion des identités IAM, y compris les bonnes pratiques pour les rôles IAM, consultez Identity and Access Management dans Amazon Redshift.

Authentification à l'aide du plugin du fournisseur d'identité ADFS

Voici un exemple d'utilisation du plugin du fournisseur d'identité ADFS (Active Directory Federation Service) pour authentifier un utilisateur se connectant à une base de données Amazon Redshift.

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='AdfsCredentialsProvider',
    user='brooke@myadfshostname.com',
    password='Hunter2',
    idp_host='myadfshostname.com'
)
```

Authentification à l'aide du plugin du fournisseur d'identité Azure

Voici un exemple d'authentification à l'aide du plugin du fournisseur d'identité Azure. Vous pouvez créer des valeurs pour un `client_id` et un `client_secret` pour une application métier Azure, comme illustré ci-dessous.

```
>>>  con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='AzureCredentialsProvider',
    user='brooke@myazure.org',
    password='Hunter2',
    idp_tenant='my_idp_tenant',
    client_id='my_client_id',
    client_secret='my_client_secret',
    preferred_role='arn:aws:iam:123:role/DataScientist'
)
```

Authentification à l'aide du AWS Plug-in de fournisseur d'identité IAM Identity Center

Voici un exemple d'authentification à l'aide du plug-in de fournisseur d'identité AWS IAM Identity Center.

```
with redshift_connector.connect(
credentials_provider='BrowserIdcAuthPlugin',
host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
database='dev',
idc_region='us-east-1',
issuer_url='https://identitycenter.amazonaws.com/ssoins-790723ebe09c86f9',
```

```
idp_response_timeout=60,
listen_port=8100,
idc_client_display_name='Test Display Name',
# port value of 5439 is specified by default
)
```

Authentification à l'aide du plugin du fournisseur d'identité de navigateur Azure

Voici un exemple d'utilisation du plugin du fournisseur d'identité de navigateur Azure pour authentifier un utilisateur se connectant à une base de données Amazon Redshift.

Multi-factor l'authentification a lieu dans le navigateur, où les informations de connexion sont fournies par l'utilisateur.

```
>>>con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='BrowserAzureCredentialsProvider',
    idp_tenant='my_idp_tenant',
    client_id='my_client_id',
)
```

Authentification à l'aide du plugin du fournisseur d'identité Okta

Voici un exemple d'authentification à l'aide du plugin du fournisseur d'identité Okta. Vous pouvez obtenir les valeurs pour `idp_host`, `app_id` et `app_name` via l'application Okta.

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='OktaCredentialsProvider',
    user='brooke@myazure.org',
    password='hunter2',
    idp_host='my_idp_host',
    app_id='my_first_appetizer',
    app_name='dinner_party'
)
```

Authentification à l' JumpCloud aide d'un plugin de fournisseur d'identité de navigateur SAML générique

Voici un exemple d'utilisation d'un plug-in JumpCloud de fournisseur d'identité de navigateur SAML générique pour l'authentification.

Le paramètre de mot de passe est obligatoire. Toutefois, il n'est pas nécessaire de saisir ce paramètre, car l'authentification multifacteur a lieu dans le navigateur.

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='BrowserSamlCredentialsProvider',
    user='brooke@myjumpcloud.org',
    password='',
    login_url='https://sso.jumpcloud.com/saml2/plustwo_melody'
)
```

Exemples d'utilisation du connecteur Amazon Redshift Python

Vous trouverez ci-dessous des exemples d'utilisation du connecteur Amazon Redshift Python. Pour les exécuter, vous devez installer au préalable le connecteur Python. Pour plus d'informations sur l'installation du connecteur Python Amazon Redshift, consultez Installation du connecteur Amazon Redshift Python. Pour plus d'informations sur les options de configuration que vous pouvez utiliser avec le connecteur Python, consultez Options de configuration du connecteur Amazon Redshift Python.

Rubriques

- Connexion à un cluster Amazon Redshift et interrogation à l'aide de AWS informations d’identification
- Activation de la validation automatique
- Configuration du paramstyle d'un curseur
- Utilisation de COPY pour copier des données à partir d'un compartiment Amazon S3 et de UNLOAD pour y écrire des données

Connexion à un cluster Amazon Redshift et interrogation à l'aide de AWS informations d’identification

L'exemple suivant vous explique comment vous connecter à un cluster Amazon Redshift à l'aide de vos AWS informations d'identification, puis comment interroger une table et récupérer les résultats de la requête.

```
#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(
     host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
     database='dev',
     port=5439,
     user='awsuser',
     password='my_password'
  )

# Create a Cursor object
>>> cursor = conn.cursor()

# Query a table using the Cursor
>>> cursor.execute("select * from book")

#Retrieve the query result set
>>> result: tuple = cursor.fetchall()
>>> print(result)
 >> (['One Hundred Years of Solitude', 'Gabriel García Márquez'], ['A Brief History of
 Time', 'Stephen Hawking'])
```

Activation de la validation automatique

La propriété autocommit est désactivée par défaut, conformément à la spécification de l'API de base de données Python. Vous pouvez utiliser les commandes suivantes pour activer la propriété de validation automatique de la connexion après avoir exécuté une commande de restauration pour vous assurer qu'une transaction n'est pas en cours.

```
#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(...)

# Run a rollback command
>>>  conn.rollback()
```

```
# Turn on autocommit
>>>  conn.autocommit = True
>>>  conn.run("VACUUM")

# Turn off autocommit
>>>  conn.autocommit = False
```

Configuration du paramstyle d'un curseur

Le paramstyle d'un curseur peut être modifié via cursor.paramstyle. Le paramstyle par défaut utilisé est `format`. Les valeurs valides pour paramstyle sont `qmark`, `numeric`, `named`, `format` et `pyformat`.

Vous trouverez ci-dessous des exemples d'utilisation de différents paramstyles pour transmettre des paramètres à un exemple d'instruction SQL.

```
# qmark
redshift_connector.paramstyle = 'qmark'
sql = 'insert into foo(bar, jar) VALUES(?, ?)'
cursor.execute(sql, (1, "hello world"))

# numeric
redshift_connector.paramstyle = 'numeric'
sql = 'insert into foo(bar, jar) VALUES(:1, :2)'
cursor.execute(sql, (1, "hello world"))

# named
redshift_connector.paramstyle = 'named'
sql = 'insert into foo(bar, jar) VALUES(:p1, :p2)'
cursor.execute(sql, {"p1":1, "p2":"hello world"})

# format
redshift_connector.paramstyle = 'format'
sql = 'insert into foo(bar, jar) VALUES(%s, %s)'
cursor.execute(sql, (1, "hello world"))

# pyformat
redshift_connector.paramstyle = 'pyformat'
sql = 'insert into foo(bar, jar) VALUES(%(bar)s, %(jar)s)'
cursor.execute(sql, {"bar": 1, "jar": "hello world"})
```

Utilisation de COPY pour copier des données à partir d'un compartiment Amazon S3 et de UNLOAD pour y écrire des données

L'exemple suivant montre comment copier des données depuis un compartiment Amazon S3 dans une table, puis comment les décharger de cette table dans le compartiment.

Un fichier texte nommé `category_csv.txt` contenant les données suivantes est chargé dans un compartiment Amazon S3.

```
12,Shows,Musicals,Musical theatre
13,Shows,Plays,"All ""non-musical"" theatre"
14,Shows,Opera,"All opera, light, and ""rock"" opera"
15,Concerts,Classical,"All symphony, concerto, and choir concerts"
```

Voici un exemple de code Python, qui se connecte d'abord à la base de données Amazon Redshift. Il crée ensuite une table appelée `category` et copie les données CSV du compartiment S3 dans la table.

```
#Connect to the cluster and create a Cursor
>>> import redshift_connector
>>> with redshift_connector.connect(...) as conn:
>>> with conn.cursor() as cursor:

#Create an empty table
>>>     cursor.execute("create table category (catid int, cargroup varchar, catname
 varchar, catdesc varchar)")

#Use COPY to copy the contents of the S3 bucket into the empty table
>>>     cursor.execute("copy category from 's3://testing/category_csv.txt' iam_role
 'arn:aws:iam::123:role/RedshiftCopyUnload' csv;")

#Retrieve the contents of the table
>>>     cursor.execute("select * from category")
>>>     print(cursor.fetchall())

#Use UNLOAD to copy the contents of the table into the S3 bucket
>>>     cursor.execute("unload ('select * from category') to 's3://testing/
unloaded_category_csv.txt'  iam_role 'arn:aws:iam::123:role/RedshiftCopyUnload' csv;")

#Retrieve the contents of the bucket
>>>     print(cursor.fetchall())
```

```
 >> ([12, 'Shows', 'Musicals', 'Musical theatre'], [13, 'Shows', 'Plays', 'All "non-
musical" theatre'], [14, 'Shows', 'Opera', 'All opera, light, and "rock" opera'], [15,
 'Concerts', 'Classical', 'All symphony, concerto, and choir concerts'])
```

Si vous n'avez pas défini `autocommit` sur true, validez avec `conn.commit()` après avoir exécuté les instructions `execute()`.

Les données sont déchargées dans le fichier `unloaded_category_csv.text0000_part00` dans le compartiment S3, avec le contenu suivant :

```
12,Shows,Musicals,Musical theatre
13,Shows,Plays,"All ""non-musical"" theatre"
14,Shows,Opera,"All opera, light, and ""rock"" opera"
15,Concerts,Classical,"All symphony, concerto, and choir concerts"
```

Référence d'API pour le connecteur Amazon Redshift Python

Vous trouverez ci-dessous une description des opérations d'API du connecteur Amazon Redshift Python.

redshift_connector

Vous trouverez ci-dessous une description de l'opération d'API `redshift_connector`.

`connect(user, database, password[, port, …])`

Établit une connexion à un cluster Amazon Redshift. Cette fonction valide les entrées de l'utilisateur, s'authentifie éventuellement à l'aide d'un plugin de fournisseur d'identité, puis construit un objet de connexion.

`apilevel`

Le niveau DBAPI pris en charge, actuellement « 2.0 ».

`paramstyle`, `str(object='') -> str str(bytes_or_buffer[, encoding[, errors]]) -> str`

Style de paramètre d'API de base de données à utiliser globalement.

Connexion

Vous trouverez ci-dessous une description des opérations d'API de connexion pour le connecteur Amazon Redshift Python.

`__init__(user, password, database[, host, …])`

Initialise un objet de connexion brut.

`cursor`

Crée un objet de curseur lié à cette connexion.

`commit`

Valide la transaction de base de données actuelle.

`rollback`

Annule la transaction de base de données actuelle.

`close`

Ferme la connexion à la base de données.

`execute(cursor, operation, vals)`

Exécute la commande SQL spécifiée. Vous pouvez fournir les paramètres sous forme de séquence ou de mappage, en fonction de la valeur de `redshift_connector.paramstyle`.

`run(sql[, stream])`

Exécute la commande SQL spécifiée. Vous pouvez également fournir un flux à utiliser avec la commande COPY.

`xid(format_id, global_transaction_id, …)`

Créez un ID de transaction. Seul le paramètre `global_transaction_id` est utilisé dans postgres. format_id et branch_qualifier ne sont pas utilisés dans postgres. Le `global_transaction_id` peut être n'importe quel identifiant de chaîne pris en charge par postgres qui renvoie un tuple (`format_id`, `global_transaction_id`, `branch_qualifier`).

`tpc_begin(xid)`

Commence une transaction TPC avec un ID de transaction `xid` composé d'un ID de format, d'un ID de transaction global et d'un qualificateur de branche.

`tpc_prepare`

Effectue la première phase d'une transaction démarrée avec .tpc_begin.

`tpc_commit([xid])`

Lorsqu'il est appelé sans argument, .tpc_commit engage une transaction TPC préalablement préparée avec .tpc_prepare().

`tpc_rollback([xid])`

Lorsqu'il est appelé sans argument, .tpc_rollback annule une transaction TPC.

`tpc_recover`

Renvoie une liste des ID de transaction en attente pouvant être utilisés avec .tpc_commit (xid) ou .tpc_rollback (xid).

Curseur

Vous trouverez ci-dessous une description de l'opération d'API du curseur.

`__init__(connection[, paramstyle])`

Initialise un objet de curseur brut.

`insert_data_bulk(filename, table_name, parameter_indices, column_names, delimiter, batch_size)`

Exécute une instruction INSERT en bloc.

`execute(operation[, args, stream, …])`

Exécute une opération de base de données.

`executemany(operation, param_sets)`

Prépare une opération de base de données, puis l'exécute pour toutes les séquences de paramètres ou les mappages fournis.

`fetchone`

Récupère la ligne suivante d'un ensemble de résultats de requête.

`fetchmany([num])`

Récupère l'ensemble de lignes suivant d'un résultat de requête.

`fetchall`

Récupère toutes les lignes restantes d'un résultat de requête.

`close`

Fermez le curseur maintenant.

`__iter__`

Un objet de curseur peut être itéré pour récupérer les lignes d'une requête.

`fetch_dataframe([num])`

Renvoie un dataframe des résultats de la dernière requête.

`write_dataframe(df, table)`

Écrit le même dataframe de structure dans une base de données Amazon Redshift.

`fetch_numpy_array([num])`

Renvoie un NumPy tableau des derniers résultats de la requête.

`get_catalogs`

Amazon Redshift ne prend pas en charge plusieurs catalogues à partir d'une seule connexion. Amazon Redshift renvoie uniquement le catalogue actuel.

`get_tables([catalog, schema_pattern, …])`

Renvoie les tables publiques uniques définies par l'utilisateur au sein du système.

`get_columns([catalog, schema_pattern, …])`

Renvoie la liste de toutes les colonnes d'une table spécifique dans une base de données Amazon Redshift.

AdfsCredentialsProvider plugin

Voici la syntaxe du fonctionnement de l'API du AdfsCredentialsProvider plugin pour le connecteur Amazon Redshift Python.

```
redshift_connector.plugin.AdfsCredentialsProvider()
```

AzureCredentialsProvider plugin

Voici la syntaxe du fonctionnement de l'API du AzureCredentialsProvider plugin pour le connecteur Amazon Redshift Python.

```
redshift_connector.plugin.AzureCredentialsProvider()
```

BrowserAzureCredentialsProvider plugin

Voici la syntaxe du fonctionnement de l'API du BrowserAzureCredentialsProvider plugin pour le connecteur Amazon Redshift Python.

```
redshift_connector.plugin.BrowserAzureCredentialsProvider()
```

BrowserSamlCredentialsProvider plugin

Voici la syntaxe du fonctionnement de l'API du BrowserSamlCredentialsProvider plugin pour le connecteur Amazon Redshift Python.

```
redshift_connector.plugin.BrowserSamlCredentialsProvider()
```

OktaCredentialsProvider plugin

Voici la syntaxe du fonctionnement de l'API du OktaCredentialsProvider plugin pour le connecteur Amazon Redshift Python.

```
redshift_connector.plugin.OktaCredentialsProvider()
```

PingCredentialsProvider plugin

Voici la syntaxe du fonctionnement de l'API du PingCredentialsProvider plugin pour le connecteur Amazon Redshift Python.

```
redshift_connector.plugin.PingCredentialsProvider()
```

SamlCredentialsProvider plugin

Voici la syntaxe du fonctionnement de l'API du SamlCredentialsProvider plugin pour le connecteur Amazon Redshift Python.

```
redshift_connector.plugin.SamlCredentialsProvider()
```

Intégration d'Amazon Redshift à Apache Spark

Apache Spark est un modèle distribué de programmation et d'infrastructure qui vous permet d'effectuer des opérations de machine learning, de traitement de flux ou d'analyse graphique. De manière analogue à Apache Hadoop, Spark est un système de traitement distribué open source, couramment utilisé pour les charges de travail de big data. Spark dispose d'un moteur d'exécution optimisé de graphes orientés acycliques dirigés (DAG) et met activement en cache les données en mémoire. Cela peut améliorer les performances, en particulier pour certains algorithmes et requêtes interactives.

Cette intégration vous fournit un connecteur Spark que vous pouvez utiliser pour créer des applications Apache Spark qui lisent et écrivent des données dans Amazon Redshift et Amazon Redshift sans serveur. Ces applications ne compromettent pas les performances des applications ni la cohérence transactionnelle des données. Cette intégration est automatiquement incluse dans Amazon EMR et AWS Glue, ce qui vous permet d'exécuter immédiatement des tâches Apache Spark qui accèdent à des données et les chargent dans Amazon Redshift dans le cadre de vos pipelines d'ingestion et de transformation de données.

Actuellement, vous pouvez utiliser les versions 3.3.x, 3.4.x, 3.5.x, 4.0.x et 4.1.x de Spark avec cette intégration.

Cette intégration fournit les éléments suivants :

- Gestion des identités et des accès AWS Authentification (IAM). Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift.
- Pushdown des prédicats et des requêtes pour améliorer les performances.
- Types de données Amazon Redshift.
- Connectivité à Amazon Redshift et Amazon Redshift sans serveur.

Considérations et limites relatives à l'utilisation du connecteur Spark

- L'URI tempdir pointe vers un emplacement Amazon S3. Ce répertoire temporaire n'est pas nettoyé automatiquement et peut entraîner des frais supplémentaires. Nous vous recommandons d'utiliser les stratégies de cycle de vie d'Amazon S3 dans le guide d'utilisation d'Amazon Simple Storage Service pour définir les règles de conservation du compartiment Amazon S3.

- Par défaut, les copies entre Amazon S3 et Redshift ne fonctionnent pas si le compartiment S3 et le cluster Redshift se trouvent dans des régions différentes AWS . Pour utiliser AWS des régions distinctes, définissez le `tempdir_region` paramètre sur la région du compartiment S3 utilisé pour le`tempdir`.
- Cross-Region écrit entre S3 et Redshift si vous écrivez des données Parquet à l'aide du `tempformat` paramètre.
- Nous vous recommandons d'utiliser le chiffrement côté serveur Amazon S3 pour chiffrer les compartiments Amazon S3 utilisés.
- Nous vous recommandons de bloquer l'accès public aux compartiments Amazon S3.
- Nous recommandons que le cluster Amazon Redshift ne soit pas accessible au public.
- Nous vous recommandons d'activer la journalisation des audits Amazon Redshift.
- Nous vous recommandons d'activer le chiffrement au repos d'Amazon Redshift.
- Nous vous recommandons d'activer le protocole SSL pour la connexion JDBC entre Spark sur Amazon EMR et Amazon Redshift.
- Nous vous recommandons de transmettre un rôle IAM à l'aide du paramètre `aws_iam_role` pour le paramètre d'authentification Amazon Redshift.

Authentification avec le connecteur Spark

Le schéma suivant décrit l'authentification entre Amazon S3, Amazon Redshift, le pilote Spark et les exécuteurs Spark.

Authentification entre Redshift et Spark

Vous pouvez utiliser le pilote JDBC version 2.x fourni par Amazon Redshift pour vous connecter à Amazon Redshift avec le connecteur Spark en spécifiant des informations d'identification. Pour utiliser IAM, configurez votre URL JDBC pour utiliser l'authentification IAM. Pour vous connecter à un cluster Redshift depuis Amazon EMR AWS Glue, assurez-vous que votre rôle IAM dispose des autorisations nécessaires pour récupérer des informations d'identification IAM temporaires. La liste suivante décrit toutes les autorisations dont votre rôle IAM a besoin pour récupérer des informations d'identification et exécuter des opérations Amazon S3.

- Redshift:GetClusterCredentials(pour les clusters Redshift provisionnés)
- Redshift:DescribeClusters(pour les clusters Redshift provisionnés)

- Redshift:GetWorkgroup(pour les groupes de travail Amazon Redshift Serverless)
- Redshift:GetCredentials(pour les groupes de travail Amazon Redshift Serverless)
- s3 : ListBucket
- s3 : GetBucket
- s3 : GetObject
- s3 : PutObject
- s3 : GetBucketLifecycleConfiguration

Pour plus d'informations sur GetClusterCredentials, consultez les politiques IAM pour GetClusterCredentials.

Vous devez également vous assurer qu'Amazon Redshift peut assumer le rôle IAM pendant les opérations `COPY` et `UNLOAD`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "redshift.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Si vous utilisez le pilote JDBC le plus récent, le pilote gérera automatiquement la transition d'un certificat auto-signé Amazon Redshift vers un certificat ACM. Vous devez toutefois spécifier les options SSL dans l'URL JDBC.

L'exemple suivant montre comment spécifier l'URL du pilote JDBC et le `aws_iam_role` pour se connecter à Amazon Redshift.

```
df.write \
```

```
  .format("io.github.spark_redshift_community.spark.redshift ") \
  .option("url", "jdbc:redshift:iam://<the-rest-of-the-connection-string>") \
  .option("dbtable", "<your-table-name>") \
  .option("tempdir", "s3a://<your-bucket>/<your-directory-path>") \
  .option("aws_iam_role", "<your-aws-role-arn>") \
  .mode("error") \
  .save()
```

Authentification entre Amazon S3 et Spark

Si vous utilisez un rôle IAM pour vous authentifier entre Spark et Amazon S3, utilisez l'une des méthodes suivantes :

- Le AWS SDK pour Java tentera automatiquement de trouver des informations d' AWS identification à l'aide de la chaîne de fournisseurs d'informations d'identification par défaut implémentée par la DefaultAWSCredentialsProviderChain classe. Pour plus d'informations, consultez Utilisation de la chaîne de fournisseur d'informations d'identification par défaut.
- Vous pouvez spécifier AWS des clés via les propriétés de configuration Hadoop. Par exemple, si votre configuration `tempdir` pointe vers un système de fichiers `s3n://`, définissez les propriétés `fs.s3n.awsAccessKeyId` et `fs.s3n.awsSecretAccessKey` dans un fichier de configuration XML Hadoop ou appelez `sc.hadoopConfiguration.set()` pour modifier la configuration Hadoop globale de Spark.

Par exemple, si vous utilisez le système de fichiers s3n, ajoutez :

```
sc.hadoopConfiguration.set("fs.s3n.awsAccessKeyId", "YOUR_KEY_ID")
sc.hadoopConfiguration.set("fs.s3n.awsSecretAccessKey", "YOUR_SECRET_ACCESS_KEY")
```

Pour le système de fichiers s3a, ajoutez :

```
sc.hadoopConfiguration.set("fs.s3a.access.key", "YOUR_KEY_ID")
sc.hadoopConfiguration.set("fs.s3a.secret.key", "YOUR_SECRET_ACCESS_KEY")
```

Si vous utilisez Python, effectuez les opérations suivantes :

```
sc._jsc.hadoopConfiguration().set("fs.s3n.awsAccessKeyId", "YOUR_KEY_ID")
sc._jsc.hadoopConfiguration().set("fs.s3n.awsSecretAccessKey",
 "YOUR_SECRET_ACCESS_KEY")
```

- Encodez les clés d'authentification dans l'URL `tempdir`. Par exemple, l'URI `s3n://ACCESSKEY:SECRETKEY@bucket/path/to/temp/dir` encode la paire de clés (`ACCESSKEY`, `SECRETKEY`).

Authentification entre Redshift et Amazon S3

Si vous utilisez les commandes COPY et UNLOAD dans votre requête, vous devez également autoriser Amazon S3 à accéder à Amazon Redshift pour exécuter des requêtes en votre nom. Pour ce faire, autorisez d'abord Amazon Redshift à accéder à d'autres AWS services, puis autorisez les opérations COPY et UNLOAD à l'aide des rôles IAM.

Il est recommandé d'associer des politiques d'autorisation à un rôle IAM, puis de l'attribuer à des utilisateurs et à des groupes, le cas échéant. Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift.

Intégration à AWS Secrets Manager

Vous pouvez récupérer vos informations d'identification de nom d'utilisateur et de mot de passe Redshift à partir d'un secret stocké dans AWS Secrets Manager. Pour fournir automatiquement les informations d'identification Redshift, utilisez le paramètre `secret.id`. Pour plus d'informations sur la création d'un secret d'informations d'identification Redshift, consultez Création d'un secret de base de données AWS Secrets Manager.

GroupID	ArtifactID	Révision(s) prise(s) en charge	Description
com.amazonaws.secretsmanager	aws-secretsmanager-jdbc	1,0,12	La bibliothèque de connexion AWS Secrets Manager SQL pour Java permet aux développeurs Java de se connecter facilement aux bases de données SQL à l'aide de secrets stockés dans AWS Secrets Manager.

> **Note**
>
> Remerciement : cette documentation contient des exemples de code et de langage développés par l'Apache Software Foundation dans le cadre de la licence Apache 2.0.

Améliorations des performances grâce au pushdown

Le connecteur Spark applique automatiquement le pushdown des prédicats et des requêtes pour optimiser les performances. Cela signifie que si vous utilisez une fonction prise en charge dans votre requête, le connecteur Spark transformera la fonction en requête SQL et exécutera la requête dans Amazon Redshift. Cette optimisation permet de récupérer moins de données et Apache Spark peut donc traiter moins de données et obtenir de meilleures performances. Par défaut, le pushdown est automatiquement activé. Pour le désactiver, définissez `autopushdown` sur false.

```
import sqlContext.implicits._val
 sample= sqlContext.read
    .format("io.github.spark_redshift_community.spark.redshift")
    .option("url",jdbcURL )
    .option("tempdir", tempS3Dir)
    .option("dbtable", "event")
    .option("autopushdown", "false")
    .load()
```

Les fonctions suivantes sont prises en charge avec le pushdown. Si vous utilisez une fonction qui ne figure pas dans cette liste, le connecteur Spark exécutera la fonction dans Spark au lieu d'Amazon Redshift, ce qui se traduira par des performances non optimisées. Pour une liste complète des fonctions de Spark, consultez la section Built-in Fonctions.

- Fonctions d'agrégation
  - avg
  - count
  - max
  - min
  - sum
  - stddev_samp
  - stddev_pop

  - var_samp
  - var_pop
- Opérateurs booléens
  - in
  - isnull
  - isnotnull
  - contient
  - endswith
  - startswith
- Opérateurs logiques
  - and
  - or
  - not (ou !)
- Fonctions mathématiques
  - +
  - -
  - *
  - /
  - - (unaire)
  - abs
  - acos
  - asin
  - atan
  - ceil
  - cos
  - exp
  - floor
  - greatest
  - least
  - log10

- pi
- pow
- round
- sin
- sqrt
- tan

- Fonctions diverses
  - cast
  - coalesce
  - decimal
  - if
  - in
- Opérateurs relationnels
  - !=
  - =
  - >
  - >=
  - <
  - <=
- Fonctions de chaîne
  - ascii
  - lpad
  - rpad
  - translate
  - upper
  - lower
  - longueur
  - trim
  - ltrim
  - rtrim

  - like
  - substring
  - concat
- Fonctions de date et d'heure
  - add_months
  - date
  - date_add
  - date_sub
  - date_trunc
  - timestamp
  - trunc
- Operations mathématiques
  - CheckOverflow
  - PromotePrecision
- Opérations relationnelles
  - Alias (par exemple, AS)
  - CaseWhen
  - Distinct
  - InSet
  - Jointures et jointures croisées
  - Restrictions
  - Unions, union all
  - ScalarSubquery
  - Sorts (par ordre croissant et décroissant)
  - UnscaledValue

Autres options de configuration

Vous trouverez sur cette page des descriptions des options que vous pouvez spécifier pour le connecteur Amazon Redshift Spark.

Taille maximale des colonnes de chaînes

Redshift crée des colonnes de chaîne sous forme de colonnes de texte lors de la création de tables, qui sont stockées en tant que VARCHAR(256). Si vous souhaitez que les colonnes prennent en charge de plus grandes tailles, vous pouvez utiliser maxlength pour spécifier la longueur maximale des colonnes de chaîne. Voici un exemple qui montre comment spécifier `maxlength`.

```
columnLengthMap.foreach { case (colName, length) =>
  val metadata = new MetadataBuilder().putLong("maxlength", length).build()
  df = df.withColumn(colName, df(colName).as(colName, metadata))
}
```

Type de colonne

Pour définir un type de colonne, utilisez le champ `redshift_type`.

```
columnTypeMap.foreach { case (colName, colType) =>
  val metadata = new MetadataBuilder().putString("redshift_type", colType).build()
  df = df.withColumn(colName, df(colName).as(colName, metadata))
}
```

Encodage de compression dans une colonne

Pour utiliser un encodage de compression spécifique sur une colonne, utilisez le champ d'encodage. Pour obtenir la liste complète des encodages de compression pris en charge, consultez Encodages de compression.

Description d'une colonne

Pour définir une description, utilisez le champ `description`.

Authentification entre Redshift et Amazon S3

Par défaut, le résultat est déchargé sur Amazon S3 au format Parquet. Pour décharger le résultat sous forme de fichier texte séparé par une barre verticale, spécifiez l'option suivante.

```
.option("unload_s3_format", "TEXT")
```

Instructions pushdown

Paramètre	Obligatoire	Par défaut	Description
spark.datasource.redshift.community.autopushdown.lazyMode	Non	True	Spécifie si le connecteur doit exécuter lentement les instructions pushdown Redshift. S'il a pour valeur true, le connecteur Spark récupère tous les modèles et informations associés avant d'exécuter la requête, ce qui permet généralement d'obtenir de meilleures performances. S'il a pour valeur false, le connecteur Spark exécute les instructions pushdown immédiatement dans le thread principal du pilote Spark et il est sérialisé entre les expressions.

Paramètres du connecteur

La carte des paramètres ou `OPTIONS` dans Spark SQL prend en charge les paramètres suivants.

Paramètre	Obligatoire	Par défaut	Description
dbtable	Oui, sauf si la requête est spécifiée	N/A	La table à partir duquel créer ou lire dans Redshift. Ce paramètre est requis lors du réenregis trement de données dans Redshift.
query	Oui, sauf si dbtable est spécifié	N/A	La requête à partir de laquelle lire dans Redshift.
user	Non	N/A	Le nom d'utilisa teur Redshift. Doit être utilisé avec le paramètre de mot de passe. Valide uniquement si l'utilisa teur et le mot de passe ne sont pas des paramètres dans l'URL. Utiliser les deux entraînera une erreur.
mot de passe	Non	N/A	Le mot de passe Redshift. Doit être utilisé avec le paramètre utilisate ur. Valide uniquemen t si l'utilisateur et le mot de passe ne sont pas des paramètres dans l'URL. Utiliser

Paramètre	Obligatoire	Par défaut	Description
			les deux entraînera une erreur.

Paramètre	Obligatoire	Par défaut	Description
url	Non	N/A	Une URL JDBC. Le format est jdbc:subprotocol : //host : ?port/database user=nom d'utilisateur&mot de passe = mot de passe. Le sous-protocole peut être postgresql ou Redshift, en fonction du pilote JDBC que vous avez chargé. Notez qu'un pilote compatible avec Redshift doit se trouver dans le chemin de classe et correspondre à cette URL. L'hôte et le port doivent pointer vers le nœud principal Redshift. Vous devez donc configurer les groupes de sécurité and/or VPC pour autoriser l'accès depuis votre application pilote. Database est le nom de la base de données Redshift.

Paramètre	Obligatoire	Par défaut	Description
			L'utilisateur et le mot de passe sont des informations d'identification pour accéder à la base de données. Ils doivent être intégrés à cette URL pour JDBC, et votre compte utilisateur doit disposer des autorisations nécessaires pour accéder à la table.
aws_iam_role	Uniquement si vous utilisez des rôles IAM pour autoriser les opérations Redshift COPY/UNLOAD	N/A	ARN entièrement spécifié du rôle IAM attaché au cluster Redshift.

Paramètre	Obligatoire	Par défaut	Description
forward_spark_s3_credentials	Non	False	Indique si cette bibliothèque doit découvrir automatiquement les informations d'identification que Spark utilise pour se connecter à Amazon S3 et s'il faut transmettre ces informations d'identification à Redshift via le pilote JDBC. Ces informations d'identification sont envoyées dans le cadre de la requête JDBC. Nous vous recommandons donc d'activer le chiffrement SSL avec une connexion JDBC lorsque vous utilisez cette option.
temporary_aws_access_key_id	Non	N/A	AWS clé d'accès. Vous devez disposer d'autorisations d'écriture sur le compartiment S3.
temporary_aws_secret_access_key	Non	N/A	AWS clé d'accès secrète correspondant à la clé d'accès.

Paramètre	Obligatoire	Par défaut	Description
temporary_aws_session_token	Non	N/A	AWS jeton de session correspondant à la clé d'accès fournie.
tempdir	Non	N/A	Emplacement accessible en écriture dans Amazon S3. Utilisé pour décharger des données lors de la lecture et charger les données Avro dans Redshift lors de l'écriture. Si vous utilisez une source de données Redshift pour Spark dans le cadre d'un pipeline ETL normal, il peut être utile de définir une politique de cycle de vie sur un compartiment et de l'utiliser comme emplacement temporaire pour ces données.

Paramètre	Obligatoire	Par défaut	Description
jdbcdriver	Non	Déterminé par le sous-protocole de l'URL JDBC	Nom de classe du pilote JDBC à utiliser. Cette classe doit se trouver sur le chemin de classe. Dans la plupart des cas, il ne devrait pas être nécessaire de spécifier cette option, car le nom de classe du pilote approprié doit être automatiq uement déterminé par le sous-protocole de l'URL JDBC.
diststyle	Non	Even	Styles de distribut ion Redshift à utiliser lors de la création d'une table. Les options valides sont EVEN, KEY ou ALL. Lorsque vous utilisez KEY, vous devez également définir une clé de distribution avec l'option distkey.
distkey	Non, sauf si vous utilisez DISTSTYLE _KEY	N/A	Nom d'une colonne de la table à utiliser comme clé de distribution lors de la création d'une table.

Paramètre	Obligatoire	Par défaut	Description
sortkeyspec	Non	N/A	Une définition complète des clés de tri Redshift.
include_column_list	Non	False	Indique si cette bibliothèque doit extraire automatiquement les colonnes du schéma et les ajouter à la commande COPY conformément aux options de mappage de colonnes.
description	Non	N/A	Description de la table. La description est définie avec la commande SQL COMMENT et apparaît dans la plupart des outils de requête. Consultez les métadonnées `description` pour définir des descriptions sur des colonnes individuelles.

Paramètre	Obligatoire	Par défaut	Description
preactions	Non	N/A	Une liste délimitée par des points-virgules de commandes SQL à exécuter avant de charger la commande COPY. Il peut être utile d'exécuter des commandes DELETE ou similaires avant de charger de nouvelles données. Si la commande contient %s, le nom de la table sera formaté avant l'exécution (si vous utilisez une table intermédiaire). Si cette commande échoue, elle est traitée comme une exception. Si vous utilisez une table intermédiaire, les modifications seront annulées et la table de sauvegarde sera restaurée si les actions préalables échouent.

Paramètre	Obligatoire	Par défaut	Description
extracopyoptions	Non	N/A	Liste d'options supplémentaires à ajouter à la commande Redshift COPY lors du chargement de données (par exemple `TRUNCATECOLUMNS` ou `MAXERROR n`). Consultez Paramètres facultatifs pour obtenir la liste complète des paramètres disponibles. Notez que ces options étant ajoutées à la fin de la commande `COPY`, vous ne pouvez utiliser que les options qui ont du sens à la fin de la commande. Cela devrait couvrir la plupart des cas d'utilisation possibles.

Paramètre	Obligatoire	Par défaut	Description
sse_kms_key	Non	N/A	ID de AWS KMS clé à utiliser pour le chiffrement côté serveur dans S3 lors de l'opération Redshift UNLOAD plutôt que pour le cryptage par défaut. AWS Le rôle IAM Redshift doit avoir accès à la clé KMS pour écrire avec elle et le rôle IAM Spark doit avoir accès à la clé pour les opérations de lecture. La lecture des données chiffrées ne nécessite aucune modification (AWS gère cela) tant que le rôle IAM de Spark dispose de l'accès approprié.

Paramètre	Obligatoire	Par défaut	Description
tempformat	Non	AVRO	Format dans lequel enregistrer les fichiers temporaires dans Amazon S3 lors de l'écriture dans Redshift. Les valeurs valides sont AVRO, CSV, CSV GZIP (CSV compressé) et PARQUET.
csvnullstring (expérimental)	Non	Null	La valeur de chaîne à écrire pour les valeurs nulles lors de l'utilisation de tempformat CSV. Il doit s'agir d'une valeur qui n'apparaît pas dans vos données réelles.

Paramètre	Obligatoire	Par défaut	Description
autopushdown	Non	True	Indique s'il faut appliquer le pushdown des prédicats et des requêtes en capturant et en analysant les plans logiques de Spark pour les opérations SQL. Les opérations sont traduites en une requête SQL, puis exécutées dans Redshift pour améliorer les performances.

Paramètre	Obligatoire	Par défaut	Description
autopushdown.s3_result_cache	Non	False	Mettez en cache la requête SQL pour décharger les données du mappage des chemins Amazon S3 en mémoire, afin que la même requête n'ait pas besoin de s'exécuter à nouveau dans la même session Spark. Uniquement pris en charge lorsque la fonction autopushdown est activée. Nous ne recommandons pas d'utiliser ce paramètre lorsque vous mélangez des opérations de lecture et d'écriture, car les résultats mis en cache peuvent contenir des informations périmées.

Paramètre	Obligatoire	Par défaut	Description
unload_s3_format	Non	Parquet	Format utilisé pour décharger les résultats de la requête. Les options valides sont Parquet et Text, qui indiquent de décharger les résultats de la requête dans un format de texte séparé par une barre verticale.
extraunloadoptions	Non	N/A	Options supplémentaires à ajouter à la commande Redshift UNLOAD. Le fonctionnement de toutes les options n'est pas garanti, car certaines d'entre elles peuvent entrer en conflit avec d'autres options définies dans le connecteur.
copydelay	Non	30 000	Le délai (en ms) entre les tentatives pour les opérations COPY de Redshift.
copyretrycount	Non	2	Nombre de tentatives d'opérations Redshift COPY.

Paramètre	Obligatoire	Par défaut	Description
tempdir_region	Non	N/A	La AWS région où `tempdir` se trouve. La définition de cette option améliore les performances du connecteur pour les interactions avec `tempdir` et fournit automatiq uement cette valeur dans le cadre des opérations COPY et UNLOAD au cours des opérations de lecture et d'écriture du connecteur. Ce paramètre est recommandé dans les situations suivantes : 1) Lorsque le connecteur fonctionn e en dehors de AWS, car la découverte automatique des régions échouera et affectera négativem ent les performances du connecteur. 2) Quand `tempdir` se trouve dans une autre région que

Paramètre	Obligatoire	Par défaut	Description
			le cluster Redshift, car l'utilisation de ce paramètre évite d'avoir à fournir la région manuellement à l'aide des paramètre s `extracopy options` et `extraunlo adoptions` . `tempdir` ne peut se trouver dans une autre région que le cluster Redshift lors de l'utilisation de `PARQUET` en tant que `tempformat` même si cela utilise ce paramètre. 3) Lorsque le connecteur fonctionn e dans une région différente de `tempdir`, car cela améliore les performan ces d'accès du connecteur à `tempdir`.

Paramètre	Obligatoire	Par défaut	Description
secret.id	Non	N/A	Nom ou ARN de votre secret stocké dans AWS Secrets Manager. Vous pouvez utiliser ce paramètre pour fournir automatiquement les informations d'identification Redshift, mais uniquement si les informations d'identification d'utilisateur, de mot de passe et `DbUser` ne sont pas transmises dans l'URL JDBC ni sous la forme d'autres options.

Paramètre	Obligatoire	Par défaut	Description
secret.region	Non	N/A	AWS Région principale, telle que USA Est (Virginie du Nord), dans laquelle rechercher la `secret.id` valeur. Si vous ne spécifiez pas cette région, le connecteur essaiera d'utiliser la chaîne de fournisseur d'informations d'identification par défaut pour résoudre la région de `secret.id` . Dans certains cas, par exemple si vous utilisez le connecteur en dehors d'AWS, le connecteur ne pourra pas trouver la région. Nous recommandons l'utilisation de ce paramètre dans les situations suivantes : 1) Lorsque le connecteur fonctionne en dehors de AWS, car la découverte automatique de la région échouera et empêchera

Paramètre	Obligatoire	Par défaut	Description
			l'authentification avec Redshift Lorsque le connecteur s'exécute dans une région différente de `secret.id`, car cela améliore les performances d'accès du secret du connecteur.
secret.vpc EndpointUrl	Non	N/A	URL du point de terminaison PrivateLink DNS à utiliser AWS Secrets Manager lors du remplacement de la chaîne de fournisseurs d'informations d'identification par défaut.
secret.vpc EndpointRegion	Non	N/A	La région de point de terminaison PrivateLink DNS à utiliser AWS Secrets Manager lors du remplacement de la chaîne de fournisseurs d'informations d'identification par défaut.

Paramètre	Obligatoire	Par défaut	Description
jdbc.*	Non	N/A	Paramètres supplémentaires à transmettre au pilote JDBC sous-jacent quand le caractère générique est le nom du paramètre JDBC, tels que jdbc.ssl. Notez que le préfixe `jdbc` sera supprimé avant d'être transmis au pilote JDBC. Pour voir toutes les options possibles pour le pilote JDBC Redshift, consultez Options de configuration du pilote JDBC version 2.x.

Paramètre	Obligatoire	Par défaut	Description
étiquette	Non	" "	Identifiant à inclure dans le groupe de requêtes défini lors de l'exécuti on de requêtes avec le connecteu r. Doit comporter 100 caractères ou moins, et tous les caractères doivent être des `unicodeId entifierParts` valides. Si votre identifiant comporte plus de 100 caractère s, l'excédent est supprimé. Lors de l'exécution d'une requête avec le connecteur, le groupe de requêtes est défini sous la forme d'une chaîne au format JSON, telle que `{"spark-r edshift-c onnector" :{"svc":" ","ver":" 5.1.0-amzn-1- spark_3.3","op ":"Read", "lbl":""}}`)

Paramètre	Obligatoire	Par défaut	Description
			. Cette option remplace la valeur de la clé `lbl`.

> **Note**
>
> Remerciement : cette documentation contient des exemples de code et de langage développés par l'Apache Software Foundation dans le cadre de la licence Apache 2.0.

Types de données pris en charge

Les types de données suivants dans Amazon Redshift sont pris en charge par le connecteur Spark. Pour obtenir la liste complète des types de données pris en charge dans Amazon Redshift, consultez Types de données. Si un type de données ne figure pas dans la table ci-dessous, il n'est pas pris en charge dans le connecteur Spark.

Type de données	les alias ;
SMALLINT	INT2
INTEGER	INT, INT4
BIGINT	INT8
DECIMAL	NUMERIC
REAL	FLOAT4
DOUBLE PRECISION	FLOAT8, FLOAT
BOOLEAN	BOOL
CHAR	CHARACTER, NCHAR, BPCHAR
VARCHAR	CHARACTER VARYING, NVARCHAR, TEXT

Type de données	les alias ;
DATE	
TIMESTAMP	Horodatage sans fuseau horaire
TIMESTAMPTZ	Horodatage avec fuseau horaire
SUPER	
TIME	Heure sans fuseau horaire
TIMETZ	Heure avec fuseau horaire
VARBYTE	VARBINARY, BINARY VARYING

Types de données complexes

Vous pouvez utiliser le connecteur Spark pour lire et écrire des types de données complexes Spark tels que `ArrayType`, `MapType` et `StructType` vers et depuis les colonnes de type de données Redshift SUPER. Si vous fournissez un schéma lors d'une opération de lecture, les données de la colonne sont converties dans les types complexes correspondants dans Spark, y compris les types imbriqués. De plus, si `autopushdown` est activé, la projection des attributs imbriqués, des valeurs de mappage et des indices de tableau est transférée vers Redshift afin qu'il ne soit plus nécessaire de décharger l'intégralité de la structure de données imbriquée lors de l'accès à une simple partie des données.

Lorsque vous écrivez DataFrames à partir du connecteur, n'importe quelle colonne de type `MapType` (utilisant`StringType`) ou `ArrayType` est écrite dans une colonne de type de données Redshift SUPER. `StructType` Lors de l'écriture de ces structures de données imbriquées, le paramètre `tempformat` doit être de type `CSV`, `CSV GZIP` ou `PARQUET`. L'utilisation de `AVRO` provoquera une exception. L'écriture d'une structure de données `MapType` dont le type de clé est autre que `StringType` provoquera également une exception.

StructType

L'exemple suivant montre comment créer une table avec un type de données SUPER contenant une structure.

```
create table contains_super (a super);
```

Vous pouvez ensuite utiliser le connecteur pour interroger un champ `StringType` `hello` à partir de la colonne SUPER a dans la table en utilisant un schéma comme dans l'exemple suivant.

```
import org.apache.spark.sql.types._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", StructType(StructField("hello",
 StringType) ::Nil)) :: Nil)

val helloDF = sqlContext.read
.format("io.github.spark_redshift_community.spark.redshift")
.option("url", jdbcURL )
.option("tempdir", tempS3Dir)
.option("dbtable", "contains_super")
.schema(schema)
.load().selectExpr("a.hello")
```

L'exemple suivant montre comment écrire une structure dans la colonne a.

```
import org.apache.spark.sql.types._
import org.apache.spark.sql._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", StructType(StructField("hello",
 StringType) ::Nil)) :: Nil)
val data = sc.parallelize(Seq(Row(Row("world"))))
val mydf = sqlContext.createDataFrame(data, schema)

mydf.write.format("io.github.spark_redshift_community.spark.redshift").
option("url", jdbcUrl).
option("dbtable", tableName).
option("tempdir", tempS3Dir).
option("tempformat", "CSV").
mode(SaveMode.Append).save
```

MapType

Si vous préférez utiliser `MapType` pour représenter vos données, vous pouvez utiliser une structure de données `MapType` dans votre schéma et récupérer la valeur correspondant à une clé dans le mappage. Notez que toutes les clés de votre structure de données `MapType` doivent être de type String et que toutes les valeurs doivent être du même type, par exemple int.

L'exemple suivant montre comment obtenir la valeur de la clé `hello` dans la colonne `a`.

```
import org.apache.spark.sql.types._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", MapType(StringType, IntegerType))::Nil)

val helloDF = sqlContext.read
    .format("io.github.spark_redshift_community.spark.redshift")
    .option("url", jdbcURL )
    .option("tempdir", tempS3Dir)
    .option("dbtable", "contains_super")
    .schema(schema)
    .load().selectExpr("a['hello']")
```

ArrayType

Si la colonne contient un tableau à la place d'une structure, vous pouvez utiliser le connecteur pour interroger le premier élément du tableau.

```
import org.apache.spark.sql.types._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", ArrayType(IntegerType)):: Nil)

val helloDF = sqlContext.read
    .format("io.github.spark_redshift_community.spark.redshift")
    .option("url", jdbcURL )
    .option("tempdir", tempS3Dir)
    .option("dbtable", "contains_super")
    .schema(schema)
```

```
    .load().selectExpr("a[0]")
```

Limitations

L'utilisation de types de données complexes avec le connecteur Spark présente les limites suivantes :

- Tous les noms des champs de structure imbriqués et les clés de mappage doivent être en minuscules. Si vous effectuez une requête pour obtenir les noms de champs complexes avec des lettres majuscules, vous pouvez essayer d'omettre le schéma et d'utiliser la fonction Spark `from_json` pour convertir la chaîne renvoyée localement comme solution de contournement.
- Tous les champs de mappage utilisés dans les opérations de lecture et d'écriture doivent contenir uniquement des clés `StringType`.
- Seuls `CSV`, `CSV GZIP` et `PARQUET` sont des valeurs tempformat prises en charge pour l'écriture de types complexes dans Redshift. Une tentative d'utilisation de `AVRO` lèvera une exception.

Configuration d’une connexion pour le pilote ODBC version 2.x pour Amazon Redshift

Vous pouvez utiliser une connexion ODBC pour vous connecter à votre cluster Amazon Redshift à partir de nombreux outils et applications clients SQL tiers. Si votre outil client prend en charge JDBC, vous pouvez choisir d’utiliser ce type de connexion plutôt qu’ODBC en raison de la simplicité de configuration offerte par JDBC. Toutefois, si votre outil client ne prend pas en charge JDBC, vous pouvez suivre les étapes de cette section pour configurer une connexion ODBC sur votre ordinateur client ou sur votre instance Amazon EC2.

Amazon Redshift fournit des pilotes ODBC 64 bits pour les systèmes d'exploitation Linux, Windows et Mac ; les pilotes ODBC 32 bits ne sont plus disponibles. Aucune mise à jour des pilotes ODBC 32 bits ne sera publiée, sauf pour les correctifs de sécurité urgents.

Pour obtenir les dernières informations sur les modifications du pilote ODBC, consulter le journal des modifications.

Rubriques

- Obtention de l’URL ODBC
- Utilisation d’un pilote ODBC Amazon Redshift sur Microsoft Windows
- Utilisation d’un pilote ODBC Amazon Redshift sous Linux
- Utilisation d'un pilote ODBC Amazon Redshift sur Apple macOS

- Méthodes d'authentification
- Conversions du type de données
- Options du pilote ODBC
- Versions antérieures du pilote ODBC
- Différences entre les versions 2.x et 1.x du pilote ODBC

Obtention de l'URL ODBC

Amazon Redshift affiche l'URL ODBC de votre cluster dans la console Amazon Redshift. Cette URL contient les informations nécessaires pour configurer la connexion entre votre ordinateur client et la base de données.

Une URL ODBC a le format suivant :

```
Driver={driver}; Server=endpoint_host; Database=database_name; UID=user_name;
 PWD=password; Port=port_number
```

Les champs du format précédent ont les valeurs suivantes :

Champ	Value
Driver	Nom du pilote ODBC 64 bits à utiliser : Pilote ODBC Amazon Redshift (x64).
Server	L'hôte du point de terminaison du cluster Amazon Redshift.
Database	Base de données que vous avez créée pour votre cluster.
UID	Nom d'utilisateur d'un compte utilisateur de la base de données autorisé à se connecter à la base de données. Bien que cette valeur soit une autorisation de niveau base de données, et non une autorisation de niveau cluster, vous pouvez utiliser le compte administrateur Redshift que vous avez configuré lorsque vous avez lancé le cluster.
PWD	Mot de passe du compte utilisateur de la base de données vous permettant de vous connecter à la base de données.

Champ	Value
Port	Numéro du port que vous avez spécifié lorsque vous avez lancé le cluster. Si vous avez un pare-feu, vérifiez que ce port est ouvert pour que vous l'utilisiez.

Voici un exemple d'URL ODBC :

```
Driver={Amazon Redshift ODBC Driver (x64)}; Server=examplecluster.abc123xyz789.us-
west-2.redshift.amazonaws.com; Database=dev; UID=adminuser;
 PWD=insert_your_admin_user_password_here; Port=5439
```

Pour plus d'informations sur l'emplacement de l'URL ODBC, consultez Recherche de votre chaîne de connexion au cluster.

Utilisation d'un pilote ODBC Amazon Redshift sur Microsoft Windows

Vous devez installer le pilote ODBC Amazon Redshift sur les ordinateurs clients accédant à un entrepôt des données Amazon Redshift. Pour chaque ordinateur sur lequel vous installez le pilote, les exigences minimales suivantes sont requises :

- Droits d'administrateur sur l'ordinateur.
- L'ordinateur répond à la configuration du système requise suivante :
  - L'un des systèmes d'exploitation suivants :
    - Windows 10 ou 8.1.
    - Windows Server 2025, 2022, 2019, 2016 ou 2012.
  - 100 Mo d'espace disque disponible.
  - Visual C++ Redistributable pour Visual Studio 2015 pour Windows 64 bits installé. Vous pouvez télécharger le package d'installation sur le site web de Microsoft Download Visual C++ Redistributable for Visual Studio 2022 (Télécharger Visual C++ redistribuable pour Visual Studio 2022).

Téléchargement et installation du pilote ODBC Amazon Redshift

Utilisez la procédure suivante pour télécharger et installer le pilote ODBC Amazon Redshift pour les systèmes d'exploitation Windows. N'utilisez un pilote différent que si vous exécutez une application

tierce qui est certifiée pour être utilisée avec Amazon Redshift, et que cette application nécessite ce pilote spécifique.

Pour télécharger et installer le pilote ODBC :

1. Téléchargez le pilote suivant : pilote ODBC 64 bits version 2.2.4.0 Dans la région de Chine (Pékin), utilisez le lien suivant : pilote version 2.2.4.0

   Le nom de ce pilote est Pilote ODBC Amazon Redshift (x64).
2. Vérifiez la licence de la version 2.x du pilote ODBC Amazon Redshift.
3. Double-click le fichier .msi, puis suivez les étapes de l'assistant pour installer le pilote.

Création d’une entrée du nom de la source de données (DSN) système pour une connexion ODBC

Après avoir téléchargé et installé le pilote ODBC, ajoutez une entrée de nom de source de données (DSN) à l’ordinateur client ou à l’instance Amazon EC2. Les outils clients SQL peuvent utiliser cette source de données pour se connecter à la base de données Amazon Redshift.

Nous vous recommandons de créer un DSN système au lieu d’un DSN utilisateur. Certaines applications chargent les données à l’aide d’un compte utilisateur de la base de données différent et peuvent ne pas être en mesure de détecter les DSN utilisateur créés sous un autre compte d’utilisateur de la base de données.

> **Note**
>
> Pour l'authentification à l'aide des informations d'identification Gestion des identités et des accès AWS (IAM) ou des informations d'identification du fournisseur d'identité (IdP), des étapes supplémentaires sont requises. Pour plus d’informations, consultez Configurer une connexion JDBC ou ODBC pour utiliser des informations d’identification IAM.

Pour créer une entrée DSN système pour une connexion ODBC :

1. Dans le menu Start (Démarrer) saisissez « Sources de données ODBC ». Choisissez ODBC Data sources (Sources de données ODBC).

   Veillez à choisir l’administrateur de sources de données ODBC qui a le même bitness que l’application client que vous utilisez pour vous connecter à Amazon Redshift.

2. Dans l'administrateur de source de données ODBC, choisissez l'onglet Driver (Pilote) et recherchez le dossier du pilote suivant : Pilote ODBC Amazon Redshift (x64).
3. Sélectionnez l'onglet DSN système pour configurer le pilote pour tous les utilisateurs sur l'ordinateur ou l'onglet DSN utilisateur pour configurer le pilote correspondant à votre compte utilisateur de la base de données uniquement.
4. Choisissez Ajouter. La fenêtre Créer une nouvelle source de données s'ouvre.
5. Choisissez le pilote ODBC Amazon Redshift (x64), puis cliquez sur Finish (Terminer). La fenêtre Amazon Redshift ODBC Driver DSN Setup (Configuration DSN du pilote ODBC Amazon Redshift) s'ouvre.
6. Sous la section Connection Settings (Paramètres de connexion), saisissez les informations suivantes :
   - Nom de la source de données

     Entrez un nom pour la source de données. Par exemple, si vous avez suivi le Guide de démarrage d'Amazon Redshift, vous pouvez taper `exampleclusterdsn` pour faciliter la mémorisation du cluster que vous associez à ce DSN.
   - Serveur

     Spécifiez l'hôte du point de terminaison de votre cluster Amazon Redshift. Vous trouverez ces informations dans la console Amazon Redshift sur la page des détails du cluster. Pour plus d'informations, consultez Configuration des connexions dans Amazon Redshift.
   - Port

     Entrez le numéro de port utilisé par la base de données. En fonction du port que vous avez sélectionné lors de la création, de la modification ou de la migration du cluster, autorisez l'accès au port sélectionné.
   - Base de données

     Saisissez le nom de la base de données Amazon Redshift. Si vous avez lancé votre cluster sans spécifier de nom de base de données, entrez `dev`. Sinon, utilisez le nom que vous avez choisi pendant le processus de lancement. Si vous avez suivi les étapes de Guide de démarrage d'Amazon Redshift, saisissez `dev`.
7. Sous la section Authentication (Authentification), spécifiez les options de configuration pour configurer l'authentification standard ou IAM.
8. Choisissez SSL Options (Options SSL) et spécifiez une valeur pour les éléments suivants :
   - Mode d'authentification

Sélectionnez un mode de traitement SSL (Secure Sockets Layer). Dans un environnement de test, vous pouvez utiliser `prefer`. Cependant, pour les environnements de production et lorsque l'échange de données sécurisé est nécessaire, utilisez `verify-ca` ou `verify-full`.

- TLS min

  Vous pouvez éventuellement choisir la version minimale TLS/SSL que le pilote autorise le magasin de données à utiliser pour chiffrer les connexions. Par exemple, si vous spécifiez TLS 1.2, TLS 1.1 ne peut pas être utilisé pour chiffrer des connexions. La version par défaut est TLS 1.2.

9. Dans l'onglet Proxy, spécifiez tout paramètre de connexion du proxy.
10. Dans l'onglet Cursor (Curseur), spécifiez des options de renvoi des résultats de la requête à votre outil ou application cliente SQL.
11. Dans Options avancées, spécifiez les valeurs de `logLevel`, `logPath`, `compression` et d'autres options.
12. Sélectionnez Tester). Si l'ordinateur client peut se connecter à la base de données Amazon Redshift, le message suivant apparaît : Connexion réussie. Si l'ordinateur client ne parvient pas à se connecter à la base de données, vous pouvez résoudre les problèmes éventuels en générant un fichier journal et en contactant le AWS support. Pour plus d'informations sur la génération de journaux, consultez (LIEN).
13. Choisissez OK.

Utilisation d'un pilote ODBC Amazon Redshift sous Linux

Vous devez installer le pilote ODBC Amazon Redshift sur les ordinateurs clients accédant à un entrepôt des données Amazon Redshift. Pour chaque ordinateur sur lequel vous installez le pilote, les exigences minimales suivantes sont requises :

- Accès root sur la machine.
- Une des distributions suivantes :
  - Amazon Linux 2
  - Amazon Linux 2023
  - Red Hat® Enterprise Linux® (RHEL) 8 ou version ultérieure
  - CentOS 8 ou version ultérieure
  - Debian 11 ou version ultérieure

- 150 Mo d’espace disque disponible.
- unixODBC 2.2.14 ou version ultérieure.
- glibc 2.26 ou version ultérieure.

Téléchargement et installation du pilote ODBC Amazon Redshift

Pour télécharger et installer le pilote ODBC version 2.x Amazon Redshift pour Linux :

1. Téléchargez le pilote suivant :
   - Version 2.2.4.0 du pilote RPM x86 64 bits 2.2.4.0
     -
     -
   - Version 2.2.4.0 du pilote RPM ARM 64 bits 2.2.4.0
     -
     -
   - Version 2.2.4.0 du pilote DEB x86 64 bits 2.2.4.0
     -
     -
   - Version 2.2.4.0 du pilote DEB ARM 64 bits 2.2.4.0
     -
     -

   > **Note**
   >
   > Les pilotes ODBC 32 bits sont interrompus. D’autres mises à jour ne seront pas publiées, sauf pour les correctifs de sécurité urgents.

2. Avant l'installation, vérifiez que le package du pilote est AWS signé. Après avoir téléchargé le package, sa clé de signature (certificat) et son hachage signé (signature détachée), exécutez les commandes suivantes :

```
openssl x509 -in SignatureKeyFile -pubkey -noout > redshift-odbc-pubkey.pem
openssl dgst -sha256 -verify redshift-odbc-pubkey.pem \
    -signature SignedHashFile \
    PackageFile
```

Si le colis est authentique, `openssl` imprime`Verified OK`. Si le résultat est autre chose, n'installez pas le package. Re-download les fichiers ou contactez le AWS Support.

Par exemple, pour vérifier le RPM x86 64 bits :

```
openssl x509 -in AmazonRedshiftODBC-64-bit-2.2.4.0.x86_64-certificate.pem -pubkey -
noout > redshift-odbc-pubkey.pem
openssl dgst -sha256 -verify redshift-odbc-pubkey.pem \
    -signature AmazonRedshiftODBC-64-bit-2.2.4.0.x86_64-signature.bin \
    AmazonRedshiftODBC-64-bit-2.2.4.0.x86_64.rpm
```

3. Accédez à l'emplacement dans lequel vous avez téléchargé le package et exécutez l'une des commandes suivantes. Utilisez la commande qui correspond à votre distribution Linux.

   Sur les systèmes d'exploitation RHEL et CentOS (RPM), exécutez la commande suivante :

   ```
   sudo yum --nogpgcheck localinstall RPMFileName
   ```

   Remplacez `RPMFileName` par le nom du fichier de package RPM. Par exemple, la commande suivante illustre l'installation du pilote 64 bits :

   ```
   sudo yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-2.x.xx.xxxx.x86_64.rpm
   ```

   Sur les systèmes d'exploitation Debian et Ubuntu (DEB), accédez au répertoire contenant le fichier .deb téléchargé et exécutez la commande suivante :

   ```
   sudo apt install ./DEBFileName
   ```

   Remplacez `DEBFileName` par le nom du fichier du package DEB. Par exemple :

   ```
   sudo apt install ./AmazonRedshiftODBC-64-bit-2.x.xx.xxxx.amd64.deb
   ```

Utilisation d’un gestionnaire de pilotes ODBC pour configurer le pilote ODBC

Sur Linux, vous utilisez un gestionnaire de pilotes ODBC pour configurer les paramètres de connexion ODBC. Les gestionnaires de pilotes ODBC utilisent des fichiers de configuration pour définir et configurer les pilotes et les sources de données ODBC. Le gestionnaire de pilotes ODBC que vous utilisez s’appuie sur le système d’exploitation que vous utilisez.

Configuration du pilote ODBC à l’aide du gestionnaire de pilotes unixODBC

Les fichiers suivants sont nécessaires pour configurer le pilote ODBC Amazon Redshift :

- `amazon.redshiftodbc.ini`
- `odbc.ini`
- `odbcinst.ini`

Si vous l’avez installé à l’emplacement par défaut, le fichier de configuration `amazon.redshiftodbc.ini` se trouve dans `/opt/amazon/redshiftodbcx64`.

De plus, sous `/opt/amazon/redshiftodbcx64`, vous pouvez trouver un exemple `odbc.ini` et des fichiers `odbcinst.ini`. Vous pouvez utiliser ces fichiers comme exemples pour configurer le pilote ODBC Amazon Redshift et le nom de la source de données (DSN).

Nous ne recommandons pas d’utiliser le répertoire d’installation du pilote ODBC d’Amazon Redshift pour les fichiers de configuration. Les fichiers d’exemple du répertoire installé sont proposés à titre d’exemple seulement. Si vous réinstallez le pilote ODBC Amazon Redshift ultérieurement, ou si vous effectuez une mise à niveau vers une version plus récente, le répertoire d’installation est écrasé. Vous perdez toute modification que vous avez pu apporter aux fichiers du répertoire d’installation.

Pour éviter cela, copiez le fichier `amazon.redshiftodbc.ini` dans un répertoire autre que le répertoire d’installation. Si vous copiez ce fichier vers le répertoire de base de l’utilisateur, ajouter un point (.) au début du nom de fichier pour le masquer.

Pour les fichiers `odbc.ini` et `odbcinst.ini`, utilisez les fichiers de configuration dans le répertoire personnel de l’utilisateur ou créez de nouvelles versions dans un autre répertoire. Par défaut, votre système d’exploitation Linux doit avoir un fichier `odbc.ini` et un fichier `odbcinst.ini` dans le répertoire personnel de l’utilisateur (`/home/$USER` ou `~/.`). Ces fichiers par défaut sont des fichiers cachés, ce qui est indiqué par le point (.) devant chaque nom de fichier. Ces fichiers s’affichent uniquement lorsque vous utilisez l’indicateur `-a` pour répertorier le contenu du répertoire.

Quelle que soit l'option choisie pour les fichiers `odbc.ini` et `odbcinst.ini`, modifiez les fichiers pour ajouter les informations de configuration du pilote et du DSN. Si vous avez choisi de créer de nouveaux fichiers, vous devez également définir des variables d'environnement afin de spécifier l'emplacement dans lequel se trouvent ces fichiers de configuration.

Par défaut, les gestionnaires de pilotes ODBC sont configurés pour utiliser les versions cachées des fichiers de configuration `odbc.ini` et `odbcinst.ini` (nommés `.odbc.ini` et `.odbcinst.ini`) situés dans le répertoire de base. Ils sont également configurés pour utiliser le fichier `amazon.redshiftodbc.ini` dans le répertoire d'installation du pilote. Si vous stockez ces fichiers de configuration ailleurs, définissez les variables d'environnement décrites ci-dessous afin que le gestionnaire de pilotes puisse localiser les fichiers.

Si vous utilisez unixODBC, procédez comme suit :

- Définissez `ODBCINI` vers le chemin complet et le nom du fichier `odbc.ini`.
- Définissez `ODBCSYSINI` vers le chemin complet du répertoire qui contient le fichier `odbcinst.ini`.
- Définissez `AMAZONREDSHIFTODBCINI` vers le chemin complet et le nom du fichier `amazon.redshiftodbc.ini`.

Voici un exemple de configuration des valeurs ci-dessus :

```
export ODBCINI=/usr/local/odbc/odbc.ini
export ODBCSYSINI=/usr/local/odbc
export AMAZONREDSHIFTODBCINI=/etc/amazon.redshiftodbc.ini
```

Configuration d'une connexion à l'aide d'un nom de source de données (DSN) sur Linux

Lorsque vous vous connectez à votre magasin de données à l'aide d'un nom de source de données (DSN), configurez le fichier `odbc.ini` pour définir des noms de source de données (DSN). Définissez les propriétés du fichier `odbc.ini` pour créer un DSN qui spécifie les informations de connexion pour votre magasin de données.

Sur les systèmes d'exploitation Linux, utilisez le format suivant :

```
[ODBC Data Sources]
driver_name=dsn_name
```

```
[dsn_name]
Driver=path/driver_file
Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

L'exemple suivant illustre la configuration du fichier `odbc.ini` à l'aide du pilote ODBC 64 bits sur les systèmes d'exploitation Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x64=Amazon Redshift ODBC Driver (x64)

[Amazon_Redshift_x64]
Driver=/opt/amazon/redshiftodbcx64/librsodbc64.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932Database=dev
locale=en-US
```

Configuration d'une connexion sans DSN sur Linux

Pour vous connecter à votre magasin de données via une connexion qui n'a pas de DSN, définissez le pilote dans le fichier `odbcinst.ini`. Entrez ensuite une chaîne de DSN-less connexion dans votre application.

Sur les systèmes d'exploitation Linux, utilisez le format suivant :

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file

...
```

L'exemple suivant illustre la configuration du fichier `odbcinst.ini` à l'aide du pilote ODBC 64 bits sur les systèmes d'exploitation Linux.

```
[ODBC Drivers]
Amazon Redshift ODBC Driver (x64)=Installed

[Amazon Redshift ODBC Driver (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftodbcx64/librsodbc64.so
```

Utilisation d'un pilote ODBC Amazon Redshift sur Apple macOS

Vous devez installer le pilote ODBC Amazon Redshift sur les ordinateurs clients accédant à un entrepôt des données Amazon Redshift. Pour chaque ordinateur sur lequel vous installez le pilote, voici la configuration minimale requise :

- Accès root sur la machine.
- Configuration système requise pour Apple macOS :
  - Une version 64 bits d'Apple macOS version 11.7 ou ultérieure (telle que Apple macOS Big Sur, Monterey, Ventura ou version ultérieure) est requise. Le pilote ODBC Redshift ne prend en charge que les applications clientes 64 bits.
  - 150 Mo d'espace disque disponible.
  - Le pilote prend en charge les applications créées avec iODBC 3.52.9+ ou UnixODBC 2.3.7+.

Téléchargement et installation du pilote ODBC Amazon Redshift

Suivez la procédure ci-dessous pour télécharger et installer le pilote ODBC Amazon Redshift sur Apple macOS. N'utilisez un pilote différent que si vous exécutez une application tierce qui est certifiée pour être utilisée avec Amazon Redshift, et que cette application nécessite ce pilote spécifique.

Pour télécharger et installer le pilote ODBC :

1. Téléchargez le pilote suivant : pilote ODBC 64 bits version 2.2.4.0 Dans la région de Chine (Pékin), utilisez le lien suivant : pilote version 2.2.4.0

   Ce pilote est pris en charge sur les architectures x86_64 et arm64. Le nom de ce pilote est Pilote ODBC Amazon Redshift (x64).

2. Vérifiez la licence de la version 2.x du pilote ODBC Amazon Redshift.
3. Double-click le fichier .pkg, puis suivez les étapes de l'assistant pour installer le pilote. Vous pouvez également exécuter la commande suivante :

```
sudo installer -pkg PKGFileName -target /
```

Remplacez `PKGFileName` par le nom du fichier du package pkg. Par exemple, la commande suivante illustre l'installation du pilote 64 bits :

```
sudo installer -pkg ./AmazonRedshiftODBC-64-bit.X.X.XX.X.universal.pkg -target /
```

Utilisation d'un gestionnaire de pilotes ODBC pour configurer le pilote ODBC

Sur Mac, vous utilisez un gestionnaire de pilotes ODBC pour configurer les paramètres de connexion ODBC. Les gestionnaires de pilotes ODBC utilisent des fichiers de configuration pour définir et configurer les pilotes et les sources de données ODBC. Le gestionnaire de pilotes ODBC que vous utilisez s'appuie sur le système d'exploitation que vous utilisez.

Configuration du pilote ODBC à l'aide du gestionnaire de pilotes IODBC ou UnixODBC

Les fichiers suivants sont nécessaires pour configurer le pilote ODBC Amazon Redshift :

- `amazon.redshiftodbc.ini`
- `odbc.ini`
- `odbcinst.ini`

Si vous l'avez installé à l'emplacement par défaut, le fichier de configuration `amazon.redshiftodbc.ini` se trouve dans `/opt/amazon/redshiftodbcx64`.

De plus, sous `/opt/amazon/redshiftodbcx64`, vous pouvez trouver un exemple `odbc.ini` et des fichiers `odbcinst.ini`. Vous pouvez utiliser ces fichiers comme exemples pour configurer le pilote ODBC Amazon Redshift et le nom de la source de données (DSN). Les fichiers d'exemple du répertoire installé sont proposés à titre d'exemple seulement.

Nous ne recommandons pas d'utiliser le répertoire d'installation du pilote ODBC d'Amazon Redshift pour les fichiers de configuration. Si vous réinstallez le pilote ODBC Amazon Redshift ultérieurement, ou si vous effectuez une mise à niveau vers une version plus récente, le répertoire d'installation

est écrasé. Vous perdez toute modification que vous avez pu apporter aux fichiers du répertoire d'installation.

Pour éviter cela, copiez les `odbc.ini` `amazon.redshiftodbc.ini` fichiers `odbcinst.ini` et dans un répertoire autre que le répertoire d'installation. Si vous copiez ces fichiers dans le répertoire personnel de l'utilisateur, ajoutez un point (.) au début de ces noms de fichiers pour en faire un fichier masqué.

Modifiez les fichiers pour ajouter des informations de configuration DSN. Lorsque vous créez de nouveaux fichiers, vous devez également définir des variables d'environnement pour spécifier l'emplacement de ces fichiers de configuration.

Voici un exemple de définition des variables d'environnement :

```
export ODBCINI=/Library/ODBC/odbc.ini
export ODBCSYSINI=/Library/ODBC
export ODBCINSTINI=${ODBCSYSINI}/odbcinst.ini
```

Pour les applications en ligne de commande : ajoutez les commandes d'exportation à votre fichier de démarrage du shell (par exemple, `~/.bash_profile` ou`~/.zshrc`).

Pour la version prise en charge du gestionnaire de pilotes, voir ici

Configuration d'une connexion à l'aide d'un nom de source de données (DSN) sur Apple macOS

Lorsque vous vous connectez à votre magasin de données à l'aide d'un nom de source de données (DSN), configurez le fichier `odbc.ini` pour définir des noms de source de données (DSN). Définissez les propriétés du `odbc.ini` fichier pour créer un DSN qui spécifie les informations de connexion pour votre entrepôt de données Redshift.

Sur Apple macOS, utilisez le format suivant :

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/driver_file
Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

L'exemple suivant montre la configuration `odbc.ini` avec le pilote ODBC 64 bits sur Apple macOS.

```
[ODBC Data Sources]
Amazon_Redshift_x64=Amazon Redshift ODBC Driver (x64)

[Amazon_Redshift_x64]
Driver=/opt/amazon/redshiftodbcx64/librsodbc64.dylib
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US
```

Configuration d'une connexion sans DSN sur Apple macOS

Pour vous connecter à votre entrepôt de données Redshift via une connexion sans DSN, définissez le pilote dans le fichier. `odbcinst.ini` Entrez ensuite une chaîne de DSN-less connexion dans votre application.

Sur Apple macOS, utilisez le format suivant :

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file

...
```

L'exemple suivant montre la configuration `odbcinst.ini` avec le pilote ODBC 64 bits sur Apple macOS.

```
[ODBC Drivers]
Amazon Redshift ODBC Driver (x64)=Installed

[Amazon Redshift ODBC Driver (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftodbcx64/librsodbc64.dylib
```

Méthodes d’authentification

Pour protéger les données contre les accès non autorisés, les magasins de données Amazon Redshift exigent que toutes les connexions soient authentifiées à l’aide des informations d’identification de l’utilisateur.

La table suivante illustre les options de connexion obligatoires et facultatives pour chaque méthode d’authentification pouvant être utilisée pour se connecter au pilote ODBC Amazon Redshift version 2.x :

Méthode d’authentification	Obligatoire	Facultatif
Standard	• Host (Hôte) • Port • Base de données • UID • Mot de passe	
Profil IAM	• Host (Hôte) • Port • Base de données • IAM • Profil	• ClusterID • Région • AutoCreate • EndpointURL • StsEndpointURL • InstanceProfile **Note** Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.

Méthode d’authentification	Obligatoire	Facultatif
Informations d’identification IAM	• Host (Hôte) • Port • Base de données • IAM • AccessKeyID • SecretAccessKey	• ClusterID • Région • AutoCreate • EndpointURL • StsEndpointURL • SessionToken • UID **Note** Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.

Méthode d'authentification	Obligatoire	Facultatif
AD FS	• Host (Hôte) • Port • Base de données • IAM • plugin_name • UID • Mot de passe • IdP_Host • IdP_Port	• ClusterID • Région • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • se connecter ToRp • SSL_Insecure **Note** Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.

Méthode d'authentification	Obligatoire	Facultatif
Azure AD	• Host (Hôte) • Port • Base de données • IAM • plugin_name • UID • Mot de passe • IdP_Tenant • Client_ID • Client_Secret	• ClusterID • Région • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • dbgroups_filter **Note** Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.
JWT	• Host (Hôte) • Port • Base de données • IAM • plugin_name • web_identity_token	• provider_name

Méthode d'authentification	Obligatoire	Facultatif
Okta	• Host (Hôte) • Port • Base de données • IAM • plugin_name • UID • Mot de passe • IdP_Host • App_Name • App_ID	• ClusterID • Région • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role **Note** Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.

Méthode d'authentification	Obligatoire	Facultatif
Ping Federate	• Host (Hôte) • Port • Base de données • IAM • plugin_name • UID • Mot de passe • IdP_Host • IdP_Port	• ClusterID • Région • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • SSL_Insecure • partner_spid **Note** Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.

Méthode d'authentification	Obligatoire	Facultatif
Navigateur Azure AD	• Host (Hôte) • Port • Base de données • IAM • plugin_name • IdP_Tenant • Client_ID • UID	• ClusterID • Région • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • dbgroups_filter • IdP_ Response_Timeout • listen_port **Note** Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.

Méthode d’authentification	Obligatoire	Facultatif
Navigateur SAML	• Host (Hôte) • Port • Base de données • IAM • plugin_name • login_url • UID	• ClusterID • Région • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • dbgroups_filter • IdP_ Response_Timeout • listen_port **Note** Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.
Profil d’authentification	• Host (Hôte) • Port • Base de données • AccessKeyID • SecretAccessKey	

Méthode d’authentification	Obligatoire	Facultatif
Navigateur Azure AD OAUTH2	• Host (Hôte) • Port • Base de données • IAM • plugin_name • IdP_Tenant • Client_ID • UID	• ClusterID • Région • EndpointUrl • IdP_ Response_Timeout • listen_port • scope • provider_name **Note** Les options ClusterID et Region (Région) doivent être définies sur Host (Héberger) si elles ne sont pas définies séparément.
AWS Centre d'identité IAM	• Host (Hôte) • Base de données • plugin_name • idc_region • issuer_url	• idc_client_display_name • idp_response_timeout • listen_port

Utilisation d’un service d’informations d’identification externe

En plus de la prise en charge intégrée d’AD FS, d’Azure AD et d’Okta, la version Windows du pilote ODBC Amazon Redshift prend également en charge d’autres services d’identification. Le pilote peut authentifier les connexions à l'aide de n'importe quel plugin de fournisseur SAML-based d'informations d'identification de votre choix.

Pour configurer un service d’informations d’identification externe sur Windows :

1. Créez un profil IAM qui spécifie le plug-in du fournisseur d'informations d'identification et d'autres paramètres d'authentification selon les besoins. Le profil doit être ASCII-encoded, et doit contenir, la paire clé-valeur suivante, où se `PluginPath` trouve le chemin complet vers l'application du plugin :

   ```
   plugin_name = PluginPath
   ```

   Par exemple :

   ```
   plugin_name = C:\Users\kjson\myapp\CredServiceApp.exe
   ```

   Pour plus d'informations sur la manière de créer un profil, consultez Utilisation d'un profil de configuration dans le Guide de la gestion du cluster Amazon Redshift.
2. Configurez le pilote pour utiliser ce profil. Le pilote détecte et utilise les paramètres d'authentification spécifiés dans le profil.

Conversions du type de données

Le pilote Amazon Redshift ODBC version 2.x prend en charge de nombreux formats de données courants, la conversion entre les types de données Amazon Redshift et SQL.

Le tableau suivant répertorie les mappages de types de données pris en charge.

Type Amazon Redshift	Type SQL
BIGINT	SQL_BIGINT
BOOLEAN	SQL_BIT
CHAR	SQL_CHAR
DATE	SQL_TYPE_DATE
DECIMAL	SQL_NUMERIC
DOUBLE PRECISION	SQL_DOUBLE
GEOGRAPHY	SQL_ LONGVARBINARY

Type Amazon Redshift	Type SQL
GEOMETRY	SQL_ LONGVARBINARY
INTEGER	SQL_INTEGER
REAL	SQL_REAL
SMALLINT	SQL_SMALLINT
SUPER	SQL_LONGVARCHAR
TEXT	SQL_LONGVARCHAR
TIME	SQL_TYPE_TIME
TIMETZ	SQL_TYPE_TIME
TIMESTAMP	SQL_TYPE_ TIMESTAMP
TIMESTAMPTZ	SQL_TYPE_ TIMESTAMP
VARBYTE	SQL_LONGVARBINARY
VARCHAR	SQL_VARCHAR

Options du pilote ODBC

Vous pouvez utiliser les options de configuration du pilote pour contrôler le comportement du pilote ODBC Amazon Redshift. Les options du pilote ne sont pas sensibles à la casse.

Sous Microsoft Windows, vous définissez généralement les options du pilote lorsque vous configurez un nom de source de données (DSN). Vous pouvez également définir des options de pilote dans la chaîne de connexion lorsque vous vous connectez par programme, ou en ajoutant ou en modifiant des clés de Registre dans `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\`*`your_DSN`*.

Sous Linux, vous définissez les options de configuration du pilote dans vos fichiers `odbc.ini` et `amazon.redshiftodbc.ini`. Les options de configuration définies dans un fichier `amazon.redshiftodbc.ini` s'appliquent à toutes les connexions. En revanche, les options de configuration définies dans un fichier `odbc.ini` sont spécifiques à une connexion. Les options de

configuration définies dans `odbc.ini` ont priorité sur les options de configuration définies dans `amazon.redshiftodbc.ini`.

Vous trouverez ci-dessous des descriptions des options que vous pouvez spécifier pour le pilote ODBC Amazon Redshift version 2.x :

Rubriques

- AccessKeyID
- app_id
- ApplicationName
- app_name
- AuthProfile
- AuthType
- AutoCreate
- BoolsAsChar
- CaFile
- client_id
- client_ secret
- ClusterId
- compression
- Base de données
- DatabaseMetadataCurrentDbOnly
- dbgroups_filter
- Pilote
- DSN
- EnableTableTypes
- EndpointUrl
- Fetch
- ForceLowercase
- group_federation

- https_proxy_host
- https_proxy_password
- https_proxy_port
- https_proxy_username
- IAM
- idc_client_display_name
- idc_region
- idp_host
- idp_port
- idp_response_timeout
- idp_tenant
- idp_partition
- idp_use_https_proxy
- InstanceProfile
- issuer_url
- KeepAlive
- KeepAliveCount
- KeepAliveInterval
- KeepAliveIdle
- listen_port
- login_url
- se connecter ToRp
- LogLevel
- LogPath
- LoginTimeout
- MaxLongVarcharSize
- MaxVarcharSize
- Min_TLS

- partner_spid
- Mot de passe | PWD
- plugin_name
- Port | PortNumber
- Prefer_PQ
- preferred_role
- Profil
- provider_name
- ProxyHost
- ProxyPort
- ProxyPwd
- ProxyUid
- ReadOnly
- region
- SecretAccessKey
- SessionToken
- Serveur | HostName | Hôte
- ssl_insecure
- SSLMode
- StreamingCursorRows
- StsConnectionTimeout
- StsEndpointUrl
- jeton
- token_type
- UID | Utilisateur | LogonID
- UseDeclareFetch
- UseUnicode
- web_identity_token

AccessKeyID

- Valeur par défaut – Aucune
- Types de données – Chaîne

La clé d'accès IAM pour l'utilisateur ou le rôle. Si vous définissez ce paramètre, vous devez également le spécifier SecretAccessKey.

Ce paramètre est facultatif.

app_id

- Valeur par défaut – Aucune
- Types de données – Chaîne

L'identifiant Okta-provided unique associé à votre application Amazon Redshift.

Ce paramètre est facultatif.

ApplicationName

- Valeur par défaut – Aucune
- Type de données : chaîne

Nom de l'application client à transmettre à Amazon Redshift à des fins d'audit. Le nom de l'application que vous fournissez apparaît dans la colonne « application_name » de la table SYS_CONNECTION_LOG. Cela permet de suivre et de dépanner les sources de connexion lors des problèmes de débogage.

Ce paramètre est facultatif.

app_name

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le nom de l'application Okta que vous utilisez pour authentifier la connexion à Amazon Redshift.

Ce paramètre est facultatif.

AuthProfile

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le profil d’authentification utilisé pour gérer les paramètres de connexion. Si vous définissez ce paramètre, vous devez également définir l'AccessKeyID et SecretAccessKey.

Ce paramètre est facultatif.

AuthType

- Valeur par défaut : standard
- Types de données – Chaîne

Cette option spécifie le mode d’authentification que le pilote utilise lorsque vous configurez un DSN à l’aide de la boîte de dialogue Configuration DSN du pilote ODBC Amazon Redshift :

- Standard : authentification standard en utilisant votre nom d’utilisateur et votre mot de passe Amazon Redshift.
- AWS Profil : authentification IAM à l'aide d'un profil.
- AWS Informations d'identification IAM : authentification IAM à l'aide des informations d'identification IAM.
- Fournisseur d’identité : AD FS : authentification IAM en utilisant Active Directory Federation Services (AD FS).
- Fournisseur d'identité : plug-in d'authentification : plug-in d'autorisation qui accepte un jeton AWS IAM Identity Center ou des jetons d'identité (JWT) OpenID Connect (OIDC) provenant de n'importe quel fournisseur JSON-based d'identité Web lié à IAM Identity Center. AWS
- Fournisseur d’identité : Azure AD : authentification IAM en utilisant un portail Azure AD.
- Fournisseur d’identité : JWT : authentification IAM en utilisant un jeton web JSON (JWT).
- Fournisseur d’identité : Okta : authentification IAM en utilisant Okta.
- Fournisseur d'identité PingFederate : authentification IAM à l'aide PingFederate de.

Cette option n’est disponible que lorsque vous configurez un DSN en utilisant la boîte de dialogue Configuration DSN du pilote ODBC Amazon Redshift dans le pilote Windows. Lorsque vous

configurez une connexion à l'aide d'une chaîne de connexion ou d'un ordinateur autre que Windows, le pilote détermine automatiquement s'il convient d'utiliser l'authentification standard, de AWS profil ou AWS IAM en fonction des informations d'identification que vous avez spécifiées. Pour utiliser un fournisseur d’identité, vous devez définir la propriété plugin_name.

Ce paramètre est obligatoire.

AutoCreate

- Valeur par défaut : 0
- Types de données – Booléen

Une valeur booléenne indiquant si le pilote crée un nouvel utilisateur lorsque l’utilisateur spécifié n’existe pas.

- 1 | TRUE : Si l’utilisateur spécifié par l’UID n’existe pas, le pilote crée un nouvel utilisateur.
- 0 | FALSE : Le pilote ne crée pas de nouvel utilisateur. Si l’utilisateur spécifié n’existe pas, l’authentification échoue.

Ce paramètre est facultatif.

BoolsAsChar

- Valeur par défaut : 0
- Types de données – Booléen

Spécifie si le pilote indique les colonnes BOOLÉENNES sous forme de caractères plutôt que de bits.

- 1 | VRAI : Le pilote indique les colonnes BOOLÉENNES sous la forme SQL_VARCHAR avec une taille de colonne de 1. Le pilote renvoie des valeurs booléennes sous forme de chaînes de caractères « 0 » et « 1 ».
- 0 | FALSE : le pilote indique les colonnes BOOLÉENNES sous la forme SQL_BIT. Il s’agit du comportement de par défaut.

Utilisez cette option si votre application utilise des colonnes BOOLÉENNES renvoyées sous forme de données de caractère.

Ce paramètre est facultatif. Cette option est disponible dans les versions 2.2.1 et ultérieures du pilote.

CaFile

- Valeur par défaut – Aucune
- Types de données – Chaîne

Chemin d’accès au fichier de certificat d’autorité de certification utilisé pour certaines formes d’authentification IAM.

Ce paramètre est disponible uniquement sur Linux.

Ce paramètre est facultatif.

client_id

- Valeur par défaut – Aucune
- Types de données – Chaîne

ID client associé à votre application Amazon Redshift dans Azure AD.

Ce paramètre est obligatoire si vous vous authentifiez via le service Azure AD.

client_ secret

- Valeur par défaut – Aucune
- Types de données – Chaîne

Clé secrète associée à votre application Amazon Redshift dans Azure AD.

Ce paramètre est obligatoire si vous vous authentifiez via le service Azure AD.

ClusterId

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le nom du cluster Amazon Redshift auquel vous souhaitez vous connecter. Il est utilisé dans l’authentification IAM. L’ID du cluster n’est pas spécifié dans le paramètre Server (Serveur).

Ce paramètre est facultatif.

compression

- Valeur par défaut : désactivé
- Types de données – Chaîne

Méthode de compression utilisée pour les communications par protocole filaire entre le serveur Amazon Redshift et le client ou le pilote.

Vous pouvez spécifier les valeurs suivantes :

- lz4 : définit la méthode de compression utilisée pour les communications par protocole filaire avec Amazon Redshift sur `lz4`.
- zstd : définit la méthode de compression utilisée pour les communications par protocole filaire avec Amazon Redshift sur `zstd`.
- désactivé : n'utilise pas la compression pour les communications par protocole filaire avec Amazon Redshift.

Ce paramètre est facultatif.

Base de données

- Valeur par défaut – Aucune
- Types de données – Chaîne

Nom de la base de données Amazon Redshift à laquelle vous souhaitez accéder.

Ce paramètre est obligatoire.

DatabaseMetadataCurrentDbOnly

- Valeur par défaut : 1
- Types de données – Booléen

Valeur booléenne indiquant si le pilote renvoie des métadonnées provenant de plusieurs bases de données et clusters.

- 1 | TRUE : Le pilote renvoie uniquement les métadonnées de la base de données actuelle.

- 0 | FALSE. Le pilote renvoie les métadonnées de plusieurs bases de données et clusters Amazon Redshift.

Ce paramètre est facultatif.

dbgroups_filter

- Valeur par défaut – Aucune
- Types de données – Chaîne

Expression régulière DbGroups que vous pouvez spécifier pour filtrer les informations reçues de la réponse SAML à Amazon Redshift lorsque vous utilisez les types d'authentification Azure, Browser Azure et Browser SAML.

Ce paramètre est facultatif.

Pilote

- Valeur par défaut : Pilote ODBC Amazon Redshift (64 bits)
- Types de données – Chaîne

Nom du pilote. La seule valeur prise en charge est Pilote ODBC Amazon Redshift (x64).

Ce paramètre est obligatoire si vous ne définissez pas le DSN.

DSN

- Valeur par défaut – Aucune
- Types de données – Chaîne

Nom de la source de données du pilote. L'application spécifie le DSN dans l' SQLDriverConnect API.

Ce paramètre est obligatoire si vous ne définissez pas le Pilote.

EnableTableTypes

- Valeur par défaut : 1
- Types de données – Booléen

Spécifie si le pilote reconnaît les informations détaillées sur le type de table provenant de la source de données lorsqu'une application appelle la fonction de catalogue SQLTables. Par défaut, le pilote reconnaît les types de tables détaillés.

- 1 | VRAI : Le pilote reconnaît les types de tables suivants : TABLE, VIEW, SYSTEM TABLE, SYSTEM VIEW, EXTERNAL TABLE et LOCAL TEMPORARY.
- 0 | FAUX : le pilote normalise les informations détaillées sur les types de table dans les types de table génériques TABLE et VIEW.

Ce paramètre est facultatif. Il est disponible dans les versions 2.2.1 et ultérieures du pilote.

EndpointUrl

- Valeur par défaut – Aucune
- Types de données – Chaîne

Point de terminaison principal utilisé pour communiquer avec le service Coral Amazon Redshift pour l’authentification IAM.

Ce paramètre est facultatif.

Fetch

- Valeur par défaut : 100
- Type de données – Entier

Lorsque Declare/Fetch le mode est activé, cette option contrôle le nombre de lignes que le pilote récupère par aller-retour, ce qui vous permet de trouver l'équilibre entre l'utilisation de la mémoire et la surcharge réseau en fonction de votre charge de travail. Une valeur plus élevée permet de récupérer plus de lignes à la fois, ce qui réduit le nombre d'allers-retours vers le serveur au prix d'une augmentation de la mémoire par extraction. Une valeur inférieure réduit l'utilisation de la mémoire mais augmente la fréquence à laquelle le pilote retourne sur le serveur. Il définit le nombre de lignes renvoyées par le pilote lorsqu'il `UseDeclareFetch` est activé. Pour plus d’informations, consultez UseDeclareFetch.

Ce paramètre est facultatif.

ForceLowercase

- Valeur par défaut : 0
- Types de données – Booléen

Un booléen spécifiant si le pilote met en minuscules toutes les informations DbGroups envoyées par le fournisseur d'identité à Amazon Redshift lors de l'utilisation de l'authentification unique.

- 1 | VRAI : Le pilote met en minuscules tous DbGroups les messages envoyés par le fournisseur d'identité.
- 0 | FAUX : le pilote ne change pas DbGroups.

Ce paramètre est facultatif.

group_federation

- Valeur par défaut : 0
- Types de données – Booléen

Un booléen spécifiant si l'API `getClusterCredentialsWithIAM` est utilisée pour obtenir des informations d'identification de cluster temporaires dans les clusters alloués. Cette option permet aux utilisateurs IAM d'intégrer les rôles de base de données Redshift dans les clusters alloués. Notez que cette option ne s'applique pas aux espaces de noms Redshift sans serveur.

- 1 | TRUE : Le pilote utilise l'API `getClusterCredentialsWithIAM` pour obtenir les informations d'identification temporaires du cluster dans les clusters alloués.
- 0 | FALSE : le pilote utilise l'API `getClusterCredentials` par défaut pour obtenir des informations d'identification de cluster temporaires dans les clusters alloués.

Ce paramètre est facultatif.

https_proxy_host

- Valeur par défaut – Aucune
- Types de données – Chaîne

Nom d'hôte ou adresse IP du serveur proxy via lequel vous souhaitez transmettre les processus d'authentification IAM.

Ce paramètre est facultatif.

https_proxy_password

- Valeur par défaut – Aucune
- Types de données – Chaîne

Mot de passe que vous utilisez pour accéder au serveur proxy. Il est utilisé pour l'authentification IAM.

Ce paramètre est facultatif.

https_proxy_port

- Valeur par défaut – Aucune
- Type de données – Entier

Numéro du port que le serveur proxy utilise pour écouter les connexions client. Il est utilisé pour l'authentification IAM.

Ce paramètre est facultatif.

https_proxy_username

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le nom d'utilisateur que vous utilisez pour accéder au serveur proxy. Il est utilisé pour l'authentification IAM.

Ce paramètre est facultatif.

IAM

- Valeur par défaut : 0

- Types de données – Booléen

Valeur booléenne indiquant si le pilote utilise une méthode d'authentification IAM pour authentifier la connexion.

- 1 | VRAI : Le pilote utilise l'une des méthodes d'authentification IAM (en utilisant une paire clé d'accès et clé secrète, un profil ou un service d'informations d'identification).
- 0 | FALSE. Le pilote utilise l'authentification standard (en utilisant le nom d'utilisateur et le mot de passe de votre base de données).

Ce paramètre est facultatif.

idc_client_display_name

- Valeur par défaut : pilote ODBC Amazon Redshift
- Types de données – Chaîne

Le nom d'affichage à utiliser pour le client qui l'utilise BrowserIdcAuthPlugin.

Ce paramètre est facultatif.

idc_region

- Valeur par défaut – Aucune
- Types de données – Chaîne

AWS Région dans laquelle se trouve l'instance AWS IAM Identity Center.

Ce paramètre est requis uniquement lors de l'authentification à l'aide de `BrowserIdcAuthPlugin` dans l'option de configuration plugin_name.

idp_host

- Valeur par défaut – Aucune
- Types de données – Chaîne

L'hôte IdP (fournisseur d'identité) que vous utilisez pour vous authentifier dans Amazon Redshift.

Ce paramètre est facultatif.

idp_port

- Valeur par défaut – Aucune
- Type de données – Entier

Port pour un IdP (fournisseur d’identité) que vous utilisez pour vous authentifier dans Amazon Redshift. En fonction du port que vous avez sélectionné lors de la création, de la modification ou de la migration du cluster, autorisez l’accès au port sélectionné.

Ce paramètre est facultatif.

idp_response_timeout

- Valeur par défaut – 120
- Type de données – Entier

La durée, en secondes, pendant laquelle le pilote attend la réponse SAML du fournisseur d’identité lors de l’utilisation des services SAML ou Azure AD via un plug-in de navigateur.

Ce paramètre est facultatif.

idp_tenant

- Valeur par défaut – Aucune
- Types de données – Chaîne

ID de locataire Azure AD associé à votre application Amazon Redshift.

Ce paramètre est obligatoire si vous vous authentifiez via le service Azure AD.

idp_partition

- Valeur par défaut – Aucune
- Types de données – Chaîne

Spécifie la partition cloud sur laquelle votre fournisseur d'identité (IdP) est configuré. Cela détermine le point de terminaison d'authentification IdP auquel le pilote se connecte.

Si ce paramètre est laissé vide, le pilote utilise par défaut la partition commerciale. Les valeurs possibles sont :

- `us-gov`: utilisez cette valeur si votre IdP est configuré dans Azure Government. Par exemple, Azure AD Government utilise le point de terminaison`login.microsoftonline.us`.
- `cn`: Utilisez cette valeur si votre IdP est configuré dans la partition cloud de Chine. Par exemple, Azure AD Chine utilise le point de terminaison`login.chinacloudapi.cn`.

Ce paramètre est facultatif.

idp_use_https_proxy

- Valeur par défaut : 0
- Types de données – Booléen

Valeur booléenne indiquant si le pilote transmet les processus d'authentification pour les fournisseurs d'identité (IdP) par un serveur proxy.

- 1 | TRUE : Le pilote transmet les processus d'authentification IdP par un serveur proxy.
- 0 | FALSE. Le pilote ne transmet pas les processus d'authentification IdP par un serveur proxy.

Ce paramètre est facultatif.

InstanceProfile

- Valeur par défaut : 0
- Types de données – Booléen

Valeur booléenne indiquant si le pilote utilise le profil d'instance Amazon EC2, lorsqu'il est configuré pour utiliser un profil pour l'authentification.

- 1 | TRUE : Le pilote utilise le profil d'instance Amazon EC2.
- 0 | FALSE. Le pilote utilise le profil des rôles reliés par chaîne spécifié par l'option Nom du profil (Profil) à la place.

Ce paramètre est facultatif.

issuer_url

- Valeur par défaut – Aucune
- Types de données – Chaîne

Pointe vers le point de terminaison de l'instance du serveur AWS IAM Identity Center.

Ce paramètre est requis uniquement lors de l’authentification à l’aide de `BrowserIdcAuthPlugin` dans l’option de configuration plugin_name.

KeepAlive

- Valeur par défaut : 1
- Types de données – Booléen

Valeur booléenne indiquant si le pilote utilise les keepalives TCP pour empêcher les connexions de s’interrompre.

- 1 | TRUE : Le pilote utilise les keepalives TCP pour empêcher les connexions de s’interrompre.
- 0 | FALSE. Le pilote n’utilise pas les keepalives TCP.

Ce paramètre est facultatif.

KeepAliveCount

- Valeur par défaut : 0
- Type de données – Entier

Nombre de paquets TCP keepalive qui peuvent être perdus avant que la connexion soit considérée comme interrompue. Lorsque ce paramètre est défini sur 0, le pilote utilise la valeur par défaut du système pour ce paramètre.

Ce paramètre est facultatif.

KeepAliveInterval

- Valeur par défaut : 0
- Type de données – Entier

Nombre de secondes entre chaque retransmission de paquet TCP keepalive. Lorsque ce paramètre est défini sur 0, le pilote utilise la valeur par défaut du système pour ce paramètre.

Ce paramètre est facultatif.

KeepAliveIdle

- Valeur par défaut : 0
- Type de données – Entier

Nombre de secondes d’inactivité avant que le pilote envoie un paquet TCP keepalive. Lorsque ce paramètre est défini sur 0, le pilote utilise la valeur par défaut du système pour ce paramètre.

Ce paramètre est facultatif.

listen_port

- Valeur par défaut : 7890
- Type de données – Entier

Port utilisé par le pilote pour recevoir la réponse SAML du fournisseur d'identité ou le code d'autorisation lors de l'utilisation des services SAML, Azure AD ou AWS IAM Identity Center via un plug-in de navigateur.

Ce paramètre est facultatif.

login_url

- Valeur par défaut – Aucune
- Types de données – Chaîne

URL de la ressource sur le site web du fournisseur d’identité lors de l’utilisation du plug-in générique du Navigateur SAML.

Ce paramètre est requis si vous vous authentifiez avec les services SAML ou Azure AD via un plugin de navigateur.

se connecter ToRp

- Valeur par défaut : urn:amazon:webservices

- Types de données – Chaîne

L'approbation des parties utilisatrices que vous souhaitez utiliser pour le type d'authentification AD FS.

Cette chaîne est facultative.

LogLevel

- Valeur par défaut : 0
- Type de données – Entier

> **Note**
>
> `LogLevel`et `LogPath` sont des paramètres globaux. Le conducteur les lit dans l'ordre de priorité suivant :
>
> 1. Chaîne de connexion (`LogLevel=6;LogPath=/path;`) : priorité la plus élevée, remplace tous les autres paramètres au moment de la connexion.
> 2. Sous Windows : la boîte de dialogue de configuration DSN (onglet Avancé).
>
>   Sous Linux et macOS : `[ODBC]` section de votre `odbc.ini` fichier.
> 3. **`[DRIVER]`**section du `amazon.redshiftodbc.ini` fichier — utilisée comme solution de secours si la journalisation n'est pas activée à partir de la source ci-dessus.
>
> Le réglage `LogLevel` ou `LogPath` dans une section DSN individuelle (par exemple,`[MyDSN]`) n'a aucun effet. Ces options ne sont pas lues à partir des sections par DSN.

Utilisez cette propriété pour activer ou désactiver la journalisation dans le pilote et pour spécifier la quantité de détails inclus dans les fichiers journaux. Nous vous recommandons d'activer la journalisation juste assez longtemps pour capturer un problème, car elle diminue les performances et peut consommer une grande quantité d'espace disque.

Définissez la propriété sur l'une des valeurs suivantes :

- 0 : OFF. Désactiver toute la journalisation.

- 1 : FATAL. Réservé aux erreurs fatales.
- 2 : ERREUR. Enregistre les événements d'erreur tels que les échecs de connexion et les erreurs d'authentification.
- 3 : AVERTIR. Enregistre les avertissements et les situations inattendues en plus des erreurs.
- 4 : INFORMATIONS Enregistre les informations générales de progression, telles que l'état de la connexion et les paramètres du serveur.
- 5 : DEBUG. Enregistre toutes les activités du pilote, y compris les appels aux fonctions de l'API ODBC avec des arguments et des valeurs renvoyées.
- 6 : TRACER. Enregistre toutes les activités du conducteur, y compris les informations supplémentaires relatives au protocole de bas niveau et à l'état interne.

> **Important**
>
> Le niveau de journalisation 5 (DEBUG) ou supérieur capture toutes les activités du conducteur, qui peuvent inclure des informations sensibles telles que les informations d'identification de connexion et les données de requête. N'activez ces niveaux de journalisation que temporairement pour détecter un problème et assurez-vous que toutes les informations sensibles sont supprimées avant de partager les journaux avec le support ou un tiers.

Lorsque la journalisation est activée, le pilote produit les fichiers journaux suivants à l'emplacement que vous spécifiez dans la LogPathpropriété :

- Un fichier `redshift_odbc.log.1` qui enregistre l’activité du pilote pendant la négociation d’une connexion.
- Un fichier `redshift_odbc.log` pour toutes les activités du pilote après l’établissement d’une connexion à la base de données.

Ce paramètre est facultatif.

LogPath

- Valeur par défaut — Le répertoire OS-specific TEMP
- Types de données – Chaîne

> **Note**
>
> `LogLevel`et `LogPath` sont des paramètres globaux. Le conducteur les lit dans l'ordre de priorité suivant :
>
> 1. Chaîne de connexion (`LogLevel=6;LogPath=/path;`) : priorité la plus élevée, remplace tous les autres paramètres au moment de la connexion.
> 2. Sous Windows : la boîte de dialogue de configuration DSN (onglet Avancé).
>
>   Sous Linux et macOS : `[ODBC]` section de votre `odbc.ini` fichier.
> 3. **`[DRIVER]`**section du `amazon.redshiftodbc.ini` fichier — utilisée comme solution de secours si la journalisation n'est pas activée à partir de la source ci-dessus.
>
> Le réglage `LogLevel` ou `LogPath` dans une section DSN individuelle (par exemple,`[MyDSN]`) n'a aucun effet. Ces options ne sont pas lues à partir des sections par DSN.

Le chemin complet du dossier dans lequel le pilote enregistre les fichiers journaux lorsqu'il LogLevelest supérieur à 0.

Ce paramètre est facultatif.

LoginTimeout

- Valeur par défaut : 0
- Type de données – Entier

Le nombre de secondes pendant lesquelles le pilote attend qu'une connexion au serveur soit établie avant l'expiration du délai imparti. Une valeur de 0 signifie qu'il n'y a pas de délai d'attente (le conducteur attend indéfiniment).

Vous pouvez définir cette option dans la chaîne de connexion (en utilisant `LoginTimeout` ou l'alias courtLT), dans la configuration DSN ou par programmation en utilisant with. `SQLSetConnectAttr` `SQL_ATTR_LOGIN_TIMEOUT` Sous Windows, cette option est également disponible dans la boîte de dialogue de configuration DSN (onglet Avancé).

Ce paramètre est facultatif.

MaxLongVarcharSize

- Valeur par défaut : 65535
- Type de données – Entier

Taille de colonne indiquée par le pilote pour les colonnes reclassées en gros texte (SQL_LONGVARCHAR). MaxVarcharSize Cette valeur remplace la taille réelle déclarée de la colonne dans les réponses aux métadonnées.

La valeur par défaut de 65 535 est recommandée car certaines couches intergicielles, telles que MSDASQL, rejettent les colonnes de texte volumineux dont la taille déclarée se situe entre 8 001 et 32 768 octets. En signalant 65 535, le chauffeur s'assure que les colonnes reclassées sont acceptées sans erreur. La plupart des utilisateurs n'ont pas besoin de modifier cette valeur.

Ce paramètre n'a aucun effet lorsqu'il MaxVarcharSizeest défini sur 0 (reclassification désactivée).

Ce paramètre est facultatif. Il est disponible dans les versions 2.1.16 et ultérieures du pilote.

MaxVarcharSize

- Valeur par défaut : 255
- Type de données – Entier

Taille de colonne maximale que le pilote indique sous forme de colonne de texte normale (SQL_VARCHAR). Le pilote reclasse toute CHAR VARCHAR colonne supérieure à cette valeur en texte volumineux (SQL_LONGVARCHARou SQL_WLONGVARCHAR lorsqu'elle UseUnicodeest activée).

Cette reclassification permet d'éviter les erreurs dans les applications ou les couches intergicielles qui ne peuvent pas traiter les colonnes de texte normal au-delà d'une certaine taille. Par exemple, les serveurs liés à SQL Server qui accèdent à Amazon Redshift via MSDASQL (OLE DB) ne peuvent pas traiter les colonnes de plus de 8 000 octets environ. Le fait de reclasser les SQL_VARCHAR colonnes surdimensionnées en texte volumineux permet d'éviter les échecs de conversion.

- 255(par défaut) : les colonnes de plus de 255 caractères sont signalées commeSQL_LONGVARCHAR.
- 0: Désactive le reclassement. Toutes les colonnes sont signalées SQL_VARCHAR indépendamment de leur taille.

- Valeur personnalisée : n'importe quel entier positif. Les colonnes supérieures à la valeur spécifiée sont signalées sous la formeSQL_LONGVARCHAR.

Lorsqu'une colonne est reclassée, le pilote indique sa taille en utilisant la valeur spécifiée dans MaxLongVarcharSize.

Ce paramètre est facultatif. Il est disponible dans les versions 2.1.16 et ultérieures du pilote.

Min_TLS

- Valeur par défaut : 1,2
- Types de données – Chaîne

Version minimale TLS/SSL que le pilote autorise le magasin de données à utiliser pour chiffrer les connexions. Par exemple, si le protocole TLS 1.2 est spécifié, le protocole TLS 1.1 ne peut pas être utilisé pour chiffrer les connexions.

Min_TLS accepte les valeurs suivantes :

- 1.0 : La connexion doit utiliser au moins TLS 1.0.
- 1.1 : La connexion doit utiliser au moins TLS 1.1.
- 1.2 : La connexion doit utiliser au moins TLS 1.2.

Ce paramètre est facultatif.

partner_spid

- Valeur par défaut – Aucune
- Types de données – Chaîne

La valeur SPID (ID du fournisseur de services) du partenaire à utiliser lors de l'authentification de la connexion à l'aide du PingFederate service.

Ce paramètre est facultatif.

Mot de passe | PWD

- Valeur par défaut – Aucune

- Types de données – Chaîne

Mot de passe correspondant au nom d'utilisateur de la base de données que vous avez fourni dans le champ Utilisateur (UID | Utilisateur | LogonID).

Ce paramètre est facultatif.

plugin_name

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le nom du plug-in du fournisseur d'informations d'identification que vous souhaitez utiliser pour l'authentification.

Les valeurs suivantes sont prises en charge :

- `ADFS` : utilisez Active Directory Federation Services pour l'authentification.
- `AzureAD` : utilisez le service Microsoft Azure Active Directory (AD) pour l'authentification.
- `BrowserAzureAD` : utilisez un plug-in de navigateur pour le service Microsoft Azure Active Directory (AD) pour l'authentification.
- `BrowserIdcAuthPlugin` : un plugin d'autorisation utilisant AWS IAM Identity Center.
- `BrowserSAML` : utilisez un plug-in de navigateur pour les services SAML tels qu'Okta ou Ping pour l'authentification.
- `IdpTokenAuthPlugin`: plugin d'autorisation qui accepte un jeton AWS IAM Identity Center ou des jetons d'identité (JWT) OpenID Connect (JSON-based OIDC) provenant de n'importe quel fournisseur d'identité Web AWS lié à IAM Identity Center.
- `JWT` : utilisez un jeton web JSON (JWT) pour l'authentification.
- `Ping`: utilisez le PingFederate service pour l'authentification.
- `Okta` : utilisez le service Okta pour l'authentification.

Ce paramètre est facultatif.

Port | PortNumber

- Valeur par défaut : 5439

- Type de données – Entier

Numéro du port TCP que le serveur Amazon Redshift utilise pour écouter les connexions client.

Ce paramètre est facultatif.

Prefer_PQ

- Valeur par défaut : 1
- Types de données – Booléen

Spécifie si le pilote annonce des groupes d'échange de clés hybrides post-quantiques dans le TLS 1.3. ClientHello Lorsque des groupes post-quantiques sont proposés et que le serveur les prend également en charge, le serveur en sélectionne un. Sinon, la poignée de main revient à un échange de clés classique de manière transparente.

- 1 | VRAI : Le pilote fait la promotion de groupes d'échange de clés TLS hybrides post-quantiques.
- 0 | FAUX : Le pilote ne fait pas de publicité pour les groupes post-quantiques. Utilisez ce paramètre si un boîtier intermédiaire réseau bloque les poignées de main TLS car il ne reconnaît pas les groupes d'échange de clés post-quantiques proposés par le pilote.

Ce paramètre est facultatif. Il est disponible dans les versions 2.2.1 et ultérieures du pilote.

preferred_role

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le rôle que vous souhaitez endosser lors de la connexion à Amazon Redshift. Il est utilisé pour l’authentification IAM.

Ce paramètre est facultatif.

Profil

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le nom du AWS profil utilisateur utilisé pour s'authentifier auprès d'Amazon Redshift.

- Si le paramètre Use Instance Profile (la InstanceProfilepropriété) est défini sur 1 | TRUE, ce paramètre est prioritaire et le pilote utilise le profil d'instance Amazon EC2 à la place.
- L'emplacement par défaut du fichier d'informations d'identification qui contient des profils est `~/.aws/Credentials`. La variable d'environnement `AWS_SHARED_CREDENTIALS_FILE` peut être utilisée pour désigner un autre fichier d'informations d'identification.

Ce paramètre est facultatif.

provider_name

- Valeur par défaut – Aucune
- Types de données – Chaîne

Fournisseur d'authentification créé par l'utilisateur à l'aide de la requête CREATE IDENTITY PROVIDER. Il est utilisé dans l'authentification native Amazon Redshift.

Ce paramètre est facultatif.

ProxyHost

- Valeur par défaut – Aucune
- Types de données – Chaîne

Nom d'hôte ou adresse IP du serveur proxy via lequel vous souhaitez vous connecter.

Ce paramètre est facultatif.

ProxyPort

- Valeur par défaut – Aucune
- Type de données – Entier

Numéro du port que le serveur proxy utilise pour écouter les connexions client.

Ce paramètre est facultatif.

ProxyPwd

- Valeur par défaut – Aucune
- Types de données – Chaîne

Mot de passe que vous utilisez pour accéder au serveur proxy.

Ce paramètre est facultatif.

ProxyUid

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le nom d'utilisateur que vous utilisez pour accéder au serveur proxy.

Ce paramètre est facultatif.

ReadOnly

- Valeur par défaut : 0
- Types de données – Booléen

Valeur booléenne indiquant si le pilote est en mode lecture seule.

- 1 | TRUE : La connexion est en mode lecture seule et ne peut pas écrire dans le magasin de données.
- 0 | FALSE : La connexion n'est pas en mode lecture seule et peut écrire dans le magasin de données.

Ce paramètre est facultatif.

region

- Valeur par défaut – Aucune
- Types de données – Chaîne

La AWS région dans laquelle se trouve votre cluster.

Ce paramètre est facultatif.

SecretAccessKey

- Valeur par défaut – Aucune
- Types de données – Chaîne

La clé de secret IAM pour l'utilisateur ou le rôle. Si vous définissez ce paramètre, vous devez également définir l'AccessKeyID.

Ce paramètre est facultatif.

SessionToken

- Valeur par défaut – Aucune
- Types de données – Chaîne

Le jeton de séance IAM temporaire associé au rôle IAM que vous utilisez pour vous authentifier.

Ce paramètre est facultatif.

Serveur | HostName | Hôte

- Valeur par défaut – Aucune
- Types de données – Chaîne

Serveur de point de terminaison auquel se connecter.

Ce paramètre est obligatoire.

ssl_insecure

- Valeur par défaut : 0
- Types de données – Booléen

Valeur booléenne indiquant si le pilote vérifie l'authenticité du certificat du serveur IdP.

- 1 | TRUE : Le pilote ne vérifie pas l'authenticité du certificat du serveur IdP.

- 0 | FALSE : Le pilote vérifie l'authenticité du certificat du serveur IdP.

Ce paramètre est facultatif.

SSLMode

- Valeur par défaut : `verify-ca`
- Types de données – Chaîne

Mode de vérification du certificat SSL à utiliser lors de la connexion à Amazon Redshift. Les valeurs suivantes sont possibles :

- `verify-full` : connectez-vous uniquement en utilisant un protocole SSL, une autorité de certification de confiance et un nom de serveur qui correspond au certificat.
- `verify-ca` : connectez-vous uniquement en utilisant le protocole SSL et une autorité de certification de confiance.
- `require` : connectez-vous uniquement en utilisant le protocole SSL.
- `prefer` : connectez-vous en utilisant le protocole SSL s'il est disponible. Sinon, connectez-vous sans utiliser le protocole SSL.
- `allow` : par défaut, connectez-vous sans utiliser le protocole SSL. Si le serveur nécessite des connexions SSL, utilisez le protocole SSL.
- `disable` : connectez-vous sans utiliser le protocole SSL.

> **Note**
>
> Nous vous recommandons d'utiliser `verify-full` des connexions SSL dans la mesure du possible.

Ce paramètre est facultatif.

StreamingCursorRows

- Valeur par défaut : 0
- Type de données – Entier

Limite le nombre de lignes que le pilote garde en mémoire à la fois pour un curseur avant uniquement, afin que les ensembles de résultats volumineux n'aient pas à être chargés en mémoire en une seule fois.

Définissez la propriété sur l'une des valeurs suivantes :

- 0 : le pilote charge l'ensemble des résultats en mémoire avant de renvoyer des lignes à l'application (par défaut). Les ensembles de résultats très volumineux peuvent consommer une grande quantité de mémoire.
- Nombre entier positif : pour un curseur orienté uniquement vers l'avant, le pilote ne conserve que le nombre de lignes en mémoire à la fois. Il renvoie ces lignes à l'application, les libère, puis récupère le lot suivant une fois que l'application a consommé le lot en cours.

Cette option n'a aucun effet sur les curseurs défilants, qui utilisent toujours le comportement en mémoire. Notez que sous Windows, la boîte de dialogue de configuration DSN du pilote ODBC Amazon Redshift préremplit ce champ avec une valeur de 100.

Le mode curseur de diffusion en continu nécessite un curseur uniquement vers l'avant. Si l'option CSC (Client Side Cursor) est activée, elle est prioritaire et le mode curseur de diffusion en continu est désactivé.

> **Note**
>
> `StreamingCursorRowset UseDeclareFetch` les deux résultats par lots au lieu de charger l'ensemble des résultats en mémoire. `UseDeclareFetch`hutilise un curseur côté serveur et fournit généralement un débit nettement supérieur. Il est donc préférable de le faire lorsque les performances de récupération sont votre principale préoccupation. `StreamingCursorRows`ne nécessite pas d'encapsulation des transactions ni de curseur côté serveur ; choisissez-le lorsque ces propriétés sont plus importantes que la vitesse maximale, c'est-à-dire un flux en transfert uniquement avec une empreinte mémoire limitée. Si cette option `UseDeclareFetch` est activée, elle prend la priorité et force `StreamingCursorRows` la valeur à 0. Pour plus d'informations, consultez UseDeclareFetch.

Ce paramètre est facultatif.

StsConnectionTimeout

- Valeur par défaut : 0

- Type de données – Entier

Durée d’attente maximale pour les connexions IAM, en secondes. S'il est réglé sur 0 ou non spécifié, le chauffeur attend 60 secondes pour chaque AWS STS appel.

Ce paramètre est facultatif.

StsEndpointUrl

- Valeur par défaut – Aucune
- Types de données – Chaîne

Cette option spécifie le point de terminaison principal utilisé pour communiquer avec AWS Security Token Service (AWS STS).

Ce paramètre est facultatif.

jeton

- Valeur par défaut – Aucune
- Types de données – Chaîne

Un jeton d'accès fourni par AWS IAM Identity Center ou un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d'identité Web AWS lié à IAM Identity Center. Votre application doit générer ce jeton en authentifiant l'utilisateur de votre application auprès d' AWS IAM Identity Center ou d'un fournisseur d'identité lié à AWS IAM Identity Center.

Ce paramètre fonctionne avec `IdpTokenAuthPlugin`.

token_type

- Valeur par défaut – Aucune
- Types de données – Chaîne

Type de jeton utilisé dans `IdpTokenAuthPlugin`.

Vous pouvez spécifier les valeurs suivantes :

ACCESS_TOKEN

Entrez cette valeur si vous utilisez un jeton d'accès fourni par AWS IAM Identity Center.

EXT_JWT

Entrez cette valeur si vous utilisez un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d’identité Web intégré à AWS IAM Identity Center.

Ce paramètre fonctionne avec `IdpTokenAuthPlugin`.

UID | Utilisateur | LogonID

- Valeur par défaut – Aucune
- Types de données – Chaîne

Nom d’utilisateur que vous utilisez pour accéder au serveur Amazon Redshift.

Ce paramètre est obligatoire si vous utilisez l’authentification de base de données.

UseDeclareFetch

- Valeur par défaut : 0
- Types de données – Booléen

Lorsqu'une requête renvoie un jeu de résultats trop important pour être conservé en mémoire, l'activation de cette option permet au pilote de le traiter par lots de taille fixe au lieu de mettre le résultat en une seule fois en mémoire tampon, ce qui permet de limiter et de prévoir l'empreinte mémoire du client quel que soit le nombre de lignes renvoyées par la requête. Il s'agit d'un booléen spécifiant si le pilote utilise le Declare/Fetch mode, renvoyant un certain nombre de lignes à la fois. Pour définir le nombre de lignes renvoyées par lot, utilisez l'`Fetch`option. Pour plus d’informations, consultez Fetch.

- 1 | VRAI : Le pilote utilise le Declare/Fetch mode et renvoie le nombre de lignes spécifié par l'`Fetch`option à la fois.
- 0 | FALSE : le pilote renvoie l'intégralité du résultat de la requête en une seule fois.

Ce paramètre est facultatif.

> **Note**
>
> Si cette option `UseDeclareFetch` est activée, le pilote désactive le mode curseur de diffusion et passe `StreamingCursorRows` à 0, quelle que soit la valeur définie dans votre DSN ou votre chaîne de connexion. Pour plus d'informations, consultez StreamingCursorRows.

UseUnicode

- Valeur par défaut : 0
- Types de données – Booléen

Un booléen spécifiant si le pilote renvoie les données Redshift sous forme d'Unicode ou de type SQL normal.

- 1 | VRAI : Le pilote renvoie un type SQL large pour le type de données de type caractère.
  - SQL_WCHAR est renvoyé à la place de SQL_CHAR.
  - SQL_WVARCHAR est renvoyé au lieu de SQL_VARCHAR.
  - SQL_WLONGVARCHAR est renvoyé au lieu de SQL_LONGVARCHAR.
- 0 | FAUX : le pilote renvoie un type SQL normal pour le type de données de type caractère.
  - SQL_CHAR est renvoyé au lieu de SQL_WCHAR.
  - SQL_VARCHAR est renvoyé au lieu de SQL_WVARCHAR.
  - SQL_LONGVARCHAR est renvoyé au lieu de SQL_WLONGVARCHAR.

Ce paramètre est facultatif. Il est disponible dans les versions 2.1.15 et ultérieures du pilote.

web_identity_token

- Valeur par défaut – Aucune
- Types de données – Chaîne

Jeton OAUTH fourni par le fournisseur d'identité. Il est utilisé dans le plug-in JWT.

Ce paramètre est obligatoire si vous définissez le paramètre plugin_name sur. BasicJwtCredentialsProvider

Versions antérieures du pilote ODBC

Ne téléchargez une version antérieure du pilote ODBC Amazon Redshift version 2x que si votre outil nécessite une version spécifique du pilote.

Utiliser les versions antérieures du pilote ODBC pour Microsoft Windows

Voici les versions précédentes du pilote ODBC Amazon Redshift version 2.x pour Microsoft Windows :

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.3.0/AmazonRedshiftODBC64-2.2.3.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.2.0/AmazonRedshiftODBC64-2.2.2.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.1.0/AmazonRedshiftODBC64-2.2.1.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.0.0/AmazonRedshiftODBC64-2.2.0.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.17.0/AmazonRedshiftODBC64-2.1.17.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.16.0/AmazonRedshiftODBC64-2.1.16.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.15.0/AmazonRedshiftODBC64-2.1.15.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.14.0/AmazonRedshiftODBC64-2.1.14.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.13.0/AmazonRedshiftODBC64-2.1.13.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.12.0/AmazonRedshiftODBC64-2.1.12.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.11.0/AmazonRedshiftODBC64-2.1.11.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.10.0/AmazonRedshiftODBC64-2.1.10.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.9.0/AmazonRedshiftODBC64-2.1.9.0.msi

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.9.0/AmazonRedshiftODBC64-2.1.9.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.8.0/AmazonRedshiftODBC64-2.1.8.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.7.0/AmazonRedshiftODBC64-2.1.7.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.6.0/AmazonRedshiftODBC64-2.1.6.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.4.0/AmazonRedshiftODBC64-2.1.4.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.3.0/AmazonRedshiftODBC64-2.1.3.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.2.0/AmazonRedshiftODBC64-2.1.2.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.1.0/AmazonRedshiftODBC64-2.1.1.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.0.0/AmazonRedshiftODBC64-2.1.0.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/AmazonRedshiftODBC64-2.0.1.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/AmazonRedshiftODBC64-2.0.0.11.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/AmazonRedshiftODBC64-2.0.0.9.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/AmazonRedshiftODBC64-2.0.0.8.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/AmazonRedshiftODBC64-2.0.0.7.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/AmazonRedshiftODBC64-2.0.0.6.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/AmazonRedshiftODBC64-2.0.0.5.msi

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/AmazonRedshiftODBC64-2.0.0.3.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/AmazonRedshiftODBC64-2.0.0.1.msi

Utiliser les versions antérieures du pilote ODBC pour Linux

Vous trouverez ci-dessous les versions précédentes du pilote ODBC Amazon Redshift version 2.x pour Linux :

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.3.0/AmazonRedshiftODBC-64-bit-2.2.3.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.3.0/AmazonRedshiftODBC-64-bit-2.2.3.0.aarch64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.3.0/AmazonRedshiftODBC-64-bit-2.2.3.0.amd64.deb
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.3.0/AmazonRedshiftODBC-64-bit-2.2.3.0.arm64.deb
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.2.0/AmazonRedshiftODBC-64-bit-2.2.2.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.2.0/AmazonRedshiftODBC-64-bit-2.2.2.0.aarch64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.2.0/AmazonRedshiftODBC-64-bit-2.2.2.0.amd64.deb
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.2.0/AmazonRedshiftODBC-64-bit-2.2.2.0.arm64.deb
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.1.0/AmazonRedshiftODBC-64-bit-2.2.1.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.1.0/AmazonRedshiftODBC-64-bit-2.2.1.0.aarch64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.1.0/AmazonRedshiftODBC-64-bit-2.2.1.0.amd64.deb
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.1.0/AmazonRedshiftODBC-64-bit-2.2.1.0.arm64.deb

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.0.0/AmazonRedshiftODBC-64-bit-2.2.0.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.0.0/AmazonRedshiftODBC-64-bit-2.2.0.0.aarch64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.0.0/AmazonRedshiftODBC-64-bit-2.2.0.0.amd64.deb
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.0.0/AmazonRedshiftODBC-64-bit-2.2.0.0.arm64.deb
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.17.0/AmazonRedshiftODBC-64-bit-2.1.17.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.17.0/AmazonRedshiftODBC-64-bit-2.1.17.0.aarch64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.16.0/AmazonRedshiftODBC-64-bit-2.1.16.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.16.0/AmazonRedshiftODBC-64-bit-2.1.16.0.aarch64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.15.0/AmazonRedshiftODBC-64-bit-2.1.15.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.15.0/AmazonRedshiftODBC-64-bit-2.1.15.0.aarch64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.14.0/AmazonRedshiftODBC-64-bit-2.1.14.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.14.0/AmazonRedshiftODBC-64-bit-2.1.14.0.aarch64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.13.0/AmazonRedshiftODBC-64-bit-2.1.13.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.13.0/AmazonRedshiftODBC-64-bit-2.1.13.0.aarch64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.12.0/AmazonRedshiftODBC-64-bit-2.1.12.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.12.0/AmazonRedshiftODBC-64-bit-2.1.12.0.aarch64.rpm

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.11.0/AmazonRedshiftODBC-64-bit-2.1.11.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.11.0/AmazonRedshiftODBC-64-bit-2.1.11.0.aarch64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.10.0/AmazonRedshiftODBC-64-bit-2.1.10.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.9.0/AmazonRedshiftODBC-64-bit-2.1.9.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.8.0/AmazonRedshiftODBC-64-bit-2.1.8.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.7.0/AmazonRedshiftODBC-64-bit-2.1.7.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.6.0/AmazonRedshiftODBC-64-bit-2.1.6.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.4.0/AmazonRedshiftODBC-64-bit-2.1.4.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.3.0/AmazonRedshiftODBC-64-bit-2.1.3.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.2.0/AmazonRedshiftODBC-64-bit-2.1.2.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.1.0/AmazonRedshiftODBC-64-bit-2.1.1.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.0.0/AmazonRedshiftODBC-64-bit-2.1.0.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/AmazonRedshiftODBC-64-bit-2.0.1.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/AmazonRedshiftODBC-64-bit-2.0.0.11.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/AmazonRedshiftODBC-64-bit-2.0.0.9.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/AmazonRedshiftODBC-64-bit-2.0.0.8.x86_64.rpm

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/AmazonRedshiftODBC-64-bit-2.0.0.7.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/AmazonRedshiftODBC-64-bit-2.0.0.6.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/AmazonRedshiftODBC-64-bit-2.0.0.5.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/AmazonRedshiftODBC-64-bit-2.0.0.3.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/AmazonRedshiftODBC-64-bit-2.0.0.1.x86_64.rpm

Utiliser les versions précédentes du pilote ODBC pour Apple macOS

Voici les versions précédentes du pilote ODBC Amazon Redshift version 2.x pour Apple macOS :

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.3.0/AmazonRedshiftODBC-64-bit.2.2.3.0.universal.pkg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.2.0/AmazonRedshiftODBC-64-bit.2.2.2.0.universal.pkg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.1.0/AmazonRedshiftODBC-64-bit.2.2.1.0.universal.pkg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.2.0.0/AmazonRedshiftODBC-64-bit.2.2.0.0.universal.pkg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.17.0/AmazonRedshiftODBC-64-bit.2.1.17.0.universal.pkg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.16.0/AmazonRedshiftODBC-64-bit.2.1.16.0.universal.pkg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.15.0/AmazonRedshiftODBC-64-bit.2.1.15.0.universal.pkg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.14.0/AmazonRedshiftODBC-64-bit.2.1.14.0.universal.pkg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.13.0/AmazonRedshiftODBC-64-bit.2.1.13.0.universal.pkg

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.12.0/AmazonRedshiftODBC-64-bit.2.1.12.0.universal.pkg

Différences entre les versions 2.x et 1.x du pilote ODBC

Cette section décrit les différences entre le pilote ODBC 1.x et le pilote ODBC 2.x, et fournit des conseils sur la façon de migrer vers le pilote 2.x. Il décrit les modifications susceptibles d'affecter votre application et la manière d'y remédier.

Principales différences à corriger

Les actions suivantes permettent de résoudre les problèmes de migration les plus courants. La plupart des applications n'ont besoin que d'un sous-ensemble de ces éléments.

DSN et chaîne de connexion

- Vérifiez dans votre DSN les options de pilote susceptibles d'avoir été supprimées ou renommées. Certaines options du pilote ODBC 1.x ne sont pas prises en charge dans le pilote ODBC 2.x. D'autres ont été renommés. Consultez Chaîne de connexion et options DSN pour plus de détails.
- Définissez **`UseUnicode=true`** si votre application dépend des codes de type à caractères larges (**`SQL_WVARCHAR`**,**`SQL_WCHAR`**). Dans le pilote ODBC 2.x, la `UseUnicode` valeur par défaut est`false`, qui indique les types de caractères restreints.
- Déplacez les paramètres de journalisation vers la **`[ODBC]`** section. Sur Linux et macOS, `LogPath` il doit être défini dans la `[ODBC]` section globale de`odbc.ini`, `LogLevel` et non dans une section DSN individuelle.

Requête et schéma

- Inclure **`EXTERNAL TABLE`** dans les filtres **`SQLTables`** de type. Dans ODBC 2.x, les tables Amazon Redshift Spectrum et les tables de partage de données sont signalées sous la forme. `EXTERNAL TABLE` Si vous filtrez `SQLTables` par type, `EXTERNAL TABLE` ajoutez-en pour continuer à voir ces objets. Vous pouvez également définir l'`EnableTableTypes`option sur 0 pour normaliser les informations détaillées sur les types de table dans les types de table génériques TABLE et VIEW, comme décrit dans l'élément suivant.
- Les types de tableaux détaillés sont activés par défaut. ODBC 2.x active `EnableTableTypes` cette option par défaut. Le pilote 1.x a désactivé cette option par défaut. Avec la version 2.x par défaut, `SQLTables` indique des types détaillés tels que SYSTEM TABLE, SYSTEM VIEW,

EXTERNAL TABLE et LOCAL TEMPORARY. Pour signaler chaque table en tant que type générique TABLE et chaque vue en tant que VUE, définissez `EnableTableTypes` la valeur 0.

- **`INTERVAL`**Transférez vers **`VARCHAR`** les applications qui ne prennent pas en charge le type de données d'intervalle. Certains clients ne prennent pas en charge les types d'intervalles ODBC. Pour ces clients, insérez la colonne dans votre requête : `SELECT col::VARCHAR FROM ...`

Code de l'application

- Vérifiez les paramètres de délai d'expiration des requêtes. ODBC 2.x s'applique correctement `SQL_ATTR_QUERY_TIMEOUT` conformément à la spécification ODBC. ODBC 1.x a ignoré ce paramètre en silence. Long-running les requêtes qui réussissaient auparavant peuvent désormais échouer avec une erreur de délai d'attente. Vérifiez et ajustez les valeurs de vos délais d'attente selon vos besoins.
- Indiquez la longueur des données pour les paramètres de données lors de l'exécution. 2.x est signalé `SQL_NEED_LONG_DATA_LEN` comme Y (1.x signaléN). Les applications qui lient `SQL_DATA_AT_EXEC` des paramètres doivent désormais fournir la longueur totale des données dès le départ`StrLen_or_IndPtr`.

Chaîne de connexion et options DSN

Le tableau suivant présente les options du pilote ODBC 1.x qui ont été renommées ou ont des équivalents directs dans le pilote ODBC 2.x.

Option 1.x	équivalent 2.x	Remarques
`MaxLongVarChar`	`MaxLongVarcharSize`	La valeur par défaut est passée de 8190 à 65535.
`ConnectionTimeout`	`LoginTimeout`	Même délai d'expiration de connexion, renommé. La valeur par défaut est 0 (aucun délai d'attente).
`VpcEndpointUrl`	`vpc_endpoint_url`	
`SSLCertPath`	`TrustStore` ou `CaFile`	Chemin d'accès au certificat CA utilisé pour vérifier le serveur. Sous Windows, définisse

Option 1.x	équivalent 2.x	Remarques
		z-le dans le champ Trust Store de la boîte de dialogue de configuration DSN ; la boîte de dialogue ne contient aucun `CaFile` champ. Si les deux sont définis, `TrustStore` prend la priorité.

Les options 1.x suivantes ne sont pas prises en charge dans le pilote 2.x actuel. Le pilote 2.x les ignore afin qu'ils n'affectent pas votre connexion. Leur suppression de votre DSN est facultative mais recommandée pour éviter toute confusion.

- `SingleRowMode`— pour limiter la mémoire du client, utilisez `StreamingCursorRows` ou `UseDeclareFetch` remplacez.
- `UseSystemTrustStore`— non pris en charge. Sous Windows, le pilote 1.x pouvait valider le certificat du serveur par rapport au magasin de certificats du système Windows. Le pilote 2.x valide par rapport à un fichier de certificat CA : il utilise le certificat racine Amazon Redshift fourni par défaut, ou le fichier que vous spécifiez dans ou. `TrustStore` `CaFile`
- `TextAsLongVarchar`,`CheckCertRevocation`,`EnableAwsSdkLogs`,`UseLogPrefix`,`Locale`,`UseMul` `EnforceSingleStatement` — aucun équivalent dans la version actuelle. L'équipe Amazon Redshift évalue des équivalents ou des alternatives pour ces options dans les futures versions.

Pour obtenir la liste complète des options 2.x prises en charge, consultezOptions du pilote ODBC.

Changements de type de données

Le tableau suivant présente les mappages de types de données Amazon Redshift qui ont été modifiés dans ODBC 2.x pour se conformer à la spécification ODBC. La plupart des applications ne sont pas affectées car elles lient les colonnes par index ou par nom plutôt que par code de type.

Type de données Amazon Redshift	ODBC 1.x	ODBC 2.x
`DOUBLE PRECISION`	`SQL_FLOAT (6)`	`SQL_DOUBLE (8)`

Type de données Amazon Redshift	ODBC 1.x	ODBC 2.x
INTERVAL YEAR TO MONTH	SQL_VARCHAR (12), texte	SQL_INTERVAL_YEAR_TO_MONTH (107), structure d'intervalle
INTERVAL DAY TO SECOND	SQL_VARCHAR (12), texte	SQL_INTERVAL_DAY_TO_SECOND (110), structure d'intervalle
VARCHAR / CHAR / TEXT	Types larges (SQL_WVARCHAR ,SQL_WCHAR ,SQL_WLONGVARCHAR) ; par défaut UseUnicode=true	Types étroits (SQL_VARCHAR ,SQL_CHAR,SQL_LONGVARCHAR). UseUnicode=true Paramétré pour restaurer les types étendus.
GEOMETRY/GEOGRAPHY (en tant queSQL_C_BINARY)	Hex-encoded Chaîne ASCII	Octets binaires bruts

Les COLUMN_SIZE valeurs renvoyées par ont SQLColumns également changé pour GEOMETRYGEOGRAPHY, et les types de SUPER données, qui renvoient désormais NULL pour indiquer les colonnes non dimensionnées conformément à la spécification ODBC. Les applications qui allouent des tampons en fonction de la valeur NULL COLUMN_SIZE doivent gérer la valeur NULL en utilisant une taille de tampon par défaut.

Post-migration résolution des problèmes

Le tableau suivant décrit les problèmes courants que vous pouvez rencontrer après la migration et explique comment les résoudre.

Symptôme	Cause	Que faire
Les tables externes ne sont pas visibles dans le navigateur de schémas	Les tables de spectre et de partage de données sont présentées sous la forme EXTERNAL TABLE	EXTERNAL TABLEIncluez-le dans votre filtre de SQLTables type ou EnableTableTypes définissez-le sur 0 pour normaliser les types

Symptôme	Cause	Que faire
		de tables détaillés dans les types génériques TABLE et VIEW.
erreurs pyodbc sur les colonnes d'intervalle	pyodbc ne supporte pas les types d'intervalles ODBC	Convertissez les intervalles `VARCHAR` en requêtes in.
Les données des personnages s'affiche nt sous forme de caractères inattendus (mojibake)	`UseUnicode` la valeur par défaut a été modifiée en`false`. Les applications qui attendent des données à caractères larges (UTF-16) peuvent mal interpréter les octets contenant des caractères étroits comme des paires larges, ce qui produit un résultat déformé. Les données elles-mêmes restent inchangées.	Définissez `UseUnicode=true` votre DSN ou mettez à jour votre application pour lier les colonnes au `SQL_C_CHAR` lieu de`SQL_C_WCH AR` .
Long-running les requêtes renvoient des erreurs de délai	`SQL_ATTR_QUERY_TIM EOUT` est désormais en vigueur. ODBC 1.x a ignoré ce paramètre en silence.	Augmentez ou supprimez `QueryTimeout` de votre DSN, ou réglez-le `SQL_ATTR_QUERY_TIM EOUT` sur 0 dans votre application.
Paramétrer `SQL_ATTR_ CURRENT_CATALOG` les retours `HY011`	L'attribut ne peut pas être défini sur une connexion ouverte. Le changement de base de données sur une connexion ouverte n'est pas pris en charge.	Définissez l'attribut avant de vous connecter, ou fermez et rouvrez la connexion sur la base de données cible.
La connexion se bloque dans les environne ments à double pile	Limitation dans les versions <= 2.1.16	Effectuez une mise à niveau vers la version 2.1.17 ou ultérieure.

Symptôme	Cause	Que faire
L'analyse des messages d'erreur renvoie des résultats inattendus	Format du message modifié ; codes SQLSTATE inchangés	Analysez les codes SQLSTATE au lieu du texte du message.
Data-at-execution la liaison de paramètres se comporte différemment	`SQL_NEED_LONG_DATA_LEN` passé de FAUX à VRAI ; les applications qui l'utilisent `SQL_DATA_AT_EXEC` doivent désormais fournir la longueur totale des données à l'avance	Définissez la valeur de longueur `StrLen_or_IndPtr` lors de la liaison `SQL_DATA_AT_EXEC` des paramètres.
Les journaux des pilotes ne sont pas générés	`LogLevel`et `LogPath` doit figurer dans la section `[ODBC]` globale de`odbc.ini`, et non dans des sections DSN individuelles	Déplacez les paramètres de journalisation de votre DSN vers la `[ODBC]` section.

Mise à niveau depuis une ancienne version ODBC 2.x

Si vous utilisez déjà une ancienne version ODBC 2.x, passez à la dernière version. Pour obtenir la liste complète des améliorations et des corrections de bogues apportées à toutes les versions, consultez l'enregistrement des modifications apportées au pilote ODBC Amazon Redshift. GitHub

En savoir plus

- Configuration d’une connexion pour le pilote ODBC version 2.x pour Amazon Redshift
- Options du pilote ODBC
- Journal des modifications du pilote ODBC Amazon Redshift

Configuration d'une connexion au pilote ODBC version 1.x

Vous pouvez utiliser une connexion ODBC pour vous connecter à votre cluster Amazon Redshift à partir de nombreux outils et applications clients SQL tiers. Pour ce faire, configurez la connexion sur

votre ordinateur client ou votre instance Amazon EC2. Si votre outil client prend en charge JDBC, vous pouvez choisir d'utiliser ce type de connexion plutôt qu'ODBC en raison de la simplicité de configuration offerte par JDBC. Toutefois, si votre outil client ne prend pas en charge JDBC, suivez les étapes de cette section pour configurer une connexion ODBC.

Amazon Redshift fournit des pilotes ODBC 64 bits pour les systèmes d'exploitation Linux, Windows et macOS. Les pilotes ODBC 32 bits sont interrompus. D'autres mises à jour ne seront pas publiées, sauf pour les correctifs de sécurité urgents.

Pour obtenir les dernières informations sur les fonctionnalités du pilote ODBC et les conditions préalables, consultez les Notes de mise à jour du pilote ODBC d'Amazon Redshift.

Pour obtenir des informations sur l'installation et la configuration des pilotes ODBC Amazon Redshift, consultez le Guide d'installation et de configuration du connecteur ODBC Amazon Redshift. .

Rubriques

- Obtention de l'URL ODBC
- Utilisation d'un pilote ODBC Amazon Redshift sur Microsoft Windows
- Utilisation d'un pilote ODBC Amazon Redshift sous Linux
- Utilisation d'un pilote ODBC Amazon Redshift sous macOS
- Options du pilote ODBC
- Versions antérieures du pilote ODBC

Obtention de l'URL ODBC

Amazon Redshift affiche l'URL ODBC de votre cluster dans la console Amazon Redshift. Cette URL contient les informations permettant de configurer la connexion entre votre ordinateur client et la base de données.

Une URL ODBC a le format suivant :

```
Driver={driver};Server=endpoint;Database=database_name;UID=user_name;PWD=passwor
```

Les champs du format indiqué ci-dessus ont les valeurs suivantes.

Champ	Value
`Driver`	Nom du pilote ODBC 64 bits à utiliser :Amazon Redshift (x64).

Champ	Value
	Nom du pilote ODBC 32 bits :Amazon Redshift (x86).
`Server`	Le point de terminaison du cluster Amazon Redshift.
`Database`	Base de données que vous avez créée pour votre cluster.
`UID`	Nom d'utilisateur d'un compte utilisateur autorisé à se connecter à la base de données. Cette valeur est une autorisation de base de données, et non une autorisation Amazon Redshift, bien que vous puissiez utiliser le compte administrateur que vous avez configuré lorsque vous avez lancé le cluster.
`PWD`	Mot de passe du compte utilisateur vous permettant de vous connecter à la base de données.
`Port`	Numéro du port que vous avez spécifié lorsque vous avez lancé le cluster. Si vous avez un pare-feu, vérifiez que ce port est ouvert pour que vous l'utilisiez.

Les champs des tables précédentes peuvent contenir les caractères spéciaux suivants :

```
[]{}(),;?*=!@
```

Si vous utilisez ces caractères spéciaux, vous devez placer la valeur entre accolades. Par exemple, la valeur du mot de passe `Your;password123` dans une chaîne de connexion est représentée par `PWD={Your;password123};`.

Les paires `Field=value` étant séparées par un point-virgule, la combinaison de `}` et de `;` avec n'importe quel nombre d'espaces entre les deux est considérée comme la fin d'une paire `Field={value};`. Nous vous recommandons d'éviter la séquence `};` dans les valeurs de vos champs. Par exemple, si vous définissez la valeur de votre mot de passe comme `PWD={This is a passwor} ;d};`, votre mot de passe sera `This is a passwor} ;` et l'URL sera erronée.

Voici un exemple d'URL ODBC.

```
Driver={Amazon Redshift (x64)};
                    Server=examplecluster.abc123xyz789.us-
west-2.redshift.amazonaws.com;
                    Database=dev;
```

```
UID=adminuser;
PWD=insert_your_admin_user_password_here;
Port=5439
```

Pour plus d'informations sur l'obtention d'une connexion ODBC, consultez Recherche de votre chaîne de connexion au cluster.

Utilisation d'un pilote ODBC Amazon Redshift sur Microsoft Windows

Vous installez le pilote ODBC Amazon Redshift sur les ordinateurs clients accédant à un entrepôt des données Amazon Redshift. Chaque ordinateur sur lequel vous installez le pilote doit répondre à des exigences minimales. Pour plus d'informations sur la configuration minimale requise, consultez le Guide d'installation et de configuration du connecteur ODBC d'Amazon Redshift. .

Rubriques

- Téléchargement et installation du pilote ODBC Amazon Redshift
- Création d'une entrée du nom de la source de données (DSN) système pour une connexion ODBC

Téléchargement et installation du pilote ODBC Amazon Redshift

Utilisez la procédure suivante pour télécharger les pilotes ODBC Amazon Redshift pour les systèmes d'exploitation Windows. N'utilisez un pilote autre que ceux-ci que si vous exécutez une application tierce qui est certifiée pour être utilisée avec Amazon Redshift et qui nécessite un pilote spécifique.

Pour installer le pilote ODBC

1. Téléchargez l'un des pilotes suivants, en fonction de l'architecture système de votre outil client SQL ou de votre application :

   - Version 1.6.3 du pilote ODBC 64 bits version 1.6.3.

     Le nom de ce pilote est Amazon Redshift (x64).

   - Version du pilote ODBC 32 bits 1.4.52 Dans version 1.4.52

     Le nom de ce pilote est Amazon Redshift (x86). Les pilotes ODBC 32 bits sont interrompus. D'autres mises à jour ne seront pas publiées, sauf pour les correctifs de sécurité urgents.

> **Note**
>
> Téléchargez le package MSI qui correspond à l'architecture système de votre application ou outil client SQL. Par exemple, si votre outil client SQL est en 64 bits, installez le pilote 64 bits.

Ensuite, téléchargez et consultez le Contrat de licence du pilote ODBC et JDBC d'Amazon Redshift.

2. Double-click le fichier .msi, puis suivez les étapes de l'assistant pour installer le pilote.

Création d'une entrée du nom de la source de données (DSN) système pour une connexion ODBC

Après avoir téléchargé et installé le pilote ODBC, ajoutez une entrée de nom de source de données (DSN) à l'ordinateur client ou à l'instance Amazon EC2. Les outils clients SQL utilisent cette source de données pour se connecter à la base de données Amazon Redshift.

Nous vous recommandons de créer un DSN système au lieu d'un DSN utilisateur. Certaines applications chargent les données à l'aide d'un compte utilisateur différent. Ces applications peuvent ne pas être en mesure de détecter les DSN utilisateur créés sous un autre compte d'utilisateur.

> **Note**
>
> Pour l'authentification à l'aide des informations d'identification Gestion des identités et des accès AWS (IAM) ou des informations d'identification du fournisseur d'identité (IdP), des étapes supplémentaires sont requises. Pour plus d'informations, consultez Étape 5 : Configurer une connexion JDBC ou ODBC pour utiliser des informations d'identification IAM.

Pour plus d'informations sur la création d'une entrée DSN système, consultez le Guide d'installation et de configuration du pilote ODBC d'Amazon Redshift. .

Pour créer une entrée DSN système pour une connexion ODBC sous Windows

1. Dans le menu Démarrer ouvrez Sources de données ODBC.

Veillez à choisir l'administrateur de sources de données ODBC qui a le même bitness que l'application client que vous utilisez pour vous connecter à Amazon Redshift.

2. Dans l'administrateur de source de données ODBC, choisissez l'onglet Driver (Pilote) et recherchez le dossier du pilote :

   - Pilote ODBC Amazon Redshift (64 bits)
   - Pilote ODBC Amazon Redshift (32 bits)

3. Sélectionnez l'onglet Système DSN pour configurer le pilote pour tous les utilisateurs sur l'ordinateur ; ou l'onglet Utilisateur DSN pour configurer le pilote correspondant à votre compte utilisateur uniquement.
4. Choisissez Ajouter. La fenêtre Créer une nouvelle source de données s'ouvre.
5. Choisissez le pilote ODBC Amazon Redshift, puis cliquez sur Terminer. La fenêtre Amazon Redshift ODBC Driver DSN Setup (Configuration DSN du pilote ODBC Amazon Redshift) s'ouvre.
6. Sous Paramètres de connexion, saisissez les informations suivantes :

   Nom de la source de données

   Entrez un nom pour la source de données. Vous pouvez utiliser n'importe quel nom de votre choix pour identifier la source de données ultérieurement, lorsque vous créez la connexion au cluster. Par exemple, si vous avez suivi le Guide de démarrage d'Amazon Redshift, vous pouvez taper `exampleclusterdsn` pour faciliter la mémorisation du cluster que vous associez à ce DSN.

   Serveur

   Spécifiez le point de terminaison de votre cluster Amazon Redshift. Vous trouverez ces informations dans la console Amazon Redshift sur la page des détails du cluster. Pour plus d'informations, consultez Configuration des connexions dans Amazon Redshift.

   Port

   Entrez le numéro de port utilisé par la base de données. Utilise le port que le cluster a configuré pour être utilisé lors de son lancement ou de sa modification.

   Base de données

Saisissez le nom de la base de données Amazon Redshift. Si vous avez lancé votre cluster sans spécifier de nom de base de données, entrez *dev*. Sinon, utilisez le nom que vous avez choisi pendant le processus de lancement. Si vous avez suivi les étapes de Guide de démarrage d'Amazon Redshift, saisissez *dev*.

7. Sous Authentification, spécifiez les options de configuration pour configurer l'authentification standard ou IAM. Pour plus d'informations sur les options d'authentification, consultez « Configuration de l'authentification sous Windows » dans le Guide d'installation et de configuration du connecteur ODBC d'Amazon Redshift.
8. Sous Paramètres SSL, spécifiez une valeur pour les éléments suivants :

   Authentification SSL

   Sélectionnez un mode de traitement SSL (Secure Sockets Layer). Dans un environnement de test, vous pouvez utiliser `prefer`. Cependant, pour les environnements de production et lorsque l'échange de données sécurisé est nécessaire, utilisez `verify-ca` ou `verify-full`. Pour plus d'informations sur l'utilisation de SSL sous Windows, consultez « Configuration de la vérification SSL sous Windows » dans le Guide d'installation et de configuration du connecteur ODBC d'Amazon Redshift.
9. Sous Options supplémentaires, spécifiez des options de renvoi des résultats de la requête à votre outil ou application cliente SQL. Pour plus d'informations, consultez « Configuration d'options supplémentaires sous Windows » dans le Guide d'installation et de configuration du connecteur ODBC d'Amazon Redshift.
10. Dans Options de journalisation, spécifiez les valeurs de l'option de journalisation. Pour plus d'informations, consultez « Configuration des options de journalisation sous Windows » dans le Guide d'installation et de configuration du connecteur ODBC d'Amazon Redshift.

    Choisissez ensuite OK.
11. Sous Options de type de données, spécifiez les valeurs des types de données. Pour plus d'informations, consultez « Configuration des options de type de données sous Windows » dans le Guide d'installation et de configuration du connecteur ODBC d'Amazon Redshift.

    Choisissez ensuite OK.
12. Sélectionnez Tester). Si l'ordinateur client peut se connecter à la base de données Amazon Redshift, vous voyez le message suivant : Connexion réussie.

Si l'ordinateur client ne peut pas se connecter à la base de données, il se peut que vous deviez résoudre d'éventuels problèmes. Pour plus d'informations, consultez Résolution des problèmes de connexion dans Amazon Redshift.

13. Configurez les keepalives TCP sous Windows pour empêcher la temporation des connexions. Pour plus d'informations sur la configuration des keepalives TCP sous Windows, consultez le Guide d'installation et de configuration du connecteur ODBC d'Amazon Redshift.
14. Pour faciliter le dépannage, configurez la journalisation. Pour plus d'informations sur la configuration de la journalisation sous Windows, consultez le Guide d'installation et de configuration du connecteur ODBC d'Amazon Redshift.

Utilisation d'un pilote ODBC Amazon Redshift sous Linux

Vous installez le pilote ODBC Amazon Redshift sur les ordinateurs clients accédant à un entrepôt des données Amazon Redshift. Chaque ordinateur sur lequel vous installez le pilote doit répondre à des exigences minimales. Pour plus d'informations sur la configuration minimale requise, consultez le Guide d'installation et de configuration du connecteur ODBC d'Amazon Redshift. .

Rubriques

- Téléchargement et installation du pilote ODBC Amazon Redshift
- Utilisation d'un gestionnaire de pilotes ODBC pour configurer le pilote

Téléchargement et installation du pilote ODBC Amazon Redshift

Suivez les étapes de cette section pour télécharger et installer les pilotes ODBC Amazon Redshift sur une distribution Linux prise en charge. Le processus d'installation installe les fichiers du pilote dans les répertoires suivants :

- `/opt/amazon/redshiftodbc/lib/64` (pour le pilote 64 bits)
- `/opt/amazon/redshiftodbc/ErrorMessages`
- `/opt/amazon/redshiftodbc/Setup`
- `/opt/amazon/redshiftodbc/lib/32` (pour le pilote 32 bits)

Pour installer le pilote ODBC Amazon Redshift

1. Téléchargez l'un des pilotes suivants, en fonction de l'architecture système de votre outil client SQL ou de votre application :

   - Version 1.6.3 du pilote RPM 64 bits .
   - Version 1.6.3 du pilote Debian 64 bits .
   - Version du pilote 32 bits 1.4.52 Dans 1.6.3.

   Le nom de chacun de ces pilotes est Amazon Redshift ODBC driver. Les pilotes ODBC 32 bits sont interrompus. D'autres mises à jour ne seront pas publiées, sauf pour les correctifs de sécurité urgents.

   > **Note**
   >
   > Téléchargez le package qui correspond à l'architecture système de votre application ou outil client SQL. Par exemple, si votre outil client est en 64 bits, installez un pilote 64 bits.

   Ensuite, téléchargez et consultez le Contrat de licence du pilote ODBC et JDBC d'Amazon Redshift.

2. Accédez à l'emplacement dans lequel vous avez téléchargé le package et exécutez l'une des commandes suivantes. Utilisez la commande qui correspond à votre distribution Linux.

   - Sur les systèmes d'exploitation RHEL et CentOS, exécutez la commande suivante.

     ```
     yum -nogpgcheck localinstall RPMFileName
     ```

     Remplacez *RPMFileName* par le nom du fichier de package RPM. Par exemple, la commande suivante illustre l'installation du pilote 64 bits :

     ```
     yum -nogpgcheck localinstall AmazonRedshiftODBC-64-bit-1.x.xx.xxxx-x.x86_64.rpm
     ```

   - Sur SLES, exécutez la commande suivante :

     ```
     zypper install RPMFileName
     ```

Remplacez *RPMFileName* par le nom du fichier de package RPM. Par exemple, la commande suivante illustre l'installation du pilote 64 bits :

```
zypper install AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.rpm
```

- Sur Debian, exécutez la commande suivante.

```
sudo apt install ./DEBFileName.deb
```

Remplacez *DEBFileName.deb* par le nom du fichier du paquet Debian. Par exemple, la commande suivante illustre l'installation du pilote 64 bits :

```
sudo apt install ./AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.deb
```

> **Important**
>
> Lorsque vous avez fini d'installer les pilotes, configurez-les pour les utiliser sur votre système. Pour plus d'informations sur la configuration du pilote, consultez Utilisation d'un gestionnaire de pilotes ODBC pour configurer le pilote.

Utilisation d'un gestionnaire de pilotes ODBC pour configurer le pilote

Sur les systèmes d'exploitation Linux, vous utilisez un gestionnaire de pilotes ODBC pour configurer les paramètres de connexion ODBC. Les gestionnaires de pilotes ODBC utilisent des fichiers de configuration pour définir et configurer les pilotes et les sources de données ODBC. Le gestionnaire de pilotes ODBC que vous utilisez s'appuie sur le système d'exploitation que vous utilisez. Pour Linux, il s'agit du gestionnaire de pilotes UnixODBC.

Pour plus d'informations sur les gestionnaires de pilotes ODBC pris en charge pour configurer les pilotes ODBC Amazon Redshift, consultez Utilisation d'un pilote ODBC Amazon Redshift sous Linux pour les systèmes d'exploitation Linux. Consultez également « Specifying ODBC Driver Managers on Non- Windows Machines » (Spécification des gestionnaires de pilotes ODBC sur des machines non Windows) dans le Guide d'installation et de configuration du connecteur ODBC Amazon Redshift. .

Trois fichiers sont nécessaires pour configurer le pilote ODBC d'Amazon Redshift : `amazon.redshiftodbc.ini`, `odbc.ini` et `odbcinst.ini`.

Si vous l'avez installé à l'emplacement par défaut, le fichier de configuration `amazon.redshiftodbc.ini` se trouve dans l'un des répertoires suivants :

- `/opt/amazon/redshiftodbc/lib/64` (pour le pilote 64 bits sur les systèmes d'exploitation Linux)
- `/opt/amazon/redshiftodbc/lib/32` (pour le pilote 32 bits sur les systèmes d'exploitation Linux)

De plus, sous `/opt/amazon/redshiftodbc/Setup` sous Linux, il existe des exemples de fichiers `odbc.ini` et `odbcinst.ini`. Vous pouvez utiliser ces fichiers comme exemples pour configurer le pilote ODBC Amazon Redshift et le nom de la source de données (DSN).

Nous ne recommandons pas d'utiliser le répertoire d'installation du pilote ODBC d'Amazon Redshift pour les fichiers de configuration. Les fichiers du répertoire `Setup` sont proposés à titre d'exemple seulement. Si vous réinstallez le pilote ODBC Amazon Redshift ultérieurement, ou si vous effectuez une mise à niveau vers une version plus récente, le répertoire d'installation est écrasé. Vous perdez alors toute modification que vous auriez pu apporter à ces fichiers.

Pour éviter cela, copiez le fichier `amazon.redshiftodbc.ini` dans un répertoire autre que le répertoire d'installation. Si vous copiez ce fichier vers le répertoire de base de l'utilisateur, ajouter un point (.) au début du nom de fichier pour le masquer.

Pour les fichiers `odbc.ini` et `odbcinst.ini`, utilisez les fichiers de configuration dans le répertoire personnel de l'utilisateur ou créez de nouvelles versions dans un autre répertoire. Par défaut, votre système d'exploitation Linux doit avoir un fichier `odbc.ini` et un fichier `odbcinst.ini` dans le répertoire personnel de l'utilisateur (`/home/$USER` ou `~/`). Ces fichiers par défaut sont des fichiers cachés, ce qui est indiqué par le point (.) devant chaque nom de fichier. Ces fichiers s'affichent uniquement lorsque vous utilisez l'indicateur `-a` pour répertorier le contenu du répertoire.

Quelle que soit l'option choisie pour les fichiers `odbc.ini` et `odbcinst.ini`, modifiez les fichiers pour ajouter les informations de configuration du pilote et du DSN. Si vous avez choisi de créer de nouveaux fichiers, vous devez également définir des variables d'environnement afin de spécifier l'emplacement dans lequel se trouvent ces fichiers de configuration.

Par défaut, les gestionnaires de pilotes ODBC sont configurés pour utiliser les versions cachées des fichiers de configuration `odbc.ini` et `odbcinst.ini` (nommés `.odbc.ini` et `.odbcinst.ini`) situés dans le répertoire de base. Ils sont également configurés pour utiliser le fichier `amazon.redshiftodbc.ini` dans le sous-dossier `/lib` du répertoire d'installation du

pilote. Si vous stockez ces fichiers de configuration ailleurs, définissez les variables d'environnement décrites ci-dessous afin que le gestionnaire de pilotes puisse localiser les fichiers. Pour plus d'informations, consultez « Specifying the Locations of the Driver Configuration Files » (Spécification des emplacements des fichiers de configuration du pilote) dans le Guide d'installation et de configuration du connecteur ODBC Amazon Redshift. .

Création d'un nom de source de données sur les systèmes d'exploitation Linux

Lorsque vous vous connectez à votre magasin de données à l'aide d'un nom de source de données (DSN), configurez le fichier `odbc.ini` pour définir des DSN. Définissez les propriétés du fichier `odbc.ini` pour créer un DSN qui spécifie les informations de connexion pour votre magasin de données.

Pour plus d'informations sur la configuration du `odbc.ini` fichier, consultez « Création d'un nom de source de données sur une Non-Windows machine » dans le guide d'installation et de configuration du connecteur ODBC Amazon Redshift. En Chine, utilisez le lien suivant : Guide d'installation et .

Sur les systèmes d'exploitation Linux, utilisez le format suivant :

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/driver_file

Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

L'exemple suivant illustre la configuration du fichier odbc.ini à l'aide du pilote ODBC 64 bits sur les systèmes d'exploitation Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x64=Amazon Redshift (x64)

[Amazon Redshift (x64)]
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
```

```
locale=en-US
```

L'exemple suivant illustre la configuration du fichier odbc.ini à l'aide du pilote ODBC 32 bits sur les systèmes d'exploitation Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x32=Amazon Redshift (x86)

[Amazon Redshift (x86)]
Driver=/opt/amazon/redshiftodbc/lib/32/libamazonredshiftodbc32.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US
```

Configuration d'une connexion sans DSN sur les systèmes d'exploitation Linux

Pour vous connecter à votre magasin de données via une connexion qui n'a pas de DSN, définissez le pilote dans le fichier `odbcinst.ini`. Entrez ensuite une chaîne de DSN-less connexion dans votre application.

Pour plus d'informations sur la configuration du `odbcinst.ini` fichier dans ce cas, consultez la section « Configuration d'une DSN-less connexion sur une Non-Windows machine » dans le guide d'installation et de configuration du connecteur ODBC Amazon Redshift. .

Sur les systèmes d'exploitation Linux, utilisez le format suivant :

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file

...
```

L'exemple suivant illustre la configuration de `odbcinst.ini` pour le pilote 64 bits installé dans les répertoires par défaut sur les systèmes d'exploitation Linux.

```
[ODBC Drivers]
```

```
Amazon Redshift (x64)=Installed

[Amazon Redshift (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
```

L'exemple suivant illustre la configuration de `odbcinst.ini` pour le pilote 32 bits installé dans les répertoires par défaut sur les systèmes d'exploitation Linux.

```
[ODBC Drivers]
Amazon Redshift (x86)=Installed

[Amazon Redshift (x86)]
Description=Amazon Redshift ODBC Driver (32-bit)
Driver=/opt/amazon/redshiftodbc/lib/32/libamazonredshiftodbc32.so
```

Configuration des variables d'environnement

Utilisez le gestionnaire de pilotes ODBC approprié pour charger le pilote correct. Pour ce faire, définissez la variable d'environnement de chemin de bibliothèque. Pour plus d'informations, consultez la section « Spécification des gestionnaires de pilotes ODBC sur les Non-Windows machines » dans le guide d'installation et de configuration du connecteur ODBC Amazon Redshift. .

Par défaut, les gestionnaires de pilotes ODBC sont configurés pour utiliser les versions cachées des fichiers de configuration `odbc.ini` et `odbcinst.ini` (nommés `.odbc.ini` et `.odbcinst.ini`) situés dans le répertoire de base. Ils sont également configurés pour utiliser le fichier `amazon.redshiftodbc.ini` dans le sous-dossier `/lib` du répertoire d'installation du pilote. Si vous stockez ces fichiers de configuration ailleurs, définissez les variables d'environnement afin que le gestionnaire de pilotes puisse localiser les fichiers. Pour plus d'informations, consultez « Spécification des emplacements des fichiers de configuration du pilote » dans le Guide d'installation et de configuration du connecteur ODBC Amazon Redshift.

Configuration des fonctions de connexion

Vous pouvez configurer les fonctionnalités de connexion suivantes pour votre paramètre ODBC :

- Configurez le pilote ODBC pour fournir des informations d'identification et authentifier la connexion à la base de données Amazon Redshift.
- Configurez le pilote ODBC pour qu'il se connecte à un socket activé avec Secure Sockets Layer (SSL), si vous vous connectez à un serveur Amazon Redshift dont le SSL est activé.

- Configurez le pilote ODBC pour vous connecter à Amazon Redshift via un serveur proxy.
- Configurez le pilote ODBC pour qu'il utilise un mode de traitement des requêtes pour empêcher les requêtes de consommer trop de mémoire.
- Configurez le pilote ODBC pour qu'il transmette les processus d'authentification IAM via un serveur proxy.
- Configurez le pilote ODBC pour qu'il utilise les keepalives TCP pour empêcher la temporisation des connexions.

Pour plus d'informations sur ces fonctionnalités de connexion, consultez le Guide d'installation et de configuration du connecteur ODBC Amazon Redshift. .

Utilisation d'un pilote ODBC Amazon Redshift sous macOS

Vous installez le pilote sur les ordinateurs clients accédant à un entrepôt des données Amazon Redshift. Chaque ordinateur sur lequel vous installez le pilote doit répondre à des exigences minimales. Pour plus d'informations sur la configuration minimale requise, consultez le Guide d'installation et de configuration du connecteur ODBC d'Amazon Redshift. .

Rubriques

- Téléchargement et installation du pilote ODBC Amazon Redshift
- Utilisation d'un gestionnaire de pilotes ODBC pour configurer le pilote

Téléchargement et installation du pilote ODBC Amazon Redshift

Suivez les étapes décrites dans cette section pour télécharger et installer le pilote ODBC Amazon Redshift sur une version compatible de macOS. Le processus d'installation installe les fichiers du pilote dans les répertoires suivants :

- `/opt/amazon/redshift/lib/universal`
- `/opt/amazon/redshift/ErrorMessages`
- `/opt/amazon/redshift/Setup`

Pour installer le pilote ODBC Amazon Redshift sur macOS

1. Pour installer le pilote ODBC Amazon Redshift sur macOS, téléchargez la version 1.6.3 du pilote macOS.

Ensuite, téléchargez et consultez le Contrat de licence du pilote ODBC et JDBC d'Amazon Redshift.

2. Double-click AmazonRedshiftODBC.pkgpour exécuter le programme d'installation.
3. Suivez les étapes décrites dans le programme d'installation pour terminer le processus d'installation du pilote. Vous devrez accepter les conditions générales du contrat de licence pour effectuer l'installation.

> **Important**
>
> Lorsque vous avez fini d'installer le pilote, configurez-le pour l'utiliser sur votre système. Pour plus d'informations sur la configuration du pilote, consultez Utilisation d'un gestionnaire de pilotes ODBC pour configurer le pilote.

Utilisation d'un gestionnaire de pilotes ODBC pour configurer le pilote

Sur les systèmes d'exploitation macOS, vous utilisez un gestionnaire de pilotes ODBC pour configurer les paramètres de connexion ODBC. Les gestionnaires de pilotes ODBC utilisent des fichiers de configuration pour définir et configurer les pilotes et les sources de données ODBC. Le gestionnaire de pilotes ODBC que vous utilisez s'appuie sur le système d'exploitation que vous utilisez. Pour un système d'exploitation macOS, il s'agit du gestionnaire de pilotes iODBC.

Pour plus d'informations sur les gestionnaires de pilotes ODBC pris en charge pour configurer les pilotes ODBC Amazon Redshift, consultez la section relative aux systèmes Utilisation d'un pilote ODBC Amazon Redshift sous macOS d'exploitation macOS. Consultez également « Specifying ODBC Driver Managers on Non- Windows Machines » (Spécification des gestionnaires de pilotes ODBC sur des machines non Windows) dans le Guide d'installation et de configuration du connecteur ODBC Amazon Redshift. .

Trois fichiers sont nécessaires pour configurer le pilote ODBC d'Amazon Redshift : `amazon.redshiftodbc.ini`, `odbc.ini` et `odbcinst.ini`.

Si vous l'avez installé à l'emplacement par défaut, le fichier de configuration `amazon.redshiftodbc.ini` se trouve dans `/opt/amazon/redshift/lib`.

De plus, `/opt/amazon/redshift/Setup` sous macOS, vous trouverez des exemples `odbc.ini` et `odbcinst.ini` des fichiers. Vous pouvez utiliser ces fichiers comme exemples pour configurer le pilote ODBC Amazon Redshift et le nom de la source de données (DSN).

Nous ne recommandons pas d'utiliser le répertoire d'installation du pilote ODBC d'Amazon Redshift pour les fichiers de configuration. Les fichiers du répertoire `Setup` sont proposés à titre d'exemple seulement. Si vous réinstallez le pilote ODBC Amazon Redshift ultérieurement, ou si vous effectuez une mise à niveau vers une version plus récente, le répertoire d'installation est écrasé. Vous perdez alors toute modification que vous auriez pu apporter à ces fichiers.

Pour éviter cela, copiez le fichier `amazon.redshiftodbc.ini` dans un répertoire autre que le répertoire d'installation. Si vous copiez ce fichier vers le répertoire de base de l'utilisateur, ajouter un point (.) au début du nom de fichier pour le masquer.

Pour les fichiers `odbc.ini` et `odbcinst.ini`, utilisez les fichiers de configuration dans le répertoire personnel de l'utilisateur ou créez de nouvelles versions dans un autre répertoire. Par défaut, votre système d'exploitation macOS doit comporter un `odbc.ini` fichier et un `odbcinst.ini` autre dans le répertoire personnel (`/home/$USERou~/`.) de l'utilisateur. Ces fichiers par défaut sont des fichiers cachés, ce qui est indiqué par le point (.) devant chaque nom de fichier. Ces fichiers s'affichent uniquement lorsque vous utilisez l'indicateur `-a` pour répertorier le contenu du répertoire.

Quelle que soit l'option choisie pour les fichiers `odbc.ini` et `odbcinst.ini`, modifiez les fichiers pour ajouter les informations de configuration du pilote et du DSN. Si vous avez choisi de créer de nouveaux fichiers, vous devez également définir des variables d'environnement afin de spécifier l'emplacement dans lequel se trouvent ces fichiers de configuration.

Par défaut, les gestionnaires de pilotes ODBC sont configurés pour utiliser les versions cachées des fichiers de configuration `odbc.ini` et `odbcinst.ini` (nommés `.odbc.ini` et `.odbcinst.ini`) situés dans le répertoire de base. Ils sont également configurés pour utiliser le fichier `amazon.redshiftodbc.ini` dans le sous-dossier `/lib` du répertoire d'installation du pilote. Si vous stockez ces fichiers de configuration ailleurs, définissez les variables d'environnement décrites ci-dessous afin que le gestionnaire de pilotes puisse localiser les fichiers. Pour plus d'informations, consultez « Specifying the Locations of the Driver Configuration Files » (Spécification des emplacements des fichiers de configuration du pilote) dans le Guide d'installation et de configuration du connecteur ODBC Amazon Redshift. .

Création d'un nom de source de données sur les systèmes d'exploitation macOS X

Lorsque vous vous connectez à votre magasin de données à l'aide d'un nom de source de données (DSN), configurez le fichier `odbc.ini` pour définir des DSN. Définissez les propriétés du fichier `odbc.ini` pour créer un DSN qui spécifie les informations de connexion pour votre magasin de données.

Pour plus d'informations sur la configuration du `odbc.ini` fichier, consultez la section « Création d'un nom de source de données sur une Non-Windows machine » dans le guide d'installation et de configuration du connecteur ODBC Amazon Redshift.

Utilisez le format suivant sur les systèmes d'exploitation macOS.

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/lib/amazonredshiftodbc.dylib

Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

L'exemple suivant montre la configuration pour les `odbc.ini` systèmes d'exploitation macOS.

```
[ODBC Data Sources]
Amazon_Redshift_dylib=Amazon Redshift DSN for macOS

[Amazon Redshift DSN for macOS]
Driver=/opt/amazon/redshift/lib/amazonredshiftodbc.dylib
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US
```

Configuration d'une connexion sans DSN sur les systèmes d'exploitation macOS

Pour vous connecter à votre magasin de données via une connexion qui n’a pas de DSN, définissez le pilote dans le fichier `odbcinst.ini`. Entrez ensuite une chaîne de DSN-less connexion dans votre application.

Pour plus d'informations sur la configuration du `odbcinst.ini` fichier dans ce cas, consultez la section « Configuration d'une DSN-less connexion sur une Non-Windows machine » dans le guide d'installation et de configuration du connecteur ODBC Amazon Redshift. .

Utilisez le format suivant sur les systèmes d'exploitation macOS.

```
[ODBC Drivers]
```

```
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/lib/amazonredshiftodbc.dylib

...
```

L'exemple suivant montre la `odbcinst.ini` configuration du pilote installé dans le répertoire par défaut sur les systèmes d'exploitation macOS.

```
[ODBC Drivers]
Amazon RedshiftODBC DSN=Installed

[Amazon RedshiftODBC DSN]
Description=Amazon Redshift ODBC Driver for macOS
Driver=/opt/amazon/redshift/lib/amazonredshiftodbc.dylib
```

Configuration des variables d’environnement

Utilisez le gestionnaire de pilotes ODBC approprié pour charger le pilote correct. Pour ce faire, définissez la variable d’environnement de chemin de bibliothèque. Pour plus d'informations, consultez la section « Spécification des gestionnaires de pilotes ODBC sur les Non-Windows machines » dans le guide d'installation et de configuration du connecteur ODBC Amazon Redshift. .

Par défaut, les gestionnaires de pilotes ODBC sont configurés pour utiliser les versions cachées des fichiers de configuration `odbc.ini` et `odbcinst.ini` (nommés `.odbc.ini` et `.odbcinst.ini`) situés dans le répertoire de base. Ils sont également configurés pour utiliser le fichier `amazon.redshiftodbc.ini` dans le sous-dossier `/lib` du répertoire d’installation du pilote. Si vous stockez ces fichiers de configuration ailleurs, définissez les variables d’environnement afin que le gestionnaire de pilotes puisse localiser les fichiers. Pour plus d’informations, consultez « Spécification des emplacements des fichiers de configuration du pilote » dans le Guide d’installation et de configuration du connecteur ODBC Amazon Redshift.

Configuration des fonctions de connexion

Vous pouvez configurer les fonctionnalités de connexion suivantes pour votre paramètre ODBC :

- Configurez le pilote ODBC pour fournir des informations d’identification et authentifier la connexion à la base de données Amazon Redshift.

- Configurez le pilote ODBC pour qu'il se connecte à un socket activé avec Secure Sockets Layer (SSL), si vous vous connectez à un serveur Amazon Redshift dont le SSL est activé.
- Configurez le pilote ODBC pour vous connecter à Amazon Redshift via un serveur proxy.
- Configurez le pilote ODBC pour qu'il utilise un mode de traitement des requêtes pour empêcher les requêtes de consommer trop de mémoire.
- Configurez le pilote ODBC pour qu'il transmette les processus d'authentification IAM via un serveur proxy.
- Configurez le pilote ODBC pour qu'il utilise les keepalives TCP pour empêcher la temporisation des connexions.

Pour plus d'informations sur ces fonctionnalités de connexion, consultez le Guide d'installation et de configuration du connecteur ODBC Amazon Redshift. .

Options du pilote ODBC

Vous pouvez utiliser les options de configuration pour contrôler le comportement du pilote ODBC d'Amazon Redshift.

Sous Microsoft Windows, vous définissez généralement les options du pilote lorsque vous configurez un nom de source de données (DSN). Vous pouvez également définir des options de pilote dans la chaîne de connexion lorsque vous vous connectez par programme, ou en ajoutant ou en modifiant des clés de Registre dans `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\`*`your_DSN`*. Pour plus d'informations sur la configuration d'une DSN, consultez Utilisation d'un pilote ODBC Amazon Redshift sur Microsoft Windows.

Dans macOS, vous définissez les options de configuration du pilote dans vos `amazon.redshiftodbc.ini` fichiers `odbc.ini` and, comme décrit dansUtilisation d'un gestionnaire de pilotes ODBC pour configurer le pilote. Les options de configuration définies dans un fichier `amazon.redshiftodbc.ini` s'appliquent à toutes les connexions. En revanche, les options de configuration définies dans un fichier `odbc.ini` sont spécifiques à une connexion. Les options de configuration définies dans `odbc.ini` ont priorité sur les options de configuration définies dans `amazon.redshiftodbc.ini`.

Pour plus d'informations sur la configuration des options du pilote ODBC, consultez le Guide d'installation et de configuration du connecteur ODBC Amazon Redshift. .

Versions antérieures du pilote ODBC

Ne téléchargez une version antérieure du pilote ODBC Amazon Redshift que si votre outil nécessite une version spécifique du pilote.

Versions antérieures du pilote ODBC pour Windows

Voici les pilotes 64 bits :

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.6.3.1006/AmazonRedshiftODBC64-1.6.3.1006.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.6.1.1000/AmazonRedshiftODBC64-1.6.1.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.20.1024/AmazonRedshiftODBC64-1.5.20.1024.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.16.1019/AmazonRedshiftODBC64-1.5.16.1019.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.9.1011/AmazonRedshiftODBC64-1.5.9.1011.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/AmazonRedshiftODBC64-1.5.7.1007.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/AmazonRedshiftODBC64-1.4.65.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/AmazonRedshiftODBC64-1.4.62.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC64-1.4.59.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC64-1.4.56.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.53.1000/AmazonRedshiftODBC64-1.4.53.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC64-1.4.52.1000.msi

Les pilotes 32 bits ont été abandonnés et les versions précédentes ne sont pas prises en charge.

Versions antérieures du pilote ODBC pour Linux

Les versions suivantes sont celles du pilote 64 bits :

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.6.3.1006/AmazonRedshiftODBC-64-bit-1.6.3.1006-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.6.1.1000/AmazonRedshiftODBC-64-bit-1.6.1.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.20.1024/AmazonRedshiftODBC-64-bit-1.5.20.1024-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.16.1019/AmazonRedshiftODBC-64-bit-1.5.16.1019-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.9.1011/AmazonRedshiftODBC-64-bit-1.5.9.1011-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/AmazonRedshiftODBC-64-bit-1.5.7.1007-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/AmazonRedshiftODBC-64-bit-1.4.65.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/AmazonRedshiftODBC-64-bit-1.4.62.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC-64-bit-1.4.59.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC-64-bit-1.4.59.1000-1.x86_64.deb
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC-64-bit-1.4.56.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC-64-bit-1.4.56.1000-1.x86_64.deb
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-64-bit-1.4.52.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-64-bit-1.4.52.1000-1.x86_64.deb

Les pilotes 32 bits ont été abandonnés et les versions précédentes ne sont pas prises en charge.

Versions précédentes du pilote ODBC pour macOS

Voici les versions du pilote ODBC Amazon Redshift pour macOS :

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.6.3.1006/AmazonRedshiftODBC-64-bit.1.6.3.1006.universal.pkg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.6.1.1000/AmazonRedshiftODBC-64-bit.1.6.1.1000.universal.pkg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.20.1024/AmazonRedshiftODBC-1.5.20.1024.arm64.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.20.1024/AmazonRedshiftODBC-1.5.20.1024.x86_64.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.16.1019/AmazonRedshiftODBC-1.5.16.1019.x86_64.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.9.1011/AmazonRedshiftODBC-1.5.9.1011.x86_64.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/AmazonRedshiftODBC-1.5.7.1007.x86_64.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/AmazonRedshiftODBC-1.4.65.1000.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/AmazonRedshiftODBC-1.4.62.1000.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC-1.4.59.1000.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC-1.4.56.1000.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-1.4.52.1000.dmg

Bonnes pratiques pour découvrir les métadonnées

Amazon Redshift propose plusieurs méthodes pour découvrir les métadonnées. Pour les applications et les outils, y compris ceux créés avec des agents d'intelligence artificielle, nous vous recommandons d'utiliser l'API de métadonnées du pilote ou `SHOW` les commandes pour une découverte de métadonnées cohérente, fiable et performante.

Rubriques

- Utiliser l'API de métadonnées du pilote Amazon Redshift pour les applications et les outils
- Utiliser les commandes SHOW
- Interrogation des tables du système
- Définissez la propriété de connexion du nom de l'application

Utiliser l'API de métadonnées du pilote Amazon Redshift pour les applications et les outils

Pour les applications et les outils qui se connectent à Amazon Redshift, tels qu'un outil de business intelligence ou un éditeur de requêtes, nous vous recommandons d'utiliser l'API de métadonnées de pilote fournie par les pilotes Amazon Redshift JDBC 2.x, ODBC 2.x ou Python pour découvrir les métadonnées relatives aux objets de votre entrepôt de données, notamment les bases de données, les schémas, les tables, les colonnes et les types de données. Vous pouvez également utiliser les commandes Amazon Redshift`SHOW`.

Utilisez l'API de métadonnées du pilote pour bénéficier des avantages suivants :

- Specification-compliant. Les pilotes JDBC et ODBC implémentent des interfaces de métadonnées standard (`DatabaseMetaData`en JDBC et en ODBC). `SQLTables` `SQLColumns` Étant donné que Python DB-API (PEP 249) ne définit pas de spécification d'API de métadonnées, le pilote Amazon Redshift Python suit DatabaseMetaData la spécification JDBC, fournissant des méthodes équivalentes `get_tables()` telles que`get_columns()`, et. `get_schemas()` Ces API suivent des spécifications bien définies, de sorte que votre code d'intégration est portable. Au fur et à mesure qu'Amazon Redshift fait évoluer ses tables système internes, votre application n'a pas besoin de changer.
- Performance-optimized. L'API de métadonnées du pilote est optimisée pour renvoyer les métadonnées de manière efficace. AWS continue d'investir dans les performances des API de métadonnées des pilotes.
- Forward-compatible. Amazon Redshift respecte les spécifications des connecteurs JDBC, ODBC et Python. Lorsque vous codez à l'aide de ces API standard, votre application est protégée contre toute modification de la structure du catalogue du système sous-jacent.

Exemple : utilisation de JDBC DatabaseMetaData.getTables () pour récupérer les métadonnées d'une table

```
DatabaseMetaData dbmd = connection.getMetaData();

// getTables(catalog, schemaPattern, tableNamePattern, types)
//   catalog:          "test" – filters to the database named "test"
//   schemaPattern:    "test_pattern" – filters schemas matching this pattern (supports
 SQL wildcards % and _)
//   tableNamePattern: null – no filter, returns all table names
//   types:            {"TABLE", "EXTERNAL TABLE"} – only return regular tables and
 external tables
ResultSet rs = dbmd.getTables("test", "test_pattern", null, new String[] {"TABLE",
 "EXTERNAL TABLE"});
```

Exemple : utilisation de Python cursor.get_columns () pour récupérer les métadonnées des colonnes

```
cursor: redshift_connector.Cursor = conn.cursor()

# get_columns(catalog, schema_pattern, table_name_pattern, column_name_pattern)
#   catalog:             'test' – filters to the database named "test"
#   schema_pattern:      'test_pattern' – filters schemas matching this pattern
 (supports SQL wildcards % and _)
#   table_name_pattern:  'testabc' – filters to the table named "testabc"
#   column_name_pattern: '%' – wildcard, returns all columns in the matching table
result: tuple = cursor.get_columns('test', 'test_pattern', 'testabc', '%')
```

Exemple : utilisation d'ODBC SQLPrimaryKeys () pour récupérer les métadonnées de la clé primaire

```
// SQLPrimaryKeys(hstmt, catalog, catalog_len, schema, schema_len, table, table_len)
//   catalog: "test"         – filters to the database named "test"
//   schema:  "test_schema"  – filters to the schema named "test_schema"
//   table:   "test_table"   – retrieves primary key columns for this table
// Note: Unlike getTables/getColumns, SQLPrimaryKeys does NOT support wildcard
 patterns.
retcode = SQLPrimaryKeys(hstmt, (SQLCHAR *)"test", SQL_NTS, (SQLCHAR *)"test_schema",
 SQL_NTS, (SQLCHAR *)"test_table", SQL_NTS);

while (SQL_SUCCEEDED(retcode = SQLFetch(hstmt))) {
    for (i = 1; i <= columns; i++) {
        retcode = SQLGetData(hstmt, i, SQL_C_CHAR, buf, sizeof(buf), &indicator);
    }
```

```
}
```

Exemple : utilisation d'ODBC SQLtables () pour répertorier les bases de données et les schémas

L'API ODBC ne fournit pas de fonctions distinctes pour répertorier les catalogues ou les schémas. Vous utilisez plutôt des conventions d'appel spéciales de `SQLTables()` pour récupérer ces informations.

Pour répertorier toutes les bases de données (catalogues)

Appelez `SQLTables()` avec `CatalogName` réglé sur`SQL_ALL_CATALOGS`. Définissez `SchemaName` et `TableName` pour vider les chaînes. Le jeu de résultats renvoie des valeurs valides uniquement dans la `TABLE_CAT` colonne. Toutes les autres colonnes contiennent des valeurs NULL.

```
// List all catalogs (databases) available on the data source.
retcode = SQLTables(hstmt,
    (SQLCHAR *)SQL_ALL_CATALOGS, SQL_NTS, // CatalogName = "%" (SQL_ALL_CATALOGS)
    (SQLCHAR *)"", 0,                     // SchemaName = "" (empty string)
    (SQLCHAR *)"", 0,                     // TableName  = "" (empty string)
    NULL, 0);                             // TableType  = NULL (not filtered)
```

Pour répertorier tous les schémas

Appelez `SQLTables()` avec `SchemaName` réglé sur`SQL_ALL_SCHEMAS`. Définissez `CatalogName` et `TableName` pour vider les chaînes.

```
// List all schemas available on the data source.
retcode = SQLTables(hstmt,
    (SQLCHAR *)"", 0,                     // CatalogName = "" (empty string)
    (SQLCHAR *)SQL_ALL_SCHEMAS, SQL_NTS,  // SchemaName = "%" (SQL_ALL_SCHEMAS)
    (SQLCHAR *)"", 0,                     // TableName  = "" (empty string)
    NULL, 0);                             // TableType  = NULL (not filtered)
```

> **Note**
>
> La spécification ODBC définit uniquement `TABLE_SCHEM` comme valide pour l'énumération des schémas. Amazon Redshift est également renseigné `TABLE_CAT` car il prend en charge la découverte de métadonnées entre bases de données, et chaque schéma est limité à une base de données spécifique.

Utiliser les commandes SHOW

Si l'API de métadonnées du pilote ne couvre pas votre cas d'utilisation, vous pouvez utiliser les `SHOW` commandes Amazon Redshift pour récupérer les métadonnées. `SHOW`les commandes sont optimisées pour une récupération rapide des métadonnées. Ils sont utiles lorsque vous avez besoin de métadonnées dans une session SQL interactive ou lorsque votre application se connecte via un client qui n'expose pas l'API de métadonnées du pilote.

Les `SHOW` commandes suivantes sont prises en charge pour les opérations de découverte courantes :

- AFFICHER LES BASES DE DONNÉES
- AFFICHER LES SCHÉMAS
- AFFICHER LES TABLES
- AFFICHER LES COLONNES
- AFFICHER LES CONTRAINTES
- AFFICHER LES SUBVENTIONS
- AFFICHER LES FONCTIONS
- AFFICHER LES PROCÉDURES
- AFFICHER LES PARAMÈTRES

Exemples

```
SHOW SCHEMAS FROM DATABASE dev;

database_name |     schema_name      | schema_owner | schema_type |         schema_acl
         | source_database | schema_option
--------------+----------------------+--------------+-------------
+-----------------------------+-----------------+---------------
dev           | pg_automv            |            1 | local       |
         |                 |
dev           | pg_catalog           |            1 | local       | jpuser=UC/
jpuser~=U/jpuser  |                 |
dev           | public               |            1 | local       | jpuser=UC/
jpuser~=UC/jpuser |                 |
dev           | information_schema   |            1 | local       | jpuser=UC/
jpuser~=U/jpuser  |                 |
dev           | schemad79cd6d93bf043 |            1 | local       |
         |                 |
```

```
SHOW TABLES FROM SCHEMA dev.s1 LIKE '%view' LIMIT 1;

database_name | schema_name |    table_name     | table_type |              table_acl
             | remarks | owner | last_altered_time | last_modified_time | dist_style |
  table_subtype
--------------+-------------+-------------------+------------
+-------------------------------------+---------+-------+------------------
+--------------------+------------+------------------
dev           | s1          | late_binding_view | VIEW       | {alice=arwdRxtDPA/
alice,bob=d/alice} |         | alice |                  |                    |
    | LATE BINDING VIEW
```

```
SHOW COLUMNS FROM TABLE second_db.public.t22;

 database_name | schema_name | table_name | column_name | ordinal_position |
 column_default | is_nullable |          data_type          | character_maximum_length
 | numeric_precision | numeric_scale | remarks | sort_key_type | sort_key | dist_key |
 encoding | collation
--------------+-------------+------------+-------------+------------------
+----------------+-------------+-----------------------------
+--------------------------+-------------------+---------------+---------
+---------------+----------+----------+----------+-----------
 second_db     | public      | t22        | col1        |                1 |
     | YES         | integer                     |                          |
      32 |             0 |         | INTERLEAVED   |       -1 |          | mostly8  |
 second_db     | public      | t22        | col2        |                2 |
      | YES         | character varying           |                      100 |
          |               |         | INTERLEAVED   |        2 |          | text255  |
 default
 second_db     | public      | t22        | col3        |                3 |
     | YES         | timestamp without time zone |                          |
        |               |         |               |        0 |          | raw      |
 second_db     | public      | t22        | col4        |                4 |
     | YES         | numeric                     |                          |
      10 |             2 |         |               |        0 |          | az64     |
```

Pour en savoir plus, consultez SHOW dans le Guide du développeur de base de données Amazon Redshift.

Interrogation des tables du système

Si ni l'API de métadonnées du pilote ni `SHOW` les commandes ne répondent à vos besoins, vous pouvez interroger les tables de catalogue PostgreSQL `pg_*` (), le schéma d'informations () ou les `information_schema` vues du système Amazon Redshift, par exemple directement. `SVV_TABLE_INFO`

Cette approche est utile pour les tâches d'exploration, de débogage ou d'administration ad hoc que vous exécutez à partir de requêtes SQL interactives, par exemple dans l'éditeur de requêtes Amazon Redshift v2 ou. `psql` Cependant, les structures du catalogue du système peuvent changer selon les versions d'Amazon Redshift. Nous vous déconseillons de vous fier aux requêtes directes des tables système comme interface de métadonnées pour les intégrations d'applications de production.

Lorsque vous interrogez les tables système, suivez les pratiques suivantes :

- Spécifiez la base de données, le schéma et la table. Pour de meilleures performances, incluez le nom de la base de données, le nom du schéma et le nom de la table dans vos filtres de requête. La réduction de la portée réduit la quantité de métadonnées qu'Amazon Redshift doit scanner et renvoyer.
- Utilisez des filtres d'égalité ou de type LIKE. Utilisez equality (=) ou des `LIKE` prédicats dans votre `WHERE` clause pour affiner les résultats. Évitez les requêtes non filtrées portant sur des vues de catalogue volumineuses. Ils peuvent être lents sur des clusters contenant de nombreux objets.
- Évitez les fonctions dans les prédicats de filtre. N'utilisez pas de fonctions telles que `LOWER()` la concaténation de chaînes dans votre `WHERE` clause lorsque vous filtrez des requêtes de table système. Cela empêche les recherches de métadonnées efficaces et peut dégrader de manière significative les performances des requêtes.

Exemple Anti-pattern vs. Requêtes recommandées

```
-- Avoid:
SELECT * FROM svv_all_columns;

-- Recommended:
SELECT * FROM svv_all_columns WHERE database_name = 'dev' and schema_name = 'public'
 AND table_name = 'sales';
```

```
-- Avoid:
SELECT * FROM svv_all_columns WHERE LOWER(schema_name) = 'public';
```

```
-- Recommended:
SELECT * FROM svv_all_columns WHERE schema_name = 'public' AND table_name LIKE 'sales
%';
```

```
-- Avoid:
SELECT * FROM svv_all_columns WHERE database_name || '.' || schema_name || '.' ||
 table_name = 'dev.public.sales';

-- Recommended:
SELECT * FROM svv_all_columns WHERE database_name = 'dev' and schema_name = 'public'
 AND table_name = 'sales';
```

```
-- Avoid:
SELECT * FROM svv_all_columns WHERE CONCAT(database_name, '.', schema_name) =
 'dev.public';

-- Recommended:
SELECT * FROM svv_all_columns WHERE database_name = 'dev' and schema_name = 'public';
```

Définissez la propriété de connexion du nom de l'application

Lorsque vous vous connectez à Amazon Redshift, définissez la propriété facultative du pilote de nom d'application. Cette propriété identifie l'application ou l'outil qui a établi chaque connexion, ce qui facilite la surveillance, l'audit et le dépannage de votre environnement Amazon Redshift.

Le nom de l'application que vous indiquez apparaît dans la `application_name` colonne de`SYS_CONNECTION_LOG`. Vous pouvez l'utiliser pour effectuer les opérations suivantes :

- Suivez les sources de connexion. Identifiez les applications, les services ou les outils qui se connectent à votre cluster.
- Résolvez les problèmes de performances. Corrélez les requêtes avec l'application d'origine pour isoler les problèmes de performances.
- Accès aux audits. Comprenez les modèles d'utilisation au niveau des applications dans votre entrepôt de données.

Le tableau suivant indique comment définir le nom de l'application pour chaque pilote Amazon Redshift.

Pilote	Propriété	Exemple
JDBC	`ApplicationName`	`jdbc:redshift:// endpoint:port/databas ApplicationName=my-etl-pipeline`
ODBC	`ApplicationName`	Définissez `ApplicationName=my-bi-tool` dans le DSN ou la chaîne de connexion.
Python	`application_name`	`redshift_connector.connect(..., application_name='my-data-catalog')`

Pour plus d'informations sur la propriété du nom de l'application pour chaque pilote, consultez les rubriques suivantes :

- JDBC : ApplicationName
- ODBC : ApplicationName
- Python : nom_application

> **Note**
>
> Utilisez une convention de dénomination descriptive et cohérente pour les noms d'applications, telle que *team*-*service*-*environment* (par exemple,`quicksight-analytics-dashboard-prod`). Cette approche facilite le filtrage et l'analyse `SYS_CONNECTION_LOG` des données.

Configuration des options de sécurité des connexions

Amazon Redshift prend en charge les connexions SSL (Secure Sockets Layer) pour chiffrer les données et les certificats de serveur pour valider le certificat du serveur auquel le client se connecte.

SSL

Pour prendre en charge les connexions SSL, Amazon Redshift crée et installe un certificat SSL émis par AWS Certificate Manager (ACM) sur chaque cluster. Les certificats ACM sont publiquement approuvés par la plupart des systèmes d'exploitation, des navigateurs web et des clients. Vous pourriez devoir télécharger une solution groupée de certificats si vos clients ou applications SQL se connectent à Amazon Redshift en utilisant SSL avec l'option de connexion `sslmode` définie sur `require`, `verify-ca` ou `verify-full`. Si votre client a besoin d'un certificat, Amazon Redshift fournit un certificat de solution groupée comme suit :

> **Note**
>
> Nous vous recommandons d'utiliser `verify-full` des connexions SSL dans la mesure du possible.

- Téléchargez le bundle depuis https://s3.amazonaws.com/redshift-downloads/amazon-trust-ca-bundle.crt.
  - Le numéro de total de contrôle MD5 prévu est 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - Le numéro de total de contrôle sha256 est 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

  N'utilisez pas la solution groupée de certificats précédente qui se trouvait à l'adresse `https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt`.
- En Chine Région AWS, téléchargez le bundle depuis https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt.
  - Le numéro de total de contrôle MD5 prévu est 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - Le numéro de total de contrôle sha256 est 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

  N'utilisez pas les solutions groupées de certificats antérieures qui se trouvait à l'adresse `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt` et `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem`.

> **Important**
>
> Amazon Redshift a changé la méthode de gestion des certificats SSL. Il se peut que vous ayez besoin de mettre à jour vos certificats actuels d'autorité de certification racine approuvée pour pouvoir continuer à vous connecter à vos clusters à l'aide du protocole SSL. Pour plus d'informations, consultez Transition vers les certificats ACM pour les connexions SSL.

Par défaut, les bases de données du cluster acceptent une connexion qu'elle s'appuie sur le protocole SSL ou non. Pour configurer votre cluster afin d'exiger une connexion SSL, définissez le paramètre `require_SSL` sur `true` dans le groupe de paramètres associé au cluster.

Amazon Redshift prend en charge un mode SSL conforme à la norme FIPS (Federal Information Processing Standard) 140-2. FIPS-compliant Le mode SSL est désactivé par défaut.

> **Important**
>
> Activez le mode FIPS-compliant SSL uniquement si votre système est requis FIPS-compliant.

Pour activer le mode FIPS-compliant SSL, définissez le `use_fips_ssl` paramètre et le `require_SSL` paramètre sur `true` dans le groupe de paramètres associé au cluster Amazon Redshift ou au groupe de travail Redshift Serverless. Pour plus d'informations sur la modification d'un groupe de paramètres sur un cluster, consultez Groupes de paramètres Amazon Redshift. Pour plus d'informations sur la modification d'un groupe de paramètres sur un groupe de travail, consultez Configuration d'une connexion FIPS-compliant SSL à Amazon Redshift Serverless.

Amazon Redshift prend en charge le protocole d'accord de clé Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). Avec le protocole ECDHE, le client et le serveur disposent chacun d'une paire de clés publiques-privées à courbes elliptiques qui permettent d'établir un secret partagé via un canal non sécurisé. Vous n'avez pas besoin de configurer quoi que ce soit dans Amazon Redshift pour activer ECDHE. Si vous vous connectez à partir d'un outil client SQL qui utilise le protocole ECDHE pour chiffrer les communications entre le client et le serveur, Amazon Redshift utilise la liste de chiffrement fournie pour établir les connexions appropriées. Pour plus d'informations, consultez Elliptic curve diffie—hellman sur Wikipedia et Ciphers sur le site d'OpenSSL.

Protocole SSL et certificats CA approuvés dans ODBC

Si vous vous connectez à l'aide des derniers pilotes ODBC Amazon Redshift (version 1.3.7.1000 ou ultérieure), vous pouvez ignorer cette section. Pour télécharger les pilotes les plus récents, consultez Configuration d'une connexion pour le pilote ODBC version 2.x pour Amazon Redshift.

Il se peut que vous ayez besoin de mettre à jour vos certificats actuels d'autorité de certification racine approuvée pour pouvoir continuer à vous connecter à vos clusters à l'aide du protocole SSL. Pour plus d'informations, consultez SSL.

Vous pouvez vérifier que le certificat que vous avez téléchargé correspond au chiffre de la somme de contrôle MD5 attendu. Pour ce faire, vous pouvez utiliser le programme MD5sum sur les systèmes d'exploitation Linux ou un autre outil sur les systèmes d'exploitation Windows et macOS.

Les DSN ODBC contiennent un paramètre `sslmode` qui détermine comment gérer le cryptage pour les connexions client et la vérification du certificat du serveur. Amazon Redshift prend en charge les valeurs `sslmode` suivantes à partir de la connexion client :

- `disable`

  Le protocole SSL est désactivé et la connexion n'est pas chiffrée.
- `allow`

  Le protocole SSL est utilisé si le serveur l'exige.
- `prefer`

  Le protocole SSL est utilisé si le serveur le prend en charge. Amazon Redshift prend en charge le protocole SSL. Celui-ci est donc utilisé lorsque vous définissez le `sslmode` sur `prefer`.
- `require`

  Le protocole SSL est obligatoire.
- `verify-ca`

  Le protocole SSL doit être utilisé et le certificat de serveur doit être vérifié.
- `verify-full`

  Le protocole SSL doit être utilisé. Le certificat de serveur doit être vérifié et le nom d'hôte du serveur doit correspondre à l'attribut de nom d'hôte sur le certificat.

Vous pouvez déterminer si SSL est utilisé et les certificats de serveur sont vérifiés dans une connexion entre le client et le serveur. Pour ce faire, vous devez revoir le paramètre `sslmode` pour votre DSN ODBC sur le client et le paramètre `require_SSL` pour le cluster Amazon Redshift sur le serveur. Le tableau suivant décrit le résultat du chiffrement pour les différentes combinaisons de paramètres client et serveur :

sslmode (client)	require_SSL (serveur)	Résultat
`disable`	`false`	La connexion n'est pas chiffrée.
`disable`	`true`	La connexion ne peut pas être établie, car le serveur requiert le protocole SSL qui est désactivé sur le client pour la connexion.
`allow`	`true`	La connexion est chiffrée.
`allow`	`false`	La connexion n'est pas chiffrée.
`prefer` ou `require`	`true`	La connexion est chiffrée.
`prefer` ou `require`	`false`	La connexion est chiffrée.
`verify-ca`	`true`	La connexion est chiffrée et le certificat de serveur est vérifié.
`verify-ca`	`false`	La connexion est chiffrée et le certificat de serveur est vérifié.
`verify-full`	`true`	La connexion est chiffrée et le certificat de serveur et le nom d'hôte sont vérifiés.
`verify-full`	`false`	La connexion est chiffrée et le certificat de serveur et le nom d'hôte sont vérifiés.

Connexion à l'aide du certificat de serveur avec ODBC sous Microsoft Windows

Si vous souhaitez vous connecter à votre cluster en utilisant SSL et le certificat du serveur, téléchargez d'abord le certificat sur votre ordinateur client ou votre instance Amazon EC2. Configurez ensuite le DSN ODBC.

1. Téléchargez la solution groupée d'autorité de certification Amazon Redshift sur votre ordinateur client dans le dossier `lib` du répertoire d'installation de votre pilote, et enregistrez le fichier en tant que `root.crt`. Pour obtenir des informations sur le téléchargement, consultez SSL.
2. Ouvrez Administrateur de sources de données ODBC et ajoutez ou modifiez l'entrée de la DSN système pour votre connexion ODBC. Pour Mode SSL, sélectionnez `verify-full` à moins que vous n'utilisiez un alias DNS. Si vous utilisez un alias DNS, sélectionnez `verify-ca`. Ensuite, choisissez Save (Enregistrer).

   Pour plus d'informations sur la configuration de la DSN ODBC, consultez Configuration d'une connexion pour le pilote ODBC version 2.x pour Amazon Redshift.

Protocole SSL et certificats de serveur dans Java

Le protocole SSL fournit une couche de sécurité en chiffrant les données qui se déplacent entre votre client et le cluster. L'utilisation d'un certificat de serveur fournit une couche supplémentaire de sécurité en validant que le cluster est un cluster Amazon Redshift. Pour cela, il vérifie le certificat de serveur installé automatiquement sur tous les clusters que vous mettez en service. Pour plus d'informations sur l'utilisation de certificats de serveur avec JDBC, accédez à la page de configuration du client de la documentation sur PostgreSQL.

Connexion à l'aide de certificats d'autorités de certification approuvées dans Java

> **Important**
>
> Amazon Redshift a changé la méthode de gestion des certificats SSL. Il se peut que vous ayez besoin de mettre à jour vos certificats actuels d'autorité de certification racine approuvée pour pouvoir continuer à vous connecter à vos clusters à l'aide du protocole SSL. Pour plus d'informations, consultez SSL.

Pour se connecter à l'aide de certificats d'autorités de certification approuvées

Vous pouvez utiliser le `redshift-keytool.jar` fichier pour importer les certificats CA du bundle Amazon Redshift Certificate Authority dans un Java TrustStore ou dans un fichier privé. TrustStore

1. Si vous utilisez l'option de ligne de commande Java `-Djavax.net.ssl.trustStore`, supprimez-la de la ligne de commande, si possible.
2. Téléchargez redshift-keytool.jar.
3. Effectuez l'une des actions suivantes :

   - Pour importer le bundle Amazon Redshift Certificate Authority dans un Java TrustStore, exécutez la commande suivante.

     ```
     java -jar redshift-keytool.jar -s
     ```

   - Pour importer le bundle Amazon Redshift Certificate Authority dans votre compte privé TrustStore, exécutez la commande suivante :

     ```
     java -jar redshift-keytool.jar -k <your_private_trust_store> -
     p <keystore_password>
     ```

Transition vers les certificats ACM pour les connexions SSL

Amazon Redshift remplace les certificats SSL sur vos clusters par des certificats émis par AWS Certificate Manager (ACM). ACM est une autorité de certification publique de confiance, approuvée par la plupart des systèmes actuels. Il se peut que vous ayez besoin de mettre à jour vos certificats actuels d'autorité de certification racine approuvée pour pouvoir continuer à vous connecter à vos clusters à l'aide du protocole SSL.

Cette modification ne vous affecte que si l'ensemble des conditions suivantes s'applique :

- Vos clients ou applications SQL se connectent aux clusters Amazon Redshift à l'aide du protocole SSL avec l'option de connexion `sslMode` définie sur l'option de configuration `require`, `verify-ca` ou `verify-full`.
- Vous n'utilisez pas les pilotes ODBC ou JDBC d'Amazon Redshift, ou vous utilisez des pilotes Amazon Redshift antérieurs à ODBC version 1.3.7.1000 ou JDBC version 1.2.8.1005.

Si ce changement vous affecte sur les régions commerciales Amazon Redshift, alors vous devez mettre à jour vos certificats AC racine de confiance actuels avant le 23 octobre 2017. Amazon

Redshift assurera la transition de vos clusters afin qu'ils utilisent les certificats ACM entre aujourd'hui et le 23 octobre 2017. La modification n'aura aucun effet ou presque sur les performances ou la disponibilité de votre cluster.

Si cette modification vous concerne dans les régions AWS GovCloud (US) (États-Unis), vous devez mettre à jour vos certificats Trust Root CA actuels avant le 1er avril 2020 pour éviter toute interruption de service. À partir de cette date, les clients qui se connectent aux clusters Amazon Redshift en utilisant des connexions cryptées SSL ont besoin d'une autorité de certification (AC) de confiance supplémentaire. Les clients utilisent des autorités de certification de confiance pour confirmer l'identité du cluster Amazon Redshift lorsqu'ils s'y connectent. Votre action est requise pour mettre à jour vos clients et applications SQL afin d'utiliser un bundle de certificats mis à jour qui inclut la nouvelle autorité de certification approuvée.

> **Important**
>
> Dans les régions de Chine, le 5 janvier 2021, Amazon Redshift remplace les certificats SSL de vos clusters par des certificats émis AWS Certificate Manager (ACM). Si ce changement vous affecte sur la région de la Chine (Beijing) ou la région de la Chine (Ningxia), vous devez mettre à jour vos certificats d'autorité de certification racine approuvés actuels avant le 5 janvier 2021 pour éviter toute interruption de service. À partir de cette date, les clients qui se connectent aux clusters Amazon Redshift en utilisant des connexions cryptées SSL ont besoin d'une autorité de certification (AC) de confiance supplémentaire. Les clients utilisent des autorités de certification de confiance pour confirmer l'identité du cluster Amazon Redshift lorsqu'ils s'y connectent. Votre action est requise pour mettre à jour vos clients et applications SQL afin d'utiliser un bundle de certificats mis à jour qui inclut la nouvelle autorité de certification approuvée.

- Utilisation des derniers pilotes ODBC ou JDBC d'Amazon Redshift
- Utilisation de pilotes ODBC ou JDBC antérieurs d'Amazon Redshift
- Utilisation d'autres types de connexion SSL

Utilisation des derniers pilotes ODBC ou JDBC d'Amazon Redshift

La méthode privilégiée consiste à utiliser les derniers pilotes ODBC ou JDBC Amazon Redshift. Les pilotes Amazon Redshift à partir des versions ODBC 1.3.7.1000 et JDBC 1.2.8.1005 gèrent automatiquement la transition entre un certificat Amazon Redshift auto-signé et un certificat ACM.

Pour télécharger les pilotes les plus récents, consultez Configuration d'une connexion pour la version 2.x du pilote JDBC pour Amazon Redshift.

Si vous utilisez le dernier pilote JDBC Amazon Redshift, il est préférable de ne pas utiliser `-Djavax.net.ssl.trustStore` dans les options JVM. Si vous devez utiliser `-Djavax.net.ssl.trustStore`, importez le bundle d'autorités de certification Redshift dans le truststore vers lequel il pointe. Pour obtenir des informations sur le téléchargement, consultez SSL. Pour plus d'informations, consultez Importation du bundle d'autorités de certification Amazon Redshift dans un TrustStore.

Utilisation de pilotes ODBC ou JDBC antérieurs d'Amazon Redshift

- Si votre ODBC DSN est configuré avec `SSLCertPath`, remplacez le fichier de certificats dans le chemin spécifié.
- Si `SSLCertPath` n'est pas défini, remplacez le fichier de certificat nommé `root.crt` dans l'emplacement DLL du pilote.

Si vous devez utiliser un pilote JDBC Amazon Redshift antérieur à la version 1.2.8.1005, effectuez l'une des opérations suivantes :

- Si votre chaîne de connexion JDBC utilise l'option `sslCert`, supprimez l'option `sslCert`. Importez ensuite le bundle d'autorités de certification Redshift dans votre Java. TrustStore Pour obtenir des informations sur le téléchargement, consultez SSL. Pour plus d'informations, consultez Importation du bundle d'autorités de certification Amazon Redshift dans un TrustStore.
- Si vous utilisez l'option de ligne de commande Java `-Djavax.net.ssl.trustStore`, supprimez-la de la ligne de commande, si possible. Importez ensuite le bundle d'autorités de certification Redshift dans votre Java. TrustStore Pour obtenir des informations sur le téléchargement, consultez SSL. Pour plus d'informations, consultez Importation du bundle d'autorités de certification Amazon Redshift dans un TrustStore.

Importation du bundle d'autorités de certification Amazon Redshift dans un TrustStore

Vous pouvez les utiliser `redshift-keytool.jar` pour importer les certificats CA du bundle Amazon Redshift Certificate Authority dans un environnement Java TrustStore ou dans votre boutique de confiance privée.

Pour importer le bundle d'autorités de certification Amazon Redshift dans un TrustStore

1. Téléchargez redshift-keytool.jar.
2. Effectuez l’une des actions suivantes :

   - Pour importer le bundle Amazon Redshift Certificate Authority dans un Java TrustStore, exécutez la commande suivante.

     ```
     java -jar redshift-keytool.jar -s
     ```

   - Pour importer le bundle Amazon Redshift Certificate Authority dans votre compte privé TrustStore, exécutez la commande suivante :

     ```
     java -jar redshift-keytool.jar -k <your_private_trust_store> -
     p <keystore_password>
     ```

Utilisation d’autres types de connexion SSL

Si vous souhaitez vous connecter à l’aide de l’une des solutions ci-dessous, suivez les étapes décrites dans cette section :

- Pilote ODBC open source
- Pilote JDBC open source
- Interface de ligne de commande Amazon Redshift RSQL
- Toute liaison de langages basée sur libpq, telle que psycopg2 (Python) et ruby-pg (Ruby)

Pour utiliser les certificats ACM avec d’autres types de connexion SSL :

1. Téléchargez le Paquet d’autorité de certification Amazon Redshift. Pour obtenir des informations sur le téléchargement, consultez SSL.
2. Placez les certificats du bundle dans votre fichier `root.crt`.

   - Sur les systèmes d'exploitation Linux et macOS, le fichier est`~/.postgresql/root.crt`.
   - Sous Microsoft Windows, le fichier est `%APPDATA%\postgresql\root.crt`

Connexion à partir d’outils et de codes clients

Amazon Redshift fournit Amazon Redshift Query Editor V2 pour se connecter à vos clusters et groupes de travail. Pour plus d’informations, consultez Interrogation d’une base de données à l’aide de l’éditeur de requête v2.

Cette section propose quelques options pour la connexion d’outils tiers. En outre, elle explique comment vous connecter à votre cluster par programmation.

Rubriques

- Connexion avec Amazon Redshift RSQL
- Connexion à un cluster avec Amazon Redshift RSQL
- Méta-commandes Amazon Redshift RSQL
- Variables Amazon Redshift RSQL
- Codes d’erreur Amazon Redshift RSQL
- Variables d’environnement Amazon Redshift RSQL

Connexion avec Amazon Redshift RSQL

Amazon Redshift RSQL est un client en ligne de commande permettant d’interagir avec les clusters et bases de données Amazon Redshift. Vous pouvez vous connecter à un cluster Amazon Redshift, décrire des objets de base de données, interroger des données et afficher les résultats des requêtes dans différents formats de sortie.

Amazon Redshift RSQL prend en charge les fonctionnalités de l’outil de ligne de commande PostgreSQL psql avec un ensemble supplémentaire de fonctionnalités spécifiques à Amazon Redshift. Cela inclut les éléments suivants :

- Vous pouvez utiliser l'authentification unique à l'aide d'AD FS, d'Okta PingIdentity, d'Azure AdM ou d'autres fournisseurs d'identité SAML/JWT basés. Vous pouvez également utiliser des fournisseurs d’identité SAML basés sur un navigateur pour l’authentification multifactorielle (MFA).
- Vous pouvez décrire les propriétés ou les attributs des objets Amazon Redshift tels que les clés de distribution de table, les clés de tri de table, les vues de liaison tardive (LBV) et les vues matérialisées. Vous pouvez également décrire les propriétés ou les attributs des tables externes d'un AWS Glue catalogue ou d'Apache Hive Metastore, des bases de données externes dans Amazon RDS pour PostgreSQL, Amazon Aurora Edition, RDS pour MySQL (version préliminaire)

et PostgreSQL-Compatible Amazon Aurora Edition (version préliminaire), ainsi que des tables partagées MySQL-Compatible à l'aide du partage de données Amazon Redshift.

- Vous pouvez également utiliser des commandes de flux de contrôle améliorées telles que `IF` (`\ELSEIF`, `\ELSE`, `\ENDIF`), `\GOTO` et `\LABEL`.

Avec le mode de traitement par lots Amazon Redshift RSQL, qui exécute un script transmis en tant que paramètre d'entrée, vous pouvez exécuter des scripts comprenant à la fois SQL et une logique métier complexe. Si vous avez déjà des entrepôts des données sur site autogérés, vous pouvez utiliser Amazon Redshift RSQL pour remplacer les scripts d'extraction, de transfert, de chargement (ETL) et d'automatisation existants, tels que les scripts BTEQ Teradata. L'utilisation de RSQL permet d'éviter de réimplémenter manuellement des scripts dans un langage procédural.

Amazon Redshift RSQL est disponible pour les systèmes d'exploitation Linux, Windows et macOS.

Pour signaler les problèmes liés à Amazon Redshift RSQL, écrivez à `<redshift-rsql-support@amazon.com>`.

Rubriques

- Premiers pas avec Amazon Redshift RSQL
- Journal des modifications Amazon Redshift RSQL

Premiers pas avec Amazon Redshift RSQL

Installez Amazon Redshift RSQL sur un ordinateur doté d'un système d'exploitation Linux, macOS ou Microsoft Windows.

Téléchargement de RSQL

-
  -
-
-

Consultez le journal des modifications et les téléchargements des versions antérieures à l'adresse Journal des modifications Amazon Redshift RSQL.

Installation de RSQL pour Linux

Suivez les étapes ci-dessous pour installer RSQL pour Linux.

1. Installez le gestionnaire de pilotes à l'aide de la commande suivante :

```
sudo yum install unixODBC
```

2. Installez le pilote ODBC : Téléchargement et installation du pilote ODBC Amazon Redshift.
3. Copiez le fichier ini dans votre répertoire de base :

```
cp /opt/amazon/redshiftodbcx64/odbc.ini ~/.odbc.ini
```

4. Définissez les variables d'environnement pour qu'elles pointent vers l'emplacement du fichier :

```
export ODBCINI=~/.odbc.ini
export ODBCSYSINI=/opt/amazon/redshiftodbcx64/
export AMAZONREDSHIFTODBCINI=/opt/amazon/redshiftodbcx64/amazon.redshiftodbc.ini
```

5. Vous pouvez désormais installer RSQL en exécutant la commande suivante.

```
sudo rpm -i AmazonRedshiftRsql-<version>.rhel.x86_64.rpm
```

Installation de RSQL pour Mac

Suivez les étapes ci-dessous pour installer RSQL pour Mac OSX.

1. Installez le gestionnaire de pilotes à l'aide de la commande suivante :

```
brew install unixodbc --build-from-source
```

2. Installez le pilote ODBC : Téléchargement et installation du pilote ODBC Amazon Redshift.
3. Copiez le fichier ini dans votre répertoire de base :

```
cp /opt/amazon/redshift/Setup/odbc.ini ~/.odbc.ini
```

4. Définissez les variables d'environnement pour qu'elles pointent vers l'emplacement du fichier :

```
export ODBCINI=~/.odbc.ini
export ODBCSYSINI=/opt/amazon/redshift/Setup
```

```
export AMAZONREDSHIFTODBCINI=/opt/amazon/redshift/lib/amazon.redshiftodbc.ini
```

5. Définissez DYLD_LIBRARY_PATH à l'emplacement de votre libodbc.dylib s'il n'est pas dans /usr/local/lib.

```
export DYLD_LIBRARY_PATH=$DYLD_LIBRARY_PATH:/usr/local/lib
```

6. Double-click le fichier pkg pour exécuter le programme d'installation.
7. Suivez les étapes décrites dans le programme d'installation pour terminer l'installation. Acceptez les termes du contrat de licence.

Installation de RSQL pour Windows

Suivez les étapes ci-dessous pour installer RSQL pour Windows.

1. Installez le pilote ODBC : Téléchargement et installation du pilote ODBC Amazon Redshift.
2. Double-click le fichier de téléchargement RSQL pour exécuter le programme d'installation, puis suivez les instructions pour terminer l'installation.

Journal des modifications Amazon Redshift RSQL

1.1.2 (11/12/2025)

Correctifs de bogue

- Correction d'un bogue qui provoquait des échecs avec les commandes \ goto et \ label.
- Correction d'un bogue qui empêchait RSQL d'imprimer les valeurs des variables lorsque celles-ci étaient placées entre guillemets.
- Correction d'un bogue qui provoquait des blocages de RSQL lorsque les résultats de la requête dépassaient la taille du paramètre ODBC DSN Fetch alors qu'il était activé. UseDeclareFetch
- Correction d'un problème en raison duquel plusieurs pages de résultats étaient renvoyées en même temps même si le téléavertisseur était activé.
- Correction d'un bogue qui provoquait des blocages de RSQL lorsque des requêtes échouaient dans des blocs de transactions.

1.1.1 (20-11-2025)

Correctifs de bogue

- Correction d'un problème en raison duquel RSQL analysait incorrectement les requêtes lors de l'utilisation de l'indicateur -c. Ce correctif s'applique à toutes les plateformes.
- Correction d'un bogue sur Mac qui empêchait les utilisateurs d'utiliser la commande \ s dans RSQL.

1,10 (11/11/2025)

Correctifs de bogue

- Résolution d'un problème de fuite de mémoire qui provoquait des blocages inattendus dans RSQL.
- Suppression de la dépendance OpenSSL de RSQL.
- Correction de conflits de liens avec libpq/psql des installations situées dans le même environnement.
- Compatibilité de plateforme améliorée pour Amazon Linux 2023, Windows et macOS.
- Correction d'un problème à cause duquel la sortie était tronquée en cas de dépassement de la taille d'affichage actuelle.

1.0.8 (2023-06-19)

Correctifs de bogue

- Correction d’un problème où la sortie était tronquée avec les commandes SHOW.
- Ajout de la prise en charge de \de pour la description des flux Kinesis externes et des rubriques Kafka.

1.0.7 (2023-03-22)

Correctifs de bogue

- Correction d’un problème où RSQL ne pouvait pas décrire les vues matérialisées.
- Correction de l’erreur d’autorisation refusée sur stl_connection_log lors de l’utilisation d’Amazon Redshift sans serveur.
- Correction d’un problème où RSQL pouvait traiter les étiquettes \GOTO de manière incorrecte.
- Correction d’un problème d’impression des messages SSL en mode silencieux.
- Correction d’un problème d’affichage de caractères aléatoires lors de la description de procédures stockées.

- Correction d'un problème lié à l'impression de ERROR/INFO messages dupliqués.

Nouveau

- RSQL obtient désormais les informations SSL directement à partir du pilote ODBC.

1.0.6 (2023-02-21)

Correctifs de bogue

- Correction d’un problème où \d renvoie une erreur - syntaxe d’entrée invalide pour l’entier : "xid" - sur le correctif Redshift 1.0.46086 (P173).

Nouveau

- Les fichiers d’installation ont été renommés pour refléter l’architecture prise en charge.

1.0.5 (27/06/2022)

Correctifs de bogue

- Envoyer des messages d’erreur SQL à l’erreur standard (stderr).
- Correction d’un problème avec les codes de sortie lors de l’utilisation de ON_ERROR_STOP. Les scripts s’arrêtent désormais après avoir rencontré une erreur et renvoient les bons codes de sortie.
- Maxerror n’est plus sensible à la casse.

Nouveau

- Ajout de la prise en charge du pilote ODBC 2.x.

1.0.4 (2022-03-19)

- Prise en charge de la variable d’environnement RSPASSWORD. Définissez un mot de passe pour vous connecter à Amazon Redshift. Par exemple : `export RSPASSW0RD=TestPassw0rd`.

1.0.3 (2021-12-08)

Correctifs de bogue

- Correction d'une fenêtre contextuelle de boîte de dialogue lors de l'utilisation de `\c` ou de `\logon` pour basculer entre les bases de données sous Windows OS.
- Correction d'un crash lors de la vérification des informations ssl.

Versions antérieures d'Amazon Redshift RSQL

Choisissez l'un des liens pour télécharger la version d'Amazon Redshift RSQL dont vous avez besoin, en fonction de votre système d'exploitation.

Linux 64 bits RPM

- Version 1.1.1 de RSQL
- Version 1.1.0 de RSQL
- Version 1.0.8 de RSQL
- RSQL Version 1.0.7
- RSQL Version 1.0.6
- RSQL Version 1.0.5
- RSQL Version 1.0.4
- Fichier RSQL version 1.0.3
- Fichier RSQL version 1.0.1

Mac OS 64 bits DMG/PKG

- Version 1.1.1 de RSQL
- Version 1.1.0 de RSQL
- Version 1.0.8 de RSQL
- RSQL Version 1.0.7
- RSQL Version 1.0.6
- Fichier RSQL version 1.0.5

- Fichier RSQL version 1.0.4
- Fichier RSQL version 1.0.3
- Fichier RSQL64 version 1.0.1. Dans la région Chine (Beijing), utilisez le lien suivant :

MSI Windows 64 bits

- Version 1.1.1 de RSQL
- Version 1.1.0 de RSQL
- Version 1.0.8 de RSQL
- RSQL Version 1.0.7
- RSQL Version 1.0.6
- RSQL Version 1.0.5
- RSQL Version 1.0.4
- Fichier RSQL version 1.0.3
- RSQL version 1.0.1.

Connexion à un cluster avec Amazon Redshift RSQL

Avec Amazon Redshift, vous pouvez vous connecter à un cluster et interagir avec eux à l'aide de RSQL. Il s'agit d'un outil de ligne de commande qui fournit un moyen sécurisé d'interroger des données, de créer des objets de base de données et de gérer votre cluster Amazon Redshift. Les sections suivantes vous indiquent les étapes à suivre pour établir une connexion à votre cluster à l'aide de RSQL avec ou sans nom de source de données (DSN).

Connexion sans DSN

1. Sur la console Amazon Redshift, choisissez le cluster auquel vous souhaitez vous connecter et notez le point de terminaison, la base de données et le port.
2. A l'invite de commande, spécifiez les informations de connexion à l'aide des paramètres de ligne de commande.

   ```
   rsql -h <endpoint> -U <username> -d <databasename> -p <port>
   ```

   Ici, les éléments suivants s'appliquent :

- *<endpoint>*est le point de terminaison que vous avez enregistré à l'étape précédente.
- *<username>*est le nom d'un utilisateur autorisé à se connecter au cluster.
- *<databasename>*est le nom de la base de données que vous avez enregistré à l'étape précédente.
- *<port>*est le port que vous avez enregistré à l'étape précédente. *<port>*est un paramètre facultatif.

Un exemple suit.

```
rsql -h testcluster.example.amazonaws.com -U user1 -d dev -p 5439
```

3. À l'invite de mot de passe, entrez le mot de passe de l'*<username>*utilisateur.

   Une réponse de connexion réussie ressemble à ce qui suit.

```
% rsql -h testcluster.example.com -d dev -U user1 -p 5349
Password for user user1:
DSN-less Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=#
```

La commande de connexion possède les mêmes paramètres sous Linux, Mac OS et Windows.

Connexion avec un DSN

Vous pouvez connecter RSQL à Amazon Redshift à l'aide d'un DSN afin de simplifier l'organisation des propriétés de connexion. Cette rubrique inclut des instructions d'installation et des descriptions ODBC-driver des propriétés DSN.

Utilisation d’une connexion DSN avec un mot de passe

Voici un exemple de DSN-connection configuration utilisant un mot de passe. La valeur par défaut `<path to driver>` pour Mac OS X est `/opt/amazon/redshift/lib/`

`libamazonredshiftodbc.dylib` et pour Linux, il s'agit de `/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so`.

```
[testuser]
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
SSLMode=verify-ca
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
Port=<database port>
Database=<dbname>
UID=<username>
PWD=<password>
sslmode=prefer
```

La sortie suivante résulte d'une connexion réussie.

```
% rsql -D testuser
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=#
```

Utilisation du DSN à authentification unique

Vous pouvez configurer un DSN pour l'authentification unique. Voici un exemple de DSN-connection configuration qui utilise l'authentification unique Okta.

```
[testokta]
Driver=<path to driver>
SSLMode=verify-ca
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
clusterid=<cluster id>
region=<region name>
Database=<dbname>
```

```
locale=en-US
iam=1
plugin_name=<plugin name>
uid=<okta username>
pwd=<okta password>
idp_host=<idp endpoint>
app_id=<app id>
app_name=<app name>
preferred_role=<role arn>
```

Exemple de sortie d'une connexion réussie.

```
% rsql -D testokta
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=#
```

L'exemple suivant montre un exemple de DSN-connection configuration qui utilise l'authentification unique Azure.

```
[testazure]
Driver=<path to driver>
SSLMode=verify-ca
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
Port=<cluster port>
clusterid=<cluster id>
region=<region name>
Database=<dbname>
locale=en-us
iam=1
plugin_name=<plugin name>
uid=<azure username>
pwd=<azure password>
idp_tenant=<Azure idp tenant uuid>
client_id=<Azure idp client uuid>
```

```
client_secret=<Azure idp client secret>
```

Utilisation d’une connexion DSN avec un profil IAM

Vous pouvez vous connecter à Amazon Redshift à l’aide de votre profil IAM configuré. Le profil IAM doit être autorisé à appeler `GetClusterCredentials`. L’exemple suivant illustre les propriétés DSN à utiliser. Les paramètres `ClusterID` et `Region` ne sont obligatoires que si l’`Host` n’est pas un point de terminaison fourni par Amazon comme `examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com`.

```
[testiam]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
Profile=default
```

La valeur de la `Profile` clé est le profil nommé que vous avez choisi parmi les informations d'identification de votre AWS CLI. Cet exemple montre les informations d’identification du profil nommé `default`.

```
$ cat .aws/credentials
[default]
aws_access_key_id = ASIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

L’exemple de réponse de connexion est le suivant.

```
$ rsql -D testiam
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) testuser@dev=>
```

Utilisation d’une connexion DSN avec un profil d’instance

Vous pouvez vous connecter à Amazon Redshift à l’aide de votre profil d’instance Amazon EC2. Le profil d’instance doit être autorisé à appeler `GetClusterCredentials`. Voir l’exemple ci-dessous pour connaître les propriétés DSN à utiliser. Les paramètres `ClusterID` et `Region` ne sont obligatoires que si l’`Host` n’est pas un point de terminaison fourni par Amazon comme `examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com`.

```
[testinstanceprofile]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
Instanceprofile=1
```

L’exemple de réponse de connexion est le suivant.

```
$ rsql -D testinstanceprofile
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) testuser@dev=>
```

Utilisation d’une connexion DSN avec la chaîne de fournisseurs d’informations d’identification par défaut

Pour vous connecter à l'aide de la chaîne de fournisseurs d'informations d'identification par défaut, spécifiez uniquement la propriété IAM, et Amazon Redshift RSQL tentera d'obtenir les informations d'identification dans l'ordre décrit dans la section Utilisation des informations d'identification dans le AWS SDK for Java. AWS Au moins un des fournisseurs de la chaîne doit disposer de l’autorisation `GetClusterCredentials`. Cela est utile pour se connecter à partir de conteneurs ECS, par exemple.

```
[iamcredentials]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
```

Méta-commandes Amazon Redshift RSQL

Les méta-commandes Amazon Redshift RSQL renvoient des enregistrements informatifs sur des bases de données ou des objets de base de données spécifiques. Les résultats peuvent inclure diverses colonnes et métadonnées. D'autres commandes effectuent des actions spécifiques. Ces commandes sont précédées d'une barre oblique inverse.

\d[S+]

Répertorie les tables créées par les utilisateurs locaux, les vues régulières, les vues à liaison tardive et les vues matérialisées. `\dS` répertorie également les tableaux et les vues, comme \d, mais les objets système sont inclus dans les enregistrements renvoyés. Le + a pour résultat la colonne de métadonnées supplémentaires `description` pour tous les objets répertoriés. Les exemples d'enregistrements suivants sont renvoyés à la suite de la commande.

```
List of relations
 schema |   name    | type  |  owner
--------+-----------+-------+---------
 public | category  | table | awsuser
 public | date      | table | awsuser
 public | event     | table | awsuser
 public | listing   | table | awsuser
 public | sales     | table | awsuser
 public | users     | table | awsuser
 public | venue     | table | awsuser
(7 rows)
```

\d[S+] NAME

Décrit une table, une vue ou un index. Inclut les noms et les types de colonnes. Il fournit également le style de distribution diststyle, la configuration de sauvegarde, la date de création (tables créées après

octobre 2018) et les contraintes. Par exemple, `\dS+ sample` renvoie les propriétés d'objet. L'ajout de `S+` donne lieu à l'inclusion de colonnes supplémentaires dans les enregistrements renvoyés.

```
Table "public.sample"
 Column |            Type             |   Collation    | Nullable | Default Value |
 Encoding  | DistKey | SortKey
--------+-----------------------------+----------------+----------+---------------
+-----------+---------+---------
 col1   | smallint                    |                | NO       |               |
 none      | t       | 1
 col2   | character(100)              | case_sensitive | YES      |               |
 none      | f       | 2
 col3   | character varying(100)      | case_sensitive | YES      |               |
 text32k   | f       | 3
 col4   | timestamp without time zone |                | YES      |               |
 runlength | f       | 0
 col5   | super                       |                | YES      |               |
 zstd      | f       | 0
 col6   | bigint                      |                | YES      |               |
 az64      | f       | 0

Diststyle: KEY
Backup: YES
Created: 2021-07-20 19:47:27.997045
Unique Constraints:
    "sample_pkey" PRIMARY KEY (col1)
    "sample_col2_key" UNIQUE (col2)
Foreign-key constraints:
    "sample_col2_fkey" FOREIGN KEY (col2) REFERENCES lineitem(l_orderkey)
```

Le style de distribution, ou Diststyle, de la table peut être KEY, AUTO, EVEN ou ALL.

Backup (Sauvegarde) indique si la table est sauvegardée lors de la prise d'un instantané. Les valeurs valides sont `YES` ou `NO`.

Created (Créé) est l'horodatage de la date de création de la table. La date de création n'est pas disponible pour les tables Amazon Redshift créées avant novembre 2018. Les tables créées avant cette date s'affichent n/a (Non disponible).

Unique Constraints (Contraintes uniques) répertorie les contraintes uniques et les contraintes de clé principale sur la table.

Foreign-key constraints répertorie les contraintes de clé étrangère sur le tableau.

\dC[+] [PATTERN]

Répertorie les distributions. Inclut le type de source, le type de cible et indique si la distribution est implicite.

Les données suivantes présentent un sous-ensemble de résultats provenant de `\dC+`.

```
List of casts
         source type         |         target type         |      function       |
 implicit?   | description
-----------------------------+-----------------------------+---------------------
+---------------+-------------
 "char"                      | character                   | bpchar              | in
 assignment |
 "char"                      | character varying           | text                | in
 assignment |
 "char"                      | integer                     | int4                | no
          |
 "char"                      | text                        | text                | yes
          |
 "path"                      | point                       | point               | no
          |
 "path"                      | polygon                     | polygon             | in
 assignment |
 abstime                     | date                        | date                | in
 assignment |
 abstime                     | integer                     | (binary coercible)  | no
          |
 abstime                     | time without time zone      | time                | in
 assignment |
 abstime                     | timestamp with time zone    | timestamptz         | yes
          |
 abstime                     | timestamp without time zone | timestamp           | yes
          |
 bigint                      | bit                         | bit                 | no
          |
 bigint                      | boolean                     | bool                | yes
          |
 bigint                      | character                   | bpchar              | in
 assignment |
 bigint                      | character varying           | text                | in
 assignment |
```

```
bigint                      | double precision          | float8             | yes
        |
bigint                      | integer                   | int4               | in
assignment |
bigint                      | numeric                   | numeric            | yes
        |
bigint                      | oid                       | oid                | yes
        |
bigint                      | real                      | float4             | yes
        |
bigint                      | regclass                  | oid                | yes
        |
bigint                      | regoper                   | oid                | yes
        |
bigint                      | regoperator               | oid                | yes
        |
bigint                      | regproc                   | oid                | yes
        |
bigint                      | regprocedure              | oid                | yes
        |
bigint                      | regtype                   | oid                | yes
        |
bigint                      | smallint                  | int2               | in
assignment |
bigint                      | super                     | int8_partiql       | in
assignment |
```

\dd[S] [PATTERN]

Affiche les descriptions d’objets non affichées ailleurs.

\de

Répertorie les tables externes. Cela inclut les tables du AWS Glue Data Catalog Hive Metastore et les tables fédérées d'Amazon MySQL RDS/Aurora , Amazon PostgreSQL RDS/Aurora et Amazon Redshift.

\de NAME

Décrit une table externe.

L'exemple suivant montre une table AWS Glue externe.

```
# \de spectrum.lineitem
                          Glue External table "spectrum.lineitem"
     Column      | External Type | Redshift Type | Position | Partition Key | Nullable
-----------------+---------------+---------------+----------+---------------+----------
 l_orderkey      | bigint        | bigint        | 1        | 0             |
 l_partkey       | bigint        | bigint        | 2        | 0             |
 l_suppkey       | int           | int           | 3        | 0             |
 l_linenumber    | int           | int           | 4        | 0             |
 l_quantity      | decimal(12,2) | decimal(12,2) | 5        | 0             |
 l_extendedprice | decimal(12,2) | decimal(12,2) | 6        | 0             |
 l_discount      | decimal(12,2) | decimal(12,2) | 7        | 0             |
 l_tax           | decimal(12,2) | decimal(12,2) | 8        | 0             |
 l_returnflag    | char(1)       | char(1)       | 9        | 0             |
 l_linestatus    | char(1)       | char(1)       | 10       | 0             |
 l_shipdate      | date          | date          | 11       | 0             |
 l_commitdate    | date          | date          | 12       | 0             |
 l_receiptdate   | date          | date          | 13       | 0             |
 l_shipinstruct  | char(25)      | char(25)      | 14       | 0             |
 l_shipmode      | char(10)      | char(10)      | 15       | 0             |
 l_comment       | varchar(44)   | varchar(44)   | 16       | 0             |

Location: s3://redshiftbucket/kfhose2019/12/31
Input_format: org.apache.hadoop.mapred.TextInputFormat
Output_format: org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat
Serialization_lib: org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe
Serde_parameters: {"field.delim":"|","serialization.format":"|"}
Parameters:
 {"EXTERNAL":"TRUE","numRows":"178196721475","transient_lastDdlTime":"1577771873"}
```

Une table Hive Metastore.

```
# \de emr.lineitem
                    Hive Metastore External Table "emr.lineitem"
     Column      | External Type | Redshift Type | Position | Partition Key | Nullable
-----------------+---------------+---------------+----------+---------------+----------
 l_orderkey      | bigint        | bigint        | 1        | 0             |
 l_partkey       | bigint        | bigint        | 2        | 0             |
 l_suppkey       | int           | int           | 3        | 0             |
 l_linenumber    | int           | int           | 4        | 0             |
 l_quantity      | decimal(12,2) | decimal(12,2) | 5        | 0             |
 l_extendedprice | decimal(12,2) | decimal(12,2) | 6        | 0             |
 l_discount      | decimal(12,2) | decimal(12,2) | 7        | 0             |
```

```
 l_tax           | decimal(12,2) | decimal(12,2) | 8        | 0            |
 l_returnflag    | char(1)       | char(1)       | 9        | 0            |
 l_linestatus    | char(1)       | char(1)       | 10       | 0            |
 l_commitdate    | date          | date          | 11       | 0            |
 l_receiptdate   | date          | date          | 12       | 0            |
 l_shipinstruct  | char(25)      | char(25)      | 13       | 0            |
 l_shipmode      | char(10)      | char(10)      | 14       | 0            |
 l_comment       | varchar(44)   | varchar(44)   | 15       | 0            |
 l_shipdate      | date          | date          | 16       | 1            |

Location: s3://redshiftbucket/cetas
Input_format: org.apache.hadoop.hive.ql.io.parquet.MapredParquetInputFormat
Output_format: org.apache.hadoop.hive.ql.io.parquet.MapredParquetOutputFormat
Serialization_lib: org.apache.hadoop.hive.ql.io.parquet.serde.ParquetHiveSerDe
Serde_parameters: {"serialization.format":"1"}
Parameters: {"EXTERNAL":"TRUE", "numRows":"4307207",
 "transient_lastDdlTime":"1626990007"}
```

Table externe PostgreSQL.

```
# \de pgrsql.alltypes
                              Postgres Federated Table "pgrsql.alltypes"
 Column |        External Type        |        Redshift Type        | Position |
 Partition Key | Nullable
--------+-----------------------------+-----------------------------+----------
+---------------+----------
 col1   | bigint                      | bigint                      | 1        | 0
        |
 col2   | bigint                      | bigint                      | 2        | 0
        |
 col5   | boolean                     | boolean                     | 3        | 0
        |
 col6   | box                         | varchar(65535)              | 4        | 0
        |
 col7   | bytea                       | varchar(65535)              | 5        | 0
        |
 col8   | character(10)               | character(10)               | 6        | 0
        |
 col9   | character varying(10)       | character varying(10)       | 7        | 0
        |
 col10  | cidr                        | varchar(65535)              | 8        | 0
        |
```

```
col11  | circle                   | varchar(65535)           | 9        | 0
       |
col12  | date                     | date                     | 10       | 0
       |
col13  | double precision         | double precision         | 11       | 0
       |
col14  | inet                     | varchar(65535)           | 12       | 0
       |
col15  | integer                  | integer                  | 13       | 0
       |
col16  | interval                 | varchar(65535)           | 14       | 0
       |
col17  | json                     | varchar(65535)           | 15       | 0
       |
col18  | jsonb                    | varchar(65535)           | 16       | 0
       |
col19  | line                     | varchar(65535)           | 17       | 0
       |
col20  | lseg                     | varchar(65535)           | 18       | 0
       |
col21  | macaddr                  | varchar(65535)           | 19       | 0
       |
col22  | macaddr8                 | varchar(65535)           | 20       | 0
       |
col23  | money                    | varchar(65535)           | 21       | 0
       |
col24  | numeric                  | numeric(38,20)           | 22       | 0
       |
col25  | path                     | varchar(65535)           | 23       | 0
       |
col26  | pg_lsn                   | varchar(65535)           | 24       | 0
       |
col28  | point                    | varchar(65535)           | 25       | 0
       |
col29  | polygon                  | varchar(65535)           | 26       | 0
       |
col30  | real                     | real                     | 27       | 0
       |
col31  | smallint                 | smallint                 | 28       | 0
       |
col32  | smallint                 | smallint                 | 29       | 0
       |
col33  | integer                  | integer                  | 30       | 0
       |
```

```
 col34  | text                        | varchar(65535)              | 31       | 0
        |
 col35  | time without time zone      | varchar(65535)              | 32       | 0
        |
 col36  | time with time zone         | varchar(65535)              | 33       | 0
        |
 col37  | timestamp without time zone | timestamp without time zone | 34       | 0
        |
 col38  | timestamp with time zone    | timestamp with time zone    | 35       | 0
        |
 col39  | tsquery                     | varchar(65535)              | 36       | 0
        |
 col40  | tsvector                    | varchar(65535)              | 37       | 0
        |
 col41  | txid_snapshot               | varchar(65535)              | 38       | 0
        |
 col42  | uuid                        | varchar(65535)              | 39       | 0
        |
 col43  | xml                         | varchar(65535)              | 40       | 0
        |
```

\df[anptw][S+] [PATTERN]

Répertorie les fonctions de différents types. La commande `\df`, par exemple, renvoie une liste de fonctions. Les résultats incluent des propriétés telles que le nom, le type de données renvoyé, les privilèges d'accès et les métadonnées supplémentaires. Les types de fonctions peuvent inclure des déclencheurs, des procédures stockées, des fonctions de fenêtrage et d'autres types. Lorsque vous ajoutez `S+` à la commande, par exemple `\dfantS+`, des colonnes de métadonnées supplémentaires sont incluses, telles que `owner`, `security` et `access privileges`.

\dL[S+] [PATTERN]

Répertorie les données sur les langages procéduraux associés à la base de données. Les informations incluent le nom, tel que plpgsql, et des métadonnées supplémentaires, qui indiquent s'il est approuvé, les privilèges d'accès et la description. L'exemple d'appel est, par exemple, `\dLS+`, qui répertorie les langues et leurs propriétés. Lorsque vous ajoutez `S+` à la commande, des colonnes de métadonnées supplémentaires sont incluses, telles que `call handler` et `access privileges`.

Exemple de résultats :

```
List of languages
```

```
   name    | trusted | internal language |      call handler       |
      validator                         | access privileges |          description

-----------+---------+------------------+-------------------------
+-----------------------------------------------------------+-------------------
+--------------------------------
 c         | f       | t                | -                       |
 fmgr_c_validator(oid)                                       |                 |
 Dynamically-loaded C functions
 exfunc    | f       | f                | exfunc_call_handler()   | -
                                        | rdsdb=U/rdsdb     |
 internal  | f       | t                | -                       |
 fmgr_internal_validator(oid)                                |                 |
 Built-in functions
 mlfunc    | f       | f                | mlfunc_call_handler()   | -
                                        | rdsdb=U/rdsdb     |
 plpgsql   | t       | f                | plpgsql_call_handler()  |
 plpgsql_validator(oid)                                      |                 |
 plpythonu | f       | f                | plpython_call_handler() |
 plpython_compiler(cstring,cstring,cstring,cstring,cstring) | rdsdb=U/rdsdb     |
 sql       | t       | t                | -                       |
 fmgr_sql_validator(oid)                                     | =U/rdsdb          | SQL-
language functions
```

\dm[S+] [PATTERN]

Répertorie les vues matérialisées. Par exemple, `\dmS+` répertorie les vues matérialisées et leurs propriétés. Lorsque vous ajoutez S+ à la commande, des colonnes de métadonnées supplémentaires sont incluses.

\dn[S+] [PATTERN]

Répertorie les schémas. Lorsque vous ajoutez S+ à la commande, par exemple `\dnS+`, des colonnes de métadonnées supplémentaires sont incluses, telles que `description` et `access privileges`.

\dp [PATTERN]

Répertorie les privilèges d'accès aux tables, aux vues et aux séquences.

\dt[S+] [PATTERN]

Répertorie les tables. Lorsque vous ajoutez `S+` à la commande, par exemple `\dtS+`, des colonnes de métadonnées supplémentaires sont incluses, telles que `description` dans ce cas.

\du

Répertorie les utilisateurs pour la base de données. Inclut leur nom et leurs rôles, tels que super-utilisateur, ainsi que leurs attributs.

\dv[S+] [PATTERN]

Répertorie les vues. Inclut le schéma, le type et les données de propriétaire. Lorsque vous ajoutez `S+` à la commande, par exemple `\dvS+`, des colonnes de métadonnées supplémentaires sont incluses.

\H

Active la sortie HTML. Cela est utile pour renvoyer rapidement des résultats formatés. Par exemple, `select * from sales; \H` renvoie les résultats de la table des ventes, au format HTML. Pour revenir aux résultats tabulaires, utilisez `\q` ou silencieux.

\i

Exécute des commandes à partir d'un fichier. Par exemple, supposons que vous avez rsql_steps.sql dans votre répertoire de travail, les commandes suivantes exécutent les commandes dans le fichier :`\i rsql_steps.sql`.

\l[+] [PATTERN]

Répertorie les bases de données. Inclut le propriétaire, l'encodage et des informations supplémentaires.

\q

La commande de fermeture, ou `\q`, déconnecte les séances de base de données et ferme RSQL.

\sv[+] VIEWNAME

Affiche la définition d'une vue.

\timing

Affiche le délai d'exécution, pour une requête, par exemple.

\z [PATTERN]

Le même résultat que \dp.

\?

Affiche les informations d'aide. Le paramètre facultatif indique l'élément à expliquer.

\EXIT

Déconnecte toutes les séances de base de données et ferme Amazon Redshift RSQL. En outre, vous pouvez spécifier un code de sortie facultatif. Par exemple, `\EXIT 15` va fermer le terminal RSQL Amazon Redshift et renvoyer le code de sortie 15.

L'exemple suivant montre le résultat d'une connexion et la fermeture de RSQL.

```
% rsql -D testuser
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.34.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=# \exit 15

% echo $?
15
```

\EXPORT

Spécifie le nom d'un fichier d'exportation utilisé par RSQL pour stocker les informations de base de données renvoyées par une instruction SQL SELECT ultérieure.

export_01.sql

```
\export report file='E:\\accounts.out'
\rset rformat off
\rset width 1500
\rset heading "General Title"
\rset titledashes on
```

```
select * from td_dwh.accounts;
\export reset
```

Sortie de console

```
Rformat is off.
Target width is 1500.
Heading is set to: General Title
Titledashes is on.
(exported 40 rows)
```

\LOGON

Se connecte à une base de données. Vous pouvez spécifier des paramètres de connexion à l'aide de la syntaxe positionnelle ou d'une chaîne de connexion.

La syntaxe de commande est la suivante : `\logon {[DBNAME|- USERNAME|- HOST|- PORT|- [PASSWORD]] | conninfo}`

Le `DBNAME` est le nom de base de données à laquelle se connecter. Le `USERNAME` est le nom d'utilisateur utilisé pour se connecter. L'`HOST` par défaut est `localhost`. L'`PORT` par défaut est `5439`.

Lorsqu'un nom d'hôte est spécifié dans une commande `\LOGON`, il devient le nom d'hôte par défaut pour d'autres commandes `\LOGON`. Pour modifier le nom d'hôte par défaut, spécifiez un nouveau `HOST` dans une autre commande `\LOGON`.

L'exemple de résultat de la commande `\LOGON` pour `user1` suit.

```
(testcluster) user1@redshiftdb=# \logon dev
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
You are now connected to database "dev" as user "user1".
(testcluster) user1@dev=#
```

Exemple de résultat pour user2.

```
(testcluster) user1@dev=# \logon dev user2 testcluster2.example.com
```

```
Password for user user2:
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
You are now connected to database "dev" as user "user2" on host
 "testcluster2.example.com" at port "5439".
(testcluster2) user2@dev=#
```

\REMARK

Une extension de la commande \echo. \REMARK imprime la chaîne spécifiée dans le flux de sortie. \REMARK étend \echoen ajoutant la possibilité de répartir le résultat sur des lignes distinctes.

L'exemple suivant montre le résultat de la commande.

```
(testcluster) user1@dev=# \remark 'hello//world'
hello
world
```

\RSET

La commande \rset définit les paramètres de commande et les variables. \rset dispose à la fois d'un mode interactif et d'un mode de traitement par lots. Elle ne prend pas en charge les options en tant qu'options bash, comme -x, ou des arguments, par exemple --<arg>.

Elle définit des variables, telles que les suivantes :

- ERRORLEVEL
- HEADING et RTITLE
- RFORMAT
- MAXERROR
- TITLEDASHES
- WIDTH

L'exemple suivant spécifie un en-tête.

```
\rset heading "Winter Sales Report"
```

Pour obtenir plus d'exemples d'utilisation `\rset`, vous pouvez en trouver plusieurs dans les rubriques Variables Amazon Redshift RSQL.

\RUN

Exécute le script Amazon Redshift RSQL contenu dans le fichier spécifié. `\RUN` étend la commande `\i` en ajoutant une option permettant d'ignorer les lignes d'en-tête dans un fichier.

Si le nom du fichier contient une virgule, un point-virgule ou un espace, placez-le entre guillemets simples. De plus, si le texte suit le nom du fichier, placez-le entre guillemets. Sous UNIX, les noms de fichier sont sensibles à la casse. Sous Windows, les noms de fichiers ne sont pas sensibles à la casse.

L'exemple suivant montre le résultat de la commande.

```
(testcluster) user1@dev=# \! cat test.sql
select count(*) as lineitem_cnt from lineitem;
select count(*) as customer_cnt from customer;
select count(*) as orders_cnt from orders;



(testcluster) user1@dev=# \run file=test.sql
 lineitem_cnt
--------------
      4307207
(1 row)

 customer_cnt
--------------
     37796166
(1 row)

 orders_cnt
------------
          0
(1 row)


(testcluster) user1@dev=# \run file=test.sql skip=2
2 records skipped in RUN file.
 orders_cnt
------------
```

```
          0
(1 row)
```

\OS

Un alias pour la commande `\!`. `\OS` exécute la commande du système d'exploitation transmise en tant que paramètre. Le contrôle revient à Amazon Redshift RSQL une fois la commande exécutée. Par exemple, vous pouvez exécuter la commande suivante pour imprimer la date et l'heure du système actuel et revenir au terminal RSQL : `\os date`.

```
(testcluster) user1@dev=# \os date
Tue Sep 7 20:47:54 UTC 2021
```

\GOTO

Une nouvelle commande pour Amazon Redshift RSQL. `\GOTO` ignore toutes les commandes intervenantes et reprend le traitement à l'`\LABEL` spécifiée. L'`\LABEL` doit être une référence future. Vous ne pouvez pas accéder à une`\LABEL` qui précède le `\GOTO` d'un point de vue lexical.

Voici un exemple de résultat.

```
(testcluster) user1@dev=# \! cat test.sql
select count(*) as cnt from lineitem \gset
select :cnt as cnt;
\if :cnt > 100
    \goto LABELB
\endif

\label LABELA
\remark 'this is label LABELA'
\label LABELB
\remark 'this is label LABELB'


(testcluster) user1@dev=# \i test.sql
   cnt
---------
 4307207
(1 row)

\label LABELA ignored
\label LABELB processed
```

```
this is label LABELB
```

\LABEL

Une nouvelle commande pour Amazon Redshift RSQL. `\LABEL` établit un point d'entrée pour exécuter le programme, en tant que cible pour une commande `\GOTO`.

L'exemple suivant montre un exemple de résultat de la commande.

```
(testcluster) user1@dev=# \! cat test.sql
select count(*) from lineitem limit 5;
\goto LABELB
\remark "this step was skipped by goto label";
\label LABELA
\remark 'this is label LABELA'
\label LABELB
\remark 'this is label LABELB'



(testcluster) user1@dev=# \i testgoto.sql
  count
 4307193
(1 row)

\label LABELA ignored
\label LABELB processed
this is label LABELB
```

\IF (\ELSEIF, \ELSE, \ENDIF)

Les commandes `\IF`et associées exécutent conditionnellement des parties du script d'entrée. Une extension de la commande PSQL `\if` (`\elif`, `\else`, `\endif`). `\IF` et `\ELSEIF` prennent en charge les expressions booléennes, dont les conditions `AND`, `OR` et `NOT`.

L'exemple suivant montre un exemple de résultat des commandes.

```
(testcluster) user1@dev=# \! cat test.sql
SELECT query FROM stv_inflight LIMIT 1 \gset
select :query as query;
\if :query > 1000000
    \remark 'Query id is greater than 1000000'
```

```
\elseif :query = 1000000
    \remark 'Query id is equal than 1000000'
\else
    \remark 'Query id is less than 1000000'
\endif


(testcluster) user1@dev=# \i test.sql
 query
--------
 994803
(1 row)

Query id is less than 1000000
```

Utilisez ERRORCODE dans votre logique de branchement.

```
\if :'ERRORCODE' = '00000'
    \remark 'The statement was executed without error'
\else
    \remark :LAST_ERROR_MESSAGE
\endif
```

Utilisez\GOTO dans un bloc \IF pour contrôler la façon dont le code est exécuté.

Variables Amazon Redshift RSQL

Certains mots-clés agissent comme des variables dans RSQL. Vous pouvez définir chacun une valeur spécifique ou réinitialiser la valeur. La plupart sont réglées avec \rset, qui dispose d'un mode interactif et d'un mode de traitement par lots. Les commandes peuvent être définies en minuscules ou en majuscules.

ACTIVITYCOUNT

Indique le nombre de lignes affectées par la dernière demande envoyée. Pour une demande renvoyant des données, il s'agit du nombre de lignes renvoyées vers RSQL à partir de la base de données. La valeur est 0 ou un nombre entier positif. La valeur maximale est 18 446 744 073 709 551 615.

La variable spécialement traitée ACTIVITYCOUNT est semblable à la variable ROW_COUNT. Toutefois, ROW_COUNT ne signale pas le nombre de lignes affectées à l'application cliente à la fin de la commande pour SELECT, COPY ou UNLOAD. Mais ACTIVITYCOUNT le fait.

activitycount_01.sql :

```
select viewname, schemaname
from pg_views
where schemaname = 'not_existing_schema';
\if :ACTIVITYCOUNT = 0
\remark 'views do not exist'
\endif
```

Sortie de la console :

```
viewname | schemaname
----------+------------
(0 rows)

views do not exist
```

ERRORLEVEL

Attribue des niveaux de sévérité aux erreurs. Utilisez les niveaux de sévérité pour déterminer un plan d'action. Si la commande ERRORLEVEL n'a pas été utilisée, sa valeur par défaut est ON.

errorlevel_01.sql :

```
\rset errorlevel 42P01 severity 0

select * from tbl;

select 1 as col;

\echo exit
\quit
```

Sortie de la console :

```
Errorlevel is on.
rsql: ERROR: relation "tbl" does not exist
(1 row)

col
1
```

```
exit
```

HEADING et RTITLE

Permet aux utilisateurs de spécifier un en-tête qui s'affiche dans la partie supérieure d'un rapport. L'en-tête spécifiée par la commande `RSET RTITLE` inclut automatiquement la date système actuelle de l'ordinateur client.

Contenu rset_heading_rtitle_02.rsql :

```
\remark Starting...
\rset rtitle "Marketing Department||Confidential//Third Quarter//Chicago"
\rset width 70
\rset rformat on
select * from rsql_test.tbl_currency order by id limit 2;
\exit
\remark Finishing...
```

Sortie de la console :

```
Starting...
Rtitle is set to: &DATE||Marketing Department||Confidential//Third Quarter//Chicago
 (Changes will take effect after RFORMAT is
switched ON)
Target width is 70.
Rformat is on.
09/11/20       Marketing       Department Confidential
                  Third Quarter
                     Chicago
id  | bankid  | name |      start_date
100 |       1 | USD | 2020-09-11 10:51:39.106905
110 |       1 | EUR | 2020-09-11 10:51:39.106905
(2 rows)

Press any key to continue . . .
```

MAXERROR

Désigne un niveau de sévérité d'erreur maximal au-delà duquel RSQL met fin au traitement des tâches. Les codes de retour sont des valeurs entières que RSQL renvoie au système d'exploitation

client après avoir terminé chaque tâche. La valeur du code de retour indique l'état d'achèvement de la tâche. Si un script contient une instruction qui produit un niveau de sévérité d'erreur supérieur à la valeur `maxerror` désignée, RSQL s'interrompt immédiatement. Par conséquent, pour que RSQL s'interrompt à un niveau de sévérité d'erreur de 8, utilisez `RSET MAXERROR 7`.

Contenu maxerror_01.sql :

```
\rset maxerror 0

select 1 as col;

\quit
```

Sortie de la console :

```
Maxerror is default.
(1 row)

col
1
```

RFORMAT

Permet aux utilisateurs de spécifier s'il faut appliquer des paramètres aux commandes de formatage.

Contenu rset_rformat.rsql :

```
\remark Starting...
\pset border 2
\pset format wrapped
\pset expanded on
\pset title 'Great Title'
select * from rsql_test.tbl_long where id = 500;
\rset rformat
select * from rsql_test.tbl_long where id = 500;
\rset rformat off
select * from rsql_test.tbl_long where id = 500;
\rset rformat on
select * from rsql_test.tbl_long where id = 500;
\exit
\remark Finishing...
```

Sortie de la console :

```
Starting...
Border style is 2. (Changes will take effect after RFORMAT is switched ON)
Output format is wrapped. (Changes will take effect after RFORMAT is switched ON)
Expanded display is on. (Changes will take effect after RFORMAT is switched ON)
Title is "Great Title". (Changes will take effect after RFORMAT is switched ON)
id  |                                                                  long_string
500 | In general, the higher the number the more borders and lines the tables will
 have, but details depend on the particular
format.
(1 row)

Rformat is on.
Great Title
+-[ RECORD
 1 ]+-------------------------------------------------------------------------------------------------
-----------+
| id          | 500
|
| long_string | In general, the higher the number the more borders and lines the tables
 will have, but details depend on the
particular format. |
+-------------
+-------------------------------------------------------------------------------------------------
-----------+

Rformat is off.
id  |                                                                  long_string
500 | In general, the higher the number the more borders and lines the tables will
 have, but details depend on the particular format.
(1 row)

Rformat is on.
Great Title
+-[ RECORD
 1 ]+-------------------------------------------------------------------------------------------------
-----------+
| id          | 500
|
| long_string | In general, the higher the number the more borders and lines the tables
 will have, but details depend on the
particular format. |
```

```
+-------------
+-----------------------------------------------------------------------------------------------------
-----------+
Press any key to continue . . .
```

ROW_COUNT

Obtient le nombre d'enregistrements affectés par la requête précédente. Il est généralement utilisé pour vérifier un résultat, comme dans le fragment de code suivant :

```
SET result = ROW_COUNT;

IF result = 0
...
```

TITLEDASHES

Ce contrôle permet aux utilisateurs de spécifier si une ligne de caractères de tiret doit être imprimée au-dessus des données de colonne renvoyées pour les instructions SQL.

Exemple :

```
\rset titledashes on
select dept_no, emp_no, salary from rsql_test.EMPLOYEE
where dept_no = 100;
\rset titledashes off
select dept_no, emp_no, salary from rsql_test.EMPLOYEE
where dept_no = 100;
```

Sortie de la console :

```
dept_no      emp_no          salary
----------- ----------- --------------------
100         1000346        1300.00
100         1000245        5000.00
100         1000262        2450.00

dept_no     emp_no         salary
100         1000346        1300.00
100         1000245        5000.00
100         1000262        2450.00
```

WIDTH

Définit le format de sortie sur encapsulé et spécifie la largeur cible de chaque ligne d'un rapport. Sans paramètre, il renvoie les paramètres actuels pour le format et la largeur cible.

Contenu rset_width_01.rsql :

```
\echo Starting...
\rset width
\rset width 50
\rset width
\quit
\echo Finishing...
```

Sortie de la console :

```
Starting...
Target width is 75.
Target width is 50.
Target width is 50.
Press any key to continue . . .
```

Exemple avec paramètre :

```
\echo Starting...
\rset rformat on
\pset format wrapped
select * from rsql_test.tbl_long where id = 500;
\rset width 50
select * from rsql_test.tbl_long where id = 500;
\quit
\echo Finishing...
```

Sortie de la console :

```
Starting...
Rformat is on.
Output format is wrapped.
id  |                                          long_string
500 | In general, the higher the number the more borders and lines the ta.
    |.bles will have, but details depend on the particular format.
```

```
(1 row)

Target width is 50.
id  |                                            long_string
500 | In general, the higher the number the more.
    |. borders and lines the tables will have, b.
    |.ut details depend on the particular format.
    |..
(1 row)
Press any key to continue . . .
```

Codes d’erreur Amazon Redshift RSQL

Messages de réussite, avertissements et exceptions :

Code d’erreur	Classe d’erreur	Nom de la condition
00000	Classe 00 – Terminé	successful_completion
01000	Classe 01 – Avertissement	warning
0100C	Classe 01 – Avertissement	dynamic_result_sets_returned
01008	Classe 01 – Avertissement	implicit_zero_bit_padding
01003	Classe 01 – Avertissement	null_value_eliminated_in_set_function
01007	Classe 01 – Avertissement	privilege_not_granted
01006	Classe 01 – Avertissement	privilege_not_revoked
01004	Classe 01 – Avertissement	string_data_right_truncation
01P01	Classe 01 – Avertissement	deprecated_feature
02000	Classe 02 – Aucune donnée	no_data
02001	Classe 02 – Aucune donnée	no_additional_dynamic_result_sets_returned
03000	Classe 03 – Instruction SQL pas encore terminée	sql_statement_pas_yet_complete

Code d’erreur	Classe d’erreur	Nom de la condition
08000	Classe 08 – Exception de connexion	connection_exception
08003	Classe 08 – Exception de connexion	connection_does_not_exist
08006	Classe 08 – Exception de connexion	connection_failure
08001	Classe 08 – Exception de connexion	sqlclient_unable_to_establish_sqlconnection
08004	Classe 08 – Exception de connexion	sqlserver_rejected_establishment_of_sqlconnection
08007	Classe 08 – Exception de connexion	transaction_resolution_unknown
08P01	Classe 08 – Exception de connexion	protocol_violation
09000	Classe 09 – Exception d’action déclenchée	triggered_action_exception
0A000	Classe 0A – Fonctionnalité non prise en charge	feature_not_supported
0A000	Classe 0A – Fonctionnalité non prise en charge	feature_not_supported
0B000	Classe 0B – Initiation de transaction non valide	invalid_transaction_initiation
0F000	Classe 0F – Exception de Locator	locator_exception
0F001	Classe 0F – Exception de Locator	invalid_locator_specification

Code d’erreur	Classe d’erreur	Nom de la condition
0L000	Classe 0L – Concédant non valide	invalid_grantor
0LP01	Classe 0L – Concédant non valide	invalid_grant_operation
0P000	Classe 0P – Spécification de rôle non valide	invalid_role_specification
0Z000	Classe 0Z – Exception de diagnostic	diagnostics_exception
0Z002	Classe 0Z – Exception de diagnostic	stacked_diagnostics_accessed_without_active_handler
20 000	Classe 20 – Cas non trouvable	case_not_found
21 000	Classe 21 – Violation de la cardinalité	cardinality_violation

Exceptions de données :

Code d’erreur	Classe d’erreur	Nom de la condition
22 000	Classe 22 – Exception de données	data_exception
2202E	Classe 22 – Exception de données	array_subscript_error
2021	Classe 22 – Exception de données	character_not_in_repertoire
2008	Classe 22 – Exception de données	datetime_field_overflow

Code d’erreur	Classe d’erreur	Nom de la condition
2012	Classe 22 – Exception de données	division_by_zero
2005	Classe 01 – Avertissement	error_in_assignment
2200B	Classe 01 – Avertissement	escape_character_conflict
2022	Classe 01 – Avertissement	indicator_overflow
2015	Classe 01 – Avertissement	interval_field_overflow
2201E	Classe 01 – Avertissement	invalid_argument_for_logarithm
2201F	Classe 01 – Avertissement	invalid_argument_for_power_function
2201G	Classe 01 – Avertissement	invalid_argument_for_width_bucket_function
2018	Classe 01 – Avertissement	invalid_character_value_for_cast
2007	Classe 01 – Avertissement	invalid_datetime_format
2019	Classe 01 – Avertissement	invalid_escape_character
2200D	Classe 01 – Avertissement	invalid_escape_octet
22025	Classe 01 – Avertissement	invalid_escape_sequence
22P06	Classe 01 – Avertissement	nonstandard_use_of_escape_character
2010	Classe 01 – Avertissement	invalid_indicator_parameter_value
22023	Classe 01 – Avertissement	invalid_parameter_value
2201B	Classe 01 – Avertissement	invalid_regular_expression
2009	Classe 01 – Avertissement	invalid_time_zone_displacement_value
2200C	Classe 01 – Avertissement	invalid_use_of_escape_character
2200G	Classe 01 – Avertissement	most_specific_type_mismatch

Code d’erreur	Classe d’erreur	Nom de la condition
2004	Classe 01 – Avertissement	null_value_not_allowed
22002	Classe 01 – Avertissement	null_value_no_indicator_parameter
22003	Classe 01 – Avertissement	numeric_value_out_of_range
22026	Classe 01 – Avertissement	string_data_length_mismatch
22001	Classe 01 – Avertissement	string_data_right_truncation
22011	Classe 01 – Avertissement	substring_error
22027	Classe 01 – Avertissement	trim_error
22024	Classe 01 – Avertissement	unterminated_c_string
2200F	Classe 01 – Avertissement	zero_length_character_string
22P01	Classe 01 – Avertissement	floating_point_exception
22P02	Classe 01 – Avertissement	invalid_text_representation
22P03	Classe 01 – Avertissement	invalid_binary_representation
22P04	Classe 01 – Avertissement	bad_copy_file_format
22P05	Classe 01 – Avertissement	untranslatable_character

Violations des contraintes d’intégrité :

Code d’erreur	Classe d’erreur	Nom de la condition
23000	Classe 23 – Violation des contraintes d’intégrité	integrity_constraint_violation
23001	Classe 23 – Violation des contraintes d’intégrité	restrict_violation

Code d’erreur	Classe d’erreur	Nom de la condition
23502	Classe 23 – Violation des contraintes d’intégrité	not_null_violation
23503	Classe 23 – Violation des contraintes d’intégrité	foreign_key_violation
23505	Classe 23 – Violation des contraintes d’intégrité	unique_violation
23514	Classe 23 – Violation des contraintes d’intégrité	check_violation
24000	Classe 24 – État du curseur non valide	invalid_cursor_state
01004	Classe 01 – Avertissement	string_data_right_truncation
25000	Classe 25 – État de transacti on non valide	invalid_transaction_state
25001	Classe 25 – État de transacti on non valide	active_sql_transaction
25002	Classe 25 – État de transacti on non valide	invalid_transaction_state
25008	Classe 25 – État de transacti on non valide	held_cursor_requires_same_isolation_level
25003	Classe 25 – État de transacti on non valide	inappropriate_access_mode_for_branch _transaction
25004	Classe 25 – État de transacti on non valide	inappropriate_isolation_level_for_branch_tran saction
25005	Classe 25 – État de transacti on non valide	no_active_sql_transaction_for_branch_transact ion

Code d’erreur	Classe d’erreur	Nom de la condition
25006	Classe 25 – État de transacti on non valide	read_only_sql_transaction
25007	Classe 25 – État de transacti on non valide	no_active_sql_transaction_for_branch_transact ion
25P01	Classe 25 – État de transacti on non valide	no_active_sql_transaction
25P02	Classe 25 – État de transacti on non valide	in_failed_sql_transaction
26000	Classe 26 – Nom d’instruction SQL non valide	invalid_sql_statement_name
28000	Classe 28 – Spécification d’autorisation non valide	invalid_authorization_specification
2B000	Classe 2B – Descripteurs de privilèges dépendants toujours existants	dependent_privilege_descriptors_still_exist
2BP01	Classe 2B – Descripteurs de privilèges dépendants toujours existants	dependent_objects_still_exist
2D000	Classe 2D – Résiliation de transaction non valide	invalid_transaction_termination
2F000	Classe 2F – Exception de routine SQL	sql_routine_exception
2F005	Classe 2F – Exception de routine SQL	function_executed_no_return_statement
2F002	Classe 2F – Exception de routine SQL	modifying_sql_data_not_permitted

Code d’erreur	Classe d’erreur	Nom de la condition
2F003	Classe 2F – Exception de routine SQL	prohibited_sql_statement_attempted
2F004	Classe 2F – Exception de routine SQL	reading_sql_data_not_permitted
34000	Classe 34 – Nom de curseur non valide	invalid_cursor_name
38000	Classe 38 – Exception de routine externe	external_routine_exception
38001	Classe 38 – Exception de routine externe	containing_sql_not_permitted
38002	Classe 38 – Exception de routine externe	modifying_sql_data_not_permitted
38003	Classe 38 – Exception de routine externe	prohibited_sql_statement_attempted
38004	Classe 38 – Exception de routine externe	reading_sql_data_not_permitted
39000	Classe 39 – Exception d'appel de routine externe	external_routine_invocation_exception
39001	Classe 39 – Exception d'appel de routine externe	invalid_sqlstate_returned
39004	Classe 39 – Exception d'appel de routine externe	null_value_not_allowed
39P01	Classe 39 – Exception d'appel de routine externe	trigger_protocol_violated
39P02	Classe 39 – Exception d'appel de routine externe	srf_protocol_violated

Code d’erreur	Classe d’erreur	Nom de la condition
3D000	Classe 3D – Nom de catalogue non valide	invalid_catalog_name
3F000	Classe 3F – Nom de schéma non valide	invalid_schema_name
42000	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	syntax_error_or_access_rule_violation
42601	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	syntax_error
42501	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	insufficient_privilege
42846	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	cannot_coerce
42803	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	grouping_error
42830	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	invalid_foreign_key
42602	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	invalid_name
42622	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	name_too_long
42939	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	reserved_name
42804	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	datatype_mismatch
42P18	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	indeterminate_datatype

Code d’erreur	Classe d’erreur	Nom de la condition
42809	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	wrong_object_type
42703	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	undefined_column
42883	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	undefined_function
42P01	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	undefined_table
42P02	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	undefined_parameter
42704	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	undefined_object
42701	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	duplicate_column
42P03	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	duplicate_cursor
42P04	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	duplicate_database
42723	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	duplicate_function
42P05	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	duplicate_prepared_statement
42P06	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	duplicate_schema
42P07	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	duplicate_table

Code d’erreur	Classe d’erreur	Nom de la condition
42712	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	duplicate_alias
42710	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	duplicate_object
42702	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	ambiguous_column
42725	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	ambiguous_function
42P08	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	ambiguous_parameter
42P09	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	ambiguous_alias
42P10	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	invalid_column_reference
42611	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	invalid_column_definition
42P11	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	invalid_cursor_definition
42P12	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	invalid_database_definition
42P13	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	invalid_function_definition
42P14	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	invalid_prepared_statement_definition
42P15	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	invalid_schema_definition

Code d’erreur	Classe d’erreur	Nom de la condition
42P16	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	invalid_table_definition
42P17	Classe 42 – Erreur de syntaxe ou violation de règle d’accès	invalid_object_definition
44000	Classe 44 – Violation de l’option WITH CHECK OPTION	with_check_option_violation
53000	Classe 53 – Ressources insuffisantes	insufficient_resources
53100	Classe 53 – Ressources insuffisantes	disk_full
53200	Classe 53 – Ressources insuffisantes	out_of_memory
53300	Classe 53 – Ressources insuffisantes	too_many_connections
54000	Classe 54 – Limite du programme dépassée	program_limit_exceeded
54001	Classe 54 – Limite du programme dépassée	statement_too_complex
54011	Classe 54 – Limite du programme dépassée	too_many_columns
54023	Classe 54 – Limite du programme dépassée	too_many_arguments
55000	Classe 55 – Objet ne se trouvant pas dans l’état prérequis	object_not_in_prerequisite_state

Code d’erreur	Classe d’erreur	Nom de la condition
55006	Classe 55 – Objet ne se trouvant pas dans l’état prérequis	object_in_use
55P02	Classe 55 – Objet ne se trouvant pas dans l’état prérequis	cant_change_runtime_param
55P03	Classe 55 – Objet ne se trouvant pas dans l’état prérequis	lock_not_available
57000	Classe 57 – Intervention de l’opérateur	operator_intervention
57014	Classe 57 – Intervention de l’opérateur	query_canceled
57P01	Classe 57 – Intervention de l’opérateur	admin_shutdown
57P02	Classe 57 – Intervention de l’opérateur	crash_shutdown
57P03	Classe 57 – Intervention de l’opérateur	cannot_connect_now
58000	Classe 58 – Erreur système (erreurs externes à PostgreSQL)	system_error
58030	Classe 58 – Erreur système (erreurs externes à PostgreSQL)	io_error

Code d’erreur	Classe d’erreur	Nom de la condition
58P01	Classe 58 – Erreur système (erreurs externes à PostgreSQL)	undefined_file
58P02	Classe 58 – Erreur système (erreurs externes à PostgreSQL)	duplicate_file
F0000	Classe F0 – Erreur du fichier de configuration	duplicate_file
F0001	Classe F0 – Erreur du fichier de configuration	lock_file_exists
P0000	Classe P0 — Erreur PL/pgSQL	plpgsql_error
P0001	Classe P0 — Erreur PL/pgSQL	raise_exception
P0002	Classe P0 — Erreur PL/pgSQL	no_data_found
P0003	Classe P0 — Erreur PL/pgSQL	too_many_rows
XX000	Classe XX – Erreur interne	internal_error
XX001	Classe XX – Erreur interne	data_corrupted
XX002	Classe XX – Erreur interne	index_corrupted

Variables d’environnement Amazon Redshift RSQL

Amazon Redshift RSQL peut utiliser des variables d’environnement pour sélectionner des valeurs de paramètres par défaut.

RSPASSWORD

> **Important**
>
> Nous ne recommandons pas d'utiliser cette variable d'environnement pour des raisons de sécurité, car certains systèmes d'exploitation permettent aux utilisateurs non administratifs de visualiser les variables d'environnement des processus.

Définit le mot de passe pour Amazon Redshift RSQL à utiliser lors de la connexion à Amazon Redshift. Cette variable d'environnement nécessite Amazon Redshift RSQL 1.0.4 et version ultérieure.

RSQL donne la priorité à RSPASSWORD si celui-ci est défini. Si RSPASSWORD n'est pas défini et que vous vous connectez à l'aide d'un DSN, RSQL récupère le mot de passe dans les paramètres du fichier DSN. Enfin, si RSPASSWORD n'est pas défini et que vous n'utilisez pas de DSN, RSQL fournit une invite de mot de passe après une tentative de connexion.

Voici un exemple de définition d'un RSPASSWORD :

```
export RSPASSWORD=TestPassw0rd
```

Utilisation d'un profil d'authentification pour se connecter à Amazon Redshift

Si vous avez de nombreuses connexions à Amazon Redshift, il peut être difficile de gérer les paramètres de toutes ces connexions. Souvent, chaque connexion JDBC ou ODBC utilise des options de configuration spécifiques. En utilisant un profil d'authentification, vous pouvez stocker les options de connexion ensemble. De cette façon, vos utilisateurs peuvent choisir un profil pour se connecter et éviter de gérer les paramètres pour des options individuelles. Les profils peuvent s'appliquer à divers scénarios et types d'utilisateurs.

Une fois que vous avez créé un profil d'authentification, les utilisateurs peuvent ajouter le profil prêt à l'emploi à une chaîne de connexion. Ce faisant, ils peuvent se connecter à Amazon Redshift avec les paramètres appropriés pour chaque rôle et chaque cas d'utilisation.

Pour obtenir des informations sur l'API Amazon Redshift, consultez. CreateAuthenticationProfile

Création d'un profil d'authentification

À l'aide de AWS CLI, vous créez un profil d'authentification à l'aide de la `create-authentication-profile` commande. Cela suppose que vous disposez d'un cluster Amazon Redshift existant et d'une base de données existante. Vos informations d'identification doivent être autorisées à se connecter à la base de données Amazon Redshift et à récupérer le profil d'authentification. Vous fournissez les options de configuration sous forme de chaîne JSON ou référencez un fichier contenant votre chaîne JSON.

```
create-authentication-profile --authentication-profile-name<value: String> --
authentication-profile-content<value: String>
```

L'exemple suivant crée un profil appelé `ExampleProfileName`. Vous pouvez y ajouter des clés et des valeurs qui définissent le nom de votre cluster et d'autres paramètres d'options, sous forme de chaîne JSON.

```
create-authentication-profile --authentication-profile-name "ExampleProfileName"
 --authentication-profile-content "{\"AllowDBUserOverride\":\"1\",\"Client_ID
\":\"ExampleClientID\",\"App_ID\":\"ExampleAppID\",\"AutoCreate\":false,
\"enableFetchRingBuffer\":true,\"databaseMetadataCurrentDbOnly\":true}"
}
```

Cette commande crée le profil avec les paramètres JSON spécifiés. Ce qui suit est renvoyé, ce qui indique que le profil a été créé.

```
{"AuthenticationProfileName": "ExampleProfileName",
"AuthenticationProfileContent": "{\"AllowDBUserOverride\":\"1\",
\"Client_ID\":\"ExampleClientID\",\"App_ID\":\"ExampleAppID\",
\"AutoCreate\":false,\"enableFetchRingBuffer\":true,
\"databaseMetadataCurrentDbOnly\":true}" }
```

Limitations et quotas pour la création d'un profil d'authentification

Chaque client dispose d'un quota de dix (10) profils d'authentification.

Certaines erreurs peuvent survenir avec les profils d'authentification. Par exemple, vous créez un profil avec un nom existant ou si vous dépassez le quota de votre profil. Pour plus d'informations, consultez CreateAuthenticationProfile.

Vous ne pouvez pas stocker certaines clés d'option et valeurs pour les chaînes de connexion JDBC, ODBC et Python dans le magasin de profils d'authentification :

- `AccessKeyID`
- `access_key_id`
- `SecretAccessKey`
- `secret_access_key_id`
- `PWD`
- `Password`
- `password`

Vous ne pouvez pas stocker la clé ou la valeur `AuthProfile` dans le magasin de profils, pour les chaînes de connexion JDBC ou ODBC. Pour les connexions Python, vous ne pouvez pas stocker `auth_profile`.

Les profils d'authentification sont stockés dans Amazon DynamoDB et gérés par. AWS

Connexion à l'aide d'un profil d'authentification

Après avoir créé un profil d'authentification, vous pouvez inclure le nom du profil comme option de connexion pour JDBC version 2.x. `AuthProfile` L'utilisation de cette option de connexion permet d'extraire les paramètres stockés.

```
jdbc:redshift:iam://endpoint:port/database?AuthProfile=<Profile-
Name>&AccessKeyID=<Caller-Access-Key>&SecretAccessKey=<Caller-Secret-Key>
```

Voici un exemple de chaîne d'URL JDBC.

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?
AuthProfile="ExampleProfile"&AccessKeyID="AKIAIOSFODNN7EXAMPLE"&SecretAccessKey="wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY"
```

Spécifiez `AccessKeyID` et `SecretAccessKey` dans l'URL JDBC, ainsi que le nom du profil d'authentification.

Vous pouvez également séparer les options de configuration par des délimiteurs points-virgules, comme dans l'exemple suivant, qui contient des options de journalisation.

```
jdbc:redshift:iam://my_redshift_end_point:5439/dev?LogLevel=6;LogPath=/
tmp;AuthProfile=my_profile;AccessKeyID="AKIAIOSFODNN7EXAMPLE";SecretAccessKey="wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY"
```

> **Note**
>
> N'ajoutez pas d'informations confidentielles au profil d'authentification. Par exemple, ne stockez pas de valeur `AccessKeyID` ou `SecretAccessKey` dans un profil d'authentification. Le magasin de profils d'authentification comporte des règles interdisant le stockage de clés secrètes. Une erreur s'affiche si vous tentez de stocker une clé et une valeur associées à des informations sensibles.

Obtention de profils d'authentification

Pour répertorier les profils d'authentification existants, appelez la commande suivante.

```
describe-authentication-profiles --authentication-profile-name <value: String>
```

L'exemple suivant illustre deux profils récupérés. Tous les profils sont renvoyés si vous ne spécifiez pas de nom de profil.

```
{ "AuthenticationProfiles": [ { "AuthenticationProfileName":
"testProfile1", "AuthenticationProfileContent": "{\"AllowDBUserOverride
\":\"1\",\"Client_ID\":\"ExampleClientID\",\"App_ID\":\"ExampleAppID
\",\"AutoCreate\":false,\"enableFetchRingBuffer\":true,
\"databaseMetadataCurrentDbOnly\":true}" }, { "AuthenticationProfileName":
"testProfile2", "AuthenticationProfileContent": "{\"AllowDBUserOverride
\":\"1\",\"Client_ID\":\"ExampleClientID\",\"App_ID\":\"ExampleAppID
\",\"AutoCreate\":false,\"enableFetchRingBuffer\":true,
\"databaseMetadataCurrentDbOnly\":true}" } ] }
```

Résolution des problèmes de connexion dans Amazon Redshift

Si vous rencontrez des problèmes de connexion à votre cluster avec un outil client SQL, vérifiez plusieurs éléments pour cerner le problème. Si vous utilisez des certificats SSL ou serveur, commencez par supprimer cette complexité pendant que vous résolvez le problème de connexion.

Ensuite, rajoutez-la lorsque vous avez trouvé une solution. Pour plus d'informations, consultez Configuration des options de sécurité des connexions.

Pour plus d'informations sur les changements de comportement dans les fonctionnalités Amazon Redshift susceptibles d'affecter votre application, consultez Changements de comportement dans Amazon Redshift.

> **Important**
>
> Amazon Redshift a changé la méthode de gestion des certificats SSL. Si vous avez des difficultés à vous connecter avec SSL, il se peut que vous ayez besoin de mettre à jour vos certificats actuels d'autorité de certification racine. Pour plus d'informations, consultez Transition vers les certificats ACM pour les connexions SSL.

La section suivante présente des exemples de messages d'erreur et des solutions possibles aux problèmes de connexion. Etant donné que différents outils clients SQL fournissent différents messages d'erreur, cette liste n'est pas exhaustive, mais constitue un bon point de départ pour la résolution des problèmes.

Connexion depuis l'extérieur d'Amazon EC2 et survenue d'un problème de dépassement de délai du pare-feu

La connexion de votre client à la base de données semble se bloquer ou arriver à expiration lorsque vous exécutez de longues requêtes, par exemple une commande COPY. Dans ce cas, vous pouvez constater que la console Amazon Redshift affiche que la requête est terminée, mais que l'outil client lui-même semble toujours exécuter la requête. Les résultats de la requête peuvent être manquants ou incomplets en fonction selon le moment où la connexion s'est arrêtée.

Solutions possibles

Ce problème se produit lorsque vous vous connectez à Amazon Redshift depuis une machine autre qu'une instance Amazon EC2. Dans ce cas, les connexions inactives sont résiliées par un composant réseau intermédiaire, tel qu'un pare-feu, après une période d'inactivité. Ce comportement est typique lorsque vous vous connectez à partir d'un réseau VPN ou de votre réseau local.

Pour éviter ces délais d'attente, nous vous recommandons d'apporter les modifications suivantes :

- Augmentez les valeurs du système client qui traitent des TCP/IP délais d'attente. Apportez ces modifications sur l'ordinateur que vous utilisez pour vous connecter à votre cluster. Le délai d'expiration doit être réglé pour votre client et le réseau. Pour plus d'informations, consultez Modifier les paramètres TCP/IP du délai d'expiration.
- Le cas échéant, définissez le comportement keepalive au niveau de la DSN. Pour plus d'informations, consultez Modification des paramètres d'expiration de la DSN.

Modifier les paramètres TCP/IP du délai d'expiration

Pour modifier TCP/IP les paramètres de délai d'expiration, configurez-les en fonction du système d'exploitation que vous utilisez pour vous connecter à votre cluster.

- Linux — Si votre client fonctionne sous Linux, exécutez la commande suivante en tant qu'utilisateur root pour modifier les paramètres de délai d'attente pour la séance en cours :

  ```
  /sbin/sysctl -w net.ipv4.tcp_keepalive_time=200 net.ipv4.tcp_keepalive_intvl=200
   net.ipv4.tcp_keepalive_probes=5
  ```

  Pour conserver les paramètres, créez ou modifiez le fichier `/etc/sysctl.conf` avec les valeurs suivantes, puis redémarrez votre système.

  ```
  net.ipv4.tcp_keepalive_time=200
  net.ipv4.tcp_keepalive_intvl=200
  net.ipv4.tcp_keepalive_probes=5
  ```

- Windows — Si votre client fonctionne sous Windows, modifiez les valeurs des paramètres de registre suivants sous HKEY_LOCAL_MACHINE \ SYSTEM \ \ Services \ Tcpip CurrentControlSet \ Parameters \ :
  - KeepAliveTime: 30 000
  - KeepAliveInterval: 1000
  - TcpMaxDataRetransmissions : 10

  Ces paramètres utilisent le type de données DWORD. S'ils n'existent pas sous le chemin d'accès au registre, vous pouvez créer les paramètres et spécifiez ces valeurs recommandées. Pour plus d'informations sur la modification du registre Windows, reportez-vous à la documentation Windows.

Une fois ces valeurs définies, redémarrez votre ordinateur pour que les modifications prennent effet.

- Mac — Si votre client fonctionne sur un Mac, exécutez les commandes suivantes pour modifier les paramètres de délai d'attente pour la séance en cours :

```
sudo sysctl net.inet.tcp.keepintvl=200000
sudo sysctl net.inet.tcp.keepidle=200000
sudo sysctl net.inet.tcp.keepinit=200000
sudo sysctl net.inet.tcp.always_keepalive=1
```

Pour conserver les paramètres, créez ou modifiez le fichier `/etc/sysctl.conf` avec les valeurs suivantes :

```
net.inet.tcp.keepidle=200000
net.inet.tcp.keepintvl=200000
net.inet.tcp.keepinit=200000
net.inet.tcp.always_keepalive=1
```

Redémarrez votre ordinateur, puis exécutez les commandes suivantes pour vérifier que les valeurs sont définies.

```
sysctl net.inet.tcp.keepidle
sysctl net.inet.tcp.keepintvl
sysctl net.inet.tcp.keepinit
sysctl net.inet.tcp.always_keepalive
```

Modification des paramètres d'expiration de la DSN

Vous pouvez définir un comportement keepalive au niveau de la DSN si vous le souhaitez. Pour cela, vous ajoutez ou vous modifiez les paramètres suivants dans le fichier odbc.ini :

KeepAlivesCount

Nombre de paquets TCP keepalive qui peuvent être perdus avant que la connexion soit considérée comme interrompue.

KeepAlivesIdle

Nombre de secondes d’inactivité avant que le pilote envoie un paquet TCP keepalive.

KeepAlivesInterval

Nombre de secondes entre chaque retransmission de paquet TCP keepalive.

Si ces paramètres n'existent pas ou s'ils ont une valeur de 0, le système utilise les paramètres keepalive spécifiés TCP/IP pour déterminer le comportement du DSN keepalive. Sous Windows, vous pouvez trouver les TCP/IP paramètres dans le registre dans`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\`. Sur Linux et macOS, les TCP/IP paramètres se trouvent dans le fichier sysctl.conf.

La connexion est refusée ou échoue

Lorsque votre connexion est refusée ou échoue, vous pouvez recevoir une erreur similaire à l’une des suivantes.

- « Impossible d'établir une connexion avec*`<endpoint>`*. »
- « Impossible de se connecter au serveur : la connexion a expiré. Le serveur fonctionne-t-il sur l'hôte *`'<endpoint>'`* et accepte-t-il TCP/IP les connexions sur le port *`'<port>'`* ? »
- « Connexion refusée. Vérifiez que le nom d'hôte et le port sont corrects et que le maître de poste accepte les TCP/IP connexions. »

Solutions possibles

En général, lorsque vous recevez un message d’erreur indiquant qu’il est impossible d’établir une connexion, cela signifie qu’il y a un problème d’autorisation d’accès au cluster ou que le trafic réseau ne peut pas atteindre le cluster.

Pour vous connecter au cluster depuis un outil client en dehors du réseau sur lequel se trouve le cluster, ajoutez une règle d’entrée au groupe de sécurité du cluster. La configuration de la règle dépend de la création du cluster Amazon Redshift dans un cloud privé virtuel (VPC) :

- Si vous avez créé le cluster Amazon Redshift dans un cloud privé virtuel (VPC) basé sur Amazon VPC, ajoutez une règle entrante au groupe de sécurité VPC qui spécifie l'adresse du client, dans Amazon VPC. CIDR/IP Pour plus d’informations sur la configuration des groupes de sécurité du

VPC pour votre cluster et les options publiquement accessibles, consultez Ressources Redshift dans un VPC.

- Si vous avez créé votre cluster Amazon Redshift en dehors d'un VPC, ajoutez votre CIDR/IP adresse client au groupe de sécurité du cluster dans Amazon Redshift. Pour plus d'informations sur la configuration des groupes de sécurité de cluster, consultez Groupes de sécurité Amazon Redshift.

Si vous tentez de vous connecter au cluster à partir d'un outil client qui s'exécute sur une instance Amazon EC2, vous ajoutez également une règle d'entrée. Dans ce cas, ajoutez une règle au groupe de sécurité du cluster. La règle doit spécifier le groupe de sécurité Amazon EC2 associé à l'instance Amazon EC2 de l'outil client.

Dans certains cas, vous pouvez avoir une couche entre votre client et le serveur, telle qu'un pare-feu. Dans ce cas, assurez-vous que le pare-feu accepte les connexions entrantes via le port que vous avez configuré pour votre cluster.

Le client et le pilote sont incompatibles

Si votre client et votre pilote sont incompatibles, vous pouvez recevoir un message d'erreur indiquant : « The specified DSN contains an architecture mismatch between the Driver and Application ».

Solutions possibles

Lorsque vous tentez de vous connecter et que vous obtenez une erreur concernant une incompatibilité d'architecture, cela signifie que l'outil client et le pilote ne sont pas compatibles. Cela se produit parce que leur architecture système ne correspond pas. Par exemple, cela peut se produire si vous avez un outil client 32 bits, alors que vous avez installé la version 64 bits du pilote. Les outils clients 64 bits utilisent parfois des pilotes 32 bits, mais vous ne pouvez pas utiliser d'applications 32 bits avec des pilotes 64 bits. Assurez-vous que le pilote et l'outil client utilisent la même version d'architecture système.

Des requêtes semblent se bloquer et parfois échouent à atteindre le cluster

Vous rencontrez un problème pour terminer des requêtes, notamment que les requêtes semblent être en cours d'exécution, mais se bloquent dans l'outil client SQL. Parfois, les requêtes n'apparaissent pas dans le cluster, par exemple dans les tables système ou dans la console Amazon Redshift.

Solutions possibles

Ce problème peut se produire en raison de la perte de paquets. Dans ce cas, il existe une différence dans la taille maximale de l'unité de transmission (MTU) dans le chemin réseau entre deux hôtes IP (Internet Protocol). La taille de la MTU détermine la taille maximale, en octets, d'un paquet pouvant être transféré dans une trame Ethernet sur une connexion réseau. Dans AWS, certains types d'instances Amazon EC2 prennent en charge une MTU de 1500 (trames Ethernet v2) tandis que d'autres types d'instances prennent en charge une MTU de 9001 (TCP/IP trames jumbo).

Pour éviter que des problèmes se produisent en raison de différences de taille de la MTU, nous vous recommandons procéder comme suit :

- Si votre cluster utilise la EC2-VPC plate-forme, configurez le groupe de sécurité Amazon VPC avec une règle ICMP (Internet Control Message Protocol) personnalisée entrante qui renvoie. `Destination Unreachable` Cette règle indique que l'hôte d'origine utilise la taille de MTU la plus petite sur chemin d'accès réseau. Pour plus d'informations sur cette approche, consultez Configuration des groupes de sécurité pour autoriser le message ICMP « Destination inaccessible ».
- Si votre cluster utilise la EC2-Classic plate-forme ou si vous ne pouvez pas autoriser la règle entrante ICMP, désactivez les trames TCP/IP jumbo afin que les trames Ethernet v2 soient utilisées. Pour plus d'informations sur cette approche, consultez Configuration de la MTU d'une instance.

Configuration des groupes de sécurité pour autoriser le message ICMP « Destination inaccessible »

En cas de différence de taille de la MTU sur le réseau entre deux hôtes, vérifiez d'abord que vos paramètres réseau n'empêchent pas la détection de la MTU du chemin (PMTUD, path MTU discovery). La PMTUD permet à l'hôte de réception de répondre à l'hôte d'origine avec le message suivant ICMP suivant : `Destination Unreachable: fragmentation needed and DF set (ICMP Type 3, Code 4)`. Ce message indique que l'hôte d'origine utilise la taille de MTU la plus petite sur chemin d'accès réseau pour renvoyer la demande. Sans cette négociation, un rejet de paquet peut se produire, car la demande est trop volumineuse pour l'hôte de réception. Pour plus d'informations sur ce message ICMP, consultez RFC792 sur le site web Internet Engineering Task Force (IETF).

Si vous ne configurez pas explicitement cette règle ICMP entrante pour votre groupe de sécurité Amazon VPC, PMTUD est bloqué. Dans AWS, les groupes de sécurité sont des pare-feux virtuels qui spécifient des règles pour le trafic entrant et sortant vers une instance. Pour plus d'informations sur

le groupe de sécurité de cluster Amazon Redshift, consultez Groupes de sécurité Amazon Redshift. Pour les clusters utilisant la EC2-VPC plate-forme, Amazon Redshift utilise des groupes de sécurité VPC pour autoriser ou refuser le trafic vers le cluster. Par défaut, les groupes de sécurité sont verrouillés et refusent tout trafic entrant. Pour plus d'informations sur la façon de définir des règles entrantes et sortantes pour les EC2-VPC instances EC2-Classic ou, consultez la section Différences entre les instances internes EC2-Classic et un VPC dans le guide de l'utilisateur Amazon EC2.

Pour plus d'informations sur la procédure pour ajouter des règles aux groupes de sécurité VPC, consultez Groupes de sécurité VPC. Pour plus d'informations sur les paramètres PMTUD spécifiques requis dans cette règle, consultez Détection de la MTU du chemin dans le Guide de l'utilisateur Amazon EC2.

Configuration de la MTU d'une instance

Dans certains cas, votre cluster peut utiliser la EC2-Classic plate-forme ou vous ne pouvez pas autoriser la règle ICMP personnalisée pour le trafic entrant. Dans ces cas, nous vous recommandons d'ajuster le MTU à 1500 sur l'interface réseau (NIC) des instances EC2 à partir desquelles vous vous connectez à votre cluster Amazon Redshift. Ce réglage désactive les trames TCP/IP jumbo pour garantir que les connexions utilisent toujours la même taille de paquet. Toutefois, cette option réduit le débit maximal du réseau pour l'instance dans son ensemble, et pas seulement pour les connexions à Amazon Redshift. Pour plus d'informations, consultez les procédures suivantes.

Pour définir la MTU sur un système d'exploitation Microsoft Windows

Si votre client s'exécute sur un système d'exploitation Microsoft Windows, vous pouvez vérifier et définir la valeur de la MTU pour la carte Ethernet à l'aide de la commande `netsh`.

1. Exécutez la commande suivante afin de déterminer la valeur actuelle de la MTU :

   ```
   netsh interface ipv4 show subinterfaces
   ```

2. Vérifiez la valeur de la `MTU` pour la carte `Ethernet` dans la sortie.
3. Si la valeur n'est pas `1500`, exécutez la commande suivante pour la définir :

   ```
   netsh interface ipv4 set subinterface "Ethernet" mtu=1500 store=persistent
   ```

   Une fois cette valeur définie, redémarrez votre ordinateur pour que les modifications prennent effet.

Pour définir la MTU sur un système d’exploitation Linux

Si le client s’exécute sur un système d’exploitation Linux, vous pouvez vérifier et définir la valeur de la MTU à l’aide de la commande `ip`.

1. Exécutez la commande suivante afin de déterminer la valeur actuelle de la MTU :

```
$ ip link show eth0
```

2. Vérifiez la valeur suivant `mtu` dans la sortie.
3. Si la valeur n’est pas `1500`, exécutez la commande suivante pour la définir :

```
$ sudo ip link set dev eth0 mtu 1500
```

Pour définir la MTU sur un système d’exploitation Mac

- Suivez les instructions du site d'assistance de macOS à propos de`How to change the MTU for troubleshooting purposes`. Pour plus d’informations, consultez le site du support.

Définition du paramètre de taille d’extraction JDBC

Par défaut, le pilote Redshift JDBC utilise une mémoire tampon en anneau pour gérer efficacement la mémoire et éviter les erreurs liées au manque de mémoire. Le paramètre fetch size n'est applicable que lorsque le ring buffer est explicitement désactivé. Pour plus d'informations, consultez le lien. Dans cette configuration, vous devez définir la taille d'extraction pour contrôler le nombre de lignes extraites dans chaque lot.

Quand utiliser Fetch Size ?

Utilisez le paramètre fetch size lorsque :

- Vous avez besoin d'un contrôle précis du traitement par lots par lignes
- Utilisation d'applications existantes qui nécessitent un comportement de taille d'extraction traditionnel

Réglage de la taille de récupération

Lorsque la mémoire tampon en anneau est désactivée, le pilote JDBC collecte tous les résultats d'une requête en une seule fois par défaut. Les requêtes qui renvoient de grands ensembles de résultats peuvent consommer trop de mémoire. Pour récupérer les ensembles de résultats par lots au lieu de les récupérer tous en une seule fois, définissez le paramètre JDBC fetch size dans votre application.

> **Note**
>
> La taille de l'extraction n'est pas prise en charge pour ODBC.

Pour obtenir les meilleures performances, définissez la taille de l'extraction sur la valeur la plus élevée qui n'entraîne pas d'erreurs de mémoire. Une valeur d'extraction de taille inférieure entraîne plusieurs opérations du serveur, ce qui prolonge les temps d'exécution. Le serveur réserve des ressources, y compris l'emplacement de requête WLM et la mémoire associée, jusqu'à ce que le client récupère le jeu de résultats complet ou que la requête soit annulée. Lorsque vous ajustez la taille d'extraction de façon appropriée, ces ressources sont libérées plus rapidement, ce qui les rend disponibles pour d'autres requêtes.

> **Note**
>
> Si vous devez extraire de grands jeux de données, nous vous recommandons d'utiliser une instruction UNLOAD pour transférer les données vers Amazon S3. Lorsque vous utilisez UNLOAD, les nœuds de calcul fonctionnent en parallèle afin d'accélérer le transfert des données.

Pour plus d'informations sur la définition du paramètre de taille d'extraction JDBC, consultez Obtention de résultats basés sur un curseur dans la documentation de PostgreSQL.

Utilisation de l'API de données Amazon Redshift

L'API de données Amazon Redshift simplifie l'accès à votre entrepôt de données Amazon Redshift en éliminant le besoin de gérer les pilotes de base de données, les connexions, les configurations réseau, la mise en mémoire tampon des données, les informations d'identification, etc. Vous pouvez

exécuter des instructions SQL à l'aide des opérations de l'API Data avec le AWS SDK. Pour plus d'informations sur les fonctions de l'API de données, consultez la Référence de l'API de données Amazon Redshift.

L'API de données ne nécessite pas de connexion permanente à votre base de données. Au lieu de cela, il fournit un point de terminaison HTTP sécurisé et une intégration aux AWS SDK. Vous pouvez utiliser le point de terminaison pour exécuter des instructions SQL sans avoir à gérer de connexions. Les appels à l'API de données sont asynchrones. L'API Data peut utiliser des informations d'identification stockées dans la base de données AWS Secrets Manager ou des informations d'identification temporaires. Il n'est pas nécessaire de transmettre des mots de passe dans les appels d'API avec l'une ou l'autre méthode d'autorisation. Pour plus d'informations sur AWS Secrets Manager, voir Qu'est-ce que AWS Secrets Manager ? dans le Guide de AWS Secrets Manager l'utilisateur. Vous pouvez également l'utiliser AWS IAM Identity Center pour l'autorisation.

Grâce à l'API Data, vous pouvez accéder par programmation aux données Amazon Redshift via des applications basées sur des services Web AWS Lambda, notamment des blocs-notes Amazon SageMaker AI et. AWS Cloud9 Pour plus d'informations sur ces applications AWS Lambda, consultez Amazon SageMaker AI et AWS Cloud9.

Pour en savoir plus sur l'API de données, consultez Mise en route avec l'API de données Amazon Redshift sur le le blog AWS Big Data.

Utilisation de l'API de données Amazon Redshift

Avant d'utiliser l'API de données Amazon Redshift, passez en revue les étapes suivantes :

1. Déterminez si vous, en tant qu'appelant de l'API de données, disposez des autorisations requises. Pour de plus amples informations concernant l'autorisation, consultez Autorisation de l'accès à l'API de données Amazon Redshift.
2. Déterminez si vous prévoyez d'appeler l'API de données avec les informations d'identification d'authentification de Secrets Manager, avec des informations d'identification temporaires ou avec AWS IAM Identity Center. Pour de plus amples informations, veuillez consulter Choix des informations d'authentification de la base de données lors de l'appel de l'API de données Amazon Redshift..
3. Configurez un secret si vous utilisez Secrets Manager pour les informations d'identification d'authentification. Pour plus d'informations, consultez Stockage des informations d'identification de base de données AWS Secrets Manager.

4. Passez en revue les considérations et les limitations lors de l'appel de l'API de données. Pour de plus amples informations, veuillez consulter Considérations relatives à l'appel à l'API de données Amazon Redshift.
5. Appelez l'API Data depuis le AWS Command Line Interface (AWS CLI), depuis votre propre code ou à l'aide de l'éditeur de requêtes de la console Amazon Redshift. Pour obtenir des exemples d'appel depuis AWS CLI, consultez Appel à l'API de données.

Considérations relatives à l'appel à l'API de données Amazon Redshift

Tenez compte des éléments suivants lorsque vous appelez l'API de données :

- L'API de données Amazon Redshift peut accéder aux bases de données dans les clusters Amazon Redshift provisionnés et les groupes de travail Redshift sans serveur. Pour obtenir la liste des Régions AWS endroits où l'API Redshift Data est disponible, consultez les points de terminaison répertoriés pour l'API https://docs.aws.amazon.com/general/latest/gr/redshift-service.html Redshift Data dans le. Référence générale d'Amazon Web Services
- La durée maximale d'une requête est de 24 heures.
- Le nombre maximum de requêtes actives (`STARTED`et de `SUBMITTED` requêtes) par cluster Amazon Redshift est de 500.
- La taille maximale du résultat de requête est de 500 Mo (après compression gzip). Si un appel renvoie plus de 500 Mo de données de réponse, l'appel est terminé.
- La durée maximale de conservation des résultats de la requête est de 24 heures.
- La taille maximale de l'instruction de requête est de 200 Ko.
- L'API Data est disponible pour interroger tous les groupes de travail sans serveur et les clusters provisionnés à un ou plusieurs nœuds des types de nœuds suivants :
  - dc2.large
  - dc2.8xlarge
  - rg.large
  - rg.xlarge
  - environ 4 x large
  - environ 12 x large
  - ra3.large
  - ra3.xlplus

  - ra3.4xlarge
  - ra3.16xlarge
- Le clusters doit être dans un cloud privé virtuel (VPC) basé sur le service Amazon VPC.
- Par défaut, les utilisateurs ayant le même rôle IAM que l'exécutant d'une fonction API `ExecuteStatement` ou `BatchExecuteStatement` peuvent agir sur la même déclaration avec des fonctions API `CancelStatement`, `DescribeStatement`, `GetStatementResult`, `GetStatementResultV2` et `ListStatements`. Pour agir sur la même instruction SQL provenant d'un autre utilisateur, l'utilisateur doit pouvoir assumer le rôle IAM de l'utilisateur qui a exécuté l'instruction SQL. Pour plus d'informations sur la façon d'assumer un rôle, consultez Autorisation de l'accès à l'API de données Amazon Redshift.
- Les instructions SQL du `Sqls` paramètre de l'opération d'`BatchExecuteStatement`API s'exécutent en série dans l'ordre du tableau. Les instructions SQL suivantes ne démarrent pas tant que l'instruction précédente n'est pas terminée. Par défaut, toutes les instructions SQL sont exécutées en tant que transaction unique. Si une instruction SQL échoue, tout le travail est annulé. Utilisez le `ExecutionMode` paramètre pour contrôler le comportement des transactions :
  - `TRANSACTION`(par défaut) — Le service exécute toutes les instructions SQL en tant que transaction unique et les valide ou les annule toutes ensemble.
  - `AUTO_COMMIT`— Chaque instruction SQL est validée individuellement. L'échec d'une déclaration n'affecte pas les autres.

  Pour obtenir un exemple, consultez Exécuter plusieurs instructions SQL.
- La durée de conservation maximale d'un jeton client utilisé dans une opération d'API `ExecuteStatement` ou `BatchExecuteStatement` est de 8 heures.
- Le `WaitTimeSeconds` paramètre facultatif permet à l'API Data d'attendre jusqu'à 30 secondes lorsque l'opération soumet une nouvelle requête ou s'inscrit dans le cadre d'une requête en cours. Cela réduit le nombre de demandes de sondage, ce qui se traduit par une diminution des allers-retours et une diminution de la latence. Pour de plus amples informations, veuillez consulter Réduisez les appels d'API grâce à de longues interrogations.
- Si les clusters provisionnés par Amazon Redshift et le groupe de travail Redshift Serverless sont chiffrés à l'aide d'une clé gérée par le client, Redshift crée une autorisation qui permet à l'API Redshift Data d'utiliser la clé pour ses opérations. Pour plus d'informations, consultez Utilisation AWS KMS avec l'API Amazon Redshift Data.
- Chaque API de l'API de données Redshift dispose d'un quota de transactions par seconde avant de limiter les demandes. Pour ce quota, consultez Quotas pour l'API de données Amazon Redshift. Si le taux de demande dépasse le quota, une exception `ThrottlingException` avec le code

d'état HTTP : 400 est renvoyée. Pour répondre à la limitation, utilisez une stratégie de nouvelle tentative telle que décrite dans Comportement de nouvelle tentative, dans le Guide de référence des outils et des kits AWS SDK. Cette stratégie est implémentée automatiquement pour les erreurs de limitation dans certains kits AWS SDK.

> **Note**
>
> Par défaut AWS Step Functions, les nouvelles tentatives ne sont pas activées. Si vous devez appeler une API de données Redshift dans une machine d'état Step Functions, incluez le paramètre d'idempotence `ClientToken` dans votre appel d'API de données Redshift. La valeur de `ClientToken` doit être conservée entre les nouvelles tentatives. Dans l'exemple d'extrait suivant d'une demande adressée à l'API `ExecuteStatement`, l'expression `States.ArrayGetItem(States.StringSplit($$.Execution.Id, ':'), 7)` utilise une fonction intrinsèque pour extraire la partie UUID de `$$.Execution.Id`, qui est unique pour chaque exécution de la machine d'état. Pour plus d'informations, consultez Fonctions intrinsèques dans le Guide du développeur AWS Step Functions .
>
> ```
> {
>   "Database": "dev",
>   "Sql": "select 1;",
>   "ClusterIdentifier": "MyCluster",
>   "ClientToken.$": "States.ArrayGetItem(States.StringSplit($$.Execution.Id,
>  ':'), 7)"
> }
> ```

Choix des informations d'authentification de la base de données lors de l'appel de l'API de données Amazon Redshift.

Lorsque vous appelez l'API de données, vous utilisez l'une des méthodes d'authentification suivantes pour certaines fonctions de l'API. Chaque méthode nécessite une combinaison différente de paramètres.

AWS IAM Identity Center

L'API de données est accessible avec un utilisateur à authentification unique enregistré dans AWS IAM Identity Center. Pour plus d'informations sur les étapes de configuration d'IAM Identity Center, consultez Utilisation de l'API de données avec la propagation d'identité de confiance.

AWS Secrets Manager

Avec cette méthode, fournissez `secret-arn` un secret stocké dans AWS Secrets Manager lequel a `username` et`password`. Le secret spécifié contient des informations d'identification pour vous connecter à la `database` que vous spécifiez. Lorsque vous vous connectez à un cluster, vous fournissez également le nom de la base de données, Si vous fournissez un identifiant de cluster (`dbClusterIdentifier`), il doit correspondre à l'identifiant de cluster stocké dans le secret. Lorsque vous vous connectez à un groupe de travail sans serveur, vous devez également fournir le nom de la base de données. Pour de plus amples informations, veuillez consulter Stockage des informations d'identification de base de données AWS Secrets Manager.

Avec cette méthode, vous pouvez également fournir une `region` valeur qui spécifie l' Région AWS emplacement de vos données.

Informations d'identification temporaires

Avec cette méthode, choisissez l'une des options suivantes :

- Lors de la connexion à un groupe de travail sans serveur, indiquez le nom du groupe de travail et le nom de la base de données. Le nom de l'utilisateur de la base de données est dérivé de l'identité IAM. Par exemple, `arn:iam::123456789012:user:foo` a le nom d'utilisateur de la base de données `IAM:foo`. De plus, l'autorisation d'appeler l'opération `redshift-serverless:GetCredentials` est requise.
- Lorsque vous vous connectez à un cluster en tant qu'identité IAM, indiquez l'identifiant du cluster et le nom de la base de données. Le nom de l'utilisateur de la base de données est dérivé de l'identité IAM. Par exemple, `arn:iam::123456789012:user:foo` a le nom d'utilisateur de la base de données `IAM:foo`. De plus, l'autorisation d'appeler l'opération `redshift:GetClusterCredentialsWithIAM` est requise.
- Lorsque vous vous connectez à un cluster en tant qu'utilisateur de base de données, indiquez l'identifiant du cluster, le nom de la base de données et le nom de l'utilisateur de la base de données. De plus, l'autorisation d'appeler l'opération `redshift:GetClusterCredentials` est requise. Pour savoir comment rejoindre des groupes de base de données lors de la connexion avec cette méthode, consultez Rejoindre des groupes de base de données lors de la connexion à un cluster.

Avec cette méthode, vous pouvez également fournir une `region` valeur qui spécifie l' Région AWS emplacement de vos données.

Mappage de types de données JDBC lors de l'appel à l'API de données Amazon Redshift

Le tableau suivant associe les types de données Java Database Connectivity (JDBC) aux types de données que vous spécifiez dans les appels d'API de données.

Type de données JDBC	Type de données API de données
`INTEGER, SMALLINT, BIGINT`	`LONG`
`FLOAT, REAL, DOUBLE`	`DOUBLE`
`DECIMAL`	`STRING`
`BOOLEAN, BIT`	`BOOLEAN`
`BLOB, BINARY, LONGVARBINARY`	`BLOB`
`VARBINARY`	`STRING`
`CLOB`	`STRING`
Autres types (y compris les types liés à la date et à l'heure)	`STRING`

Les valeurs de chaîne de caractères sont transmises à la base de données Amazon Redshift et implicitement converties en un type de données de base de données.

> **Note**
>
> Actuellement, l'API de données ne prend pas en charge les tableaux d'identificateurs uniques universels (UUID).

Exécution d’instructions SQL avec des paramètres lors de l’appel à l’API de données Amazon Redshift

Vous pouvez contrôler le texte SQL soumis au moteur de la base de données en appelant la fonction de l’API de données tout en utilisant des paramètres pour les parties de l’instruction SQL. Les paramètres nommés constituent un moyen flexible de passer des paramètres sans les coder en dur dans le texte. Ils vous aident à réutiliser le texte SQL et à éviter les problèmes d’injection SQL.

L'exemple suivant montre les paramètres nommés d'un `parameters` champ d'une `batch-execute-statement` AWS CLI commande `execute-statement` ou.

```
--parameters "[{\"name\": \"id\", \"value\": \"1\"},{\"name\": \"address\", \"value\":
 \"Seattle\"}]"
```

Tenez compte des éléments suivants lorsque vous utilisez des paramètres nommés :

- Les paramètres nommés ne peuvent être utilisés que pour remplacer des valeurs dans les instructions SQL.
  - Vous pouvez remplacer les valeurs d’une instruction INSERT, telle que `INSERT INTO mytable VALUES(:val1)`.

    Les paramètres nommés peuvent être dans n’importe quel ordre et ils peuvent être utilisés plusieurs fois dans le texte SQL. L’option de paramétrage présentée dans un précédent exemple, les valeurs `1` et `Seattle` sont insérées dans les colonnes `id` et `address` de la table. Dans le texte SQL, vous spécifiez les paramètres nommés comme suit :

    ```
    --sql "insert into mytable values (:id, :address)"
    ```

  - Vous pouvez remplacer les valeurs dans une clause de condition, telle que `WHERE attr >= :val1`, `WHERE attr BETWEEN :val1 AND :val2` et `HAVING COUNT(attr) > :val`.
  - Vous ne pouvez pas remplacer les noms de colonnes dans une instruction SQL, tels que `SELECT column-name`, `ORDER BY column-name`, ou `GROUP BY column-name`.

    Par exemple, l’instruction SELECT suivante échoue en raison d’une syntaxe non valide.

    ```
    --sql "SELECT :colname, FROM event" --parameters "[{\"name\": \"colname\", \"value
    \": \"eventname\"}]"
    ```

Si vous décrivez (opération `describe-statement`) l'instruction avec l'erreur de syntaxe, la commande `QueryString` renvoyée ne remplace pas le nom de la colonne par le paramètre (`"QueryString": "SELECT :colname, FROM event"`) et une erreur est signalée (ERREUR : erreur de syntaxe à ou près de « FROM » Position : 12).

- Vous ne pouvez pas remplacer les noms de colonnes dans une fonction d'agrégation, tels que `COUNT(column-name)`, `AVG(column-name)`, ou `SUM(column-name)`.
- Vous ne pouvez pas remplacer les noms de colonnes dans une clause JOIN.

- Lorsque le SQL s'exécute, les données sont implicitement converties en un type de données. Pour plus d'informations sur le moulage des types de données, consultez Types de données dans le Manuel du développeur de base de données Amazon Redshift.
- Vous ne pouvez pas définir une valeur sur NULL. L'API de données l'interprète comme la chaîne littérale `NULL`. L'exemple suivant remplace `id` par la chaîne littérale `null`. Pas la valeur SQL NULL.

```
--parameters "[{\"name\": \"id\", \"value\": \"null\"}]"
```

- Vous ne pouvez pas définir une valeur de longueur de zéro. L'instruction SQL de l'API de données échoue. L'exemple suivant tente de définir `id` avec une valeur de longueur de zéro et se solde par un échec de l'instruction SQL.

```
--parameters "[{\"name\": \"id\", \"value\": \"\"}]"
```

- Vous ne pouvez pas définir un nom de table dans l'instruction SQL avec un paramètre. L'API de données suit la règle du JDBC `PreparedStatement`.
- La sortie de l'opération `describe-statement` renvoie les paramètres de requête d'une instruction SQL.
- Les `batch-execute-statement` opérations `execute-statement` et prennent en charge les instructions SQL avec des paramètres. Lors de l'utilisation`batch-execute-statement`, les paramètres sont partagés entre toutes les instructions SQL du lot. Chaque instruction SQL peut faire référence à un sous-ensemble des paramètres fournis, mais chaque paramètre doit être utilisé par au moins une instruction SQL.

Exécution d'instructions SQL avec un jeton d'idempotence lors de l'appel à l'API de données Amazon Redshift

Lorsque vous effectuez une demande d'API de mutation, la demande renvoie généralement un résultat avant la fin des flux de travail asynchrones de l'opération. Les opérations peuvent également expirer ou rencontrer d'autres problèmes de serveur avant d'être terminées, même si la demande a déjà renvoyé un résultat. Par conséquent, il peut être difficile de déterminer si la demande a abouti ou non et de multiples tentatives peuvent être déclenchées pour s'assurer que l'opération se termine correctement. Toutefois, si la demande initiale et les tentatives suivantes aboutissent, l'opération est terminée plusieurs fois. Vous pouvez ainsi mettre à jour plus de ressources que prévu.

L'idempotence garantit qu'une demande d'API se termine correctement. Avec une demande idempotente, si la demande d'origine se termine avec succès, toutes les tentatives suivantes se terminent avec succès, sans aucune action supplémentaire. Les opérations `ExecuteStatement` et `BatchExecuteStatement` de l'API de données ont un paramètre idempotent `ClientToken` facultatif. Le `ClientToken` expire au bout de 8 heures.

> **Important**
>
> Si vous appelez `ExecuteStatement` et effectuez `BatchExecuteStatement` des opérations à partir d'un AWS SDK, celui-ci génère automatiquement un jeton client à utiliser lors d'une nouvelle tentative. Dans ce cas, nous ne recommandons pas d'utiliser le paramètre `client-token` avec les opérations `ExecuteStatement` et `BatchExecuteStatement`. Consultez le CloudTrail journal pour voir les`ClientToken`. Pour un exemple de CloudTrail journal, consultezExemples d'API de données Amazon Redshift.

La `execute-statement` AWS CLI commande suivante illustre le `client-token` paramètre facultatif pour l'idempotence.

```
aws redshift-data execute-statement
    --secret-arn arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-
hKgPWn
    --cluster-identifier mycluster-test
    --sql "select * from stl_query limit 1"
    --database dev
    --client-token b855dced-259b-444c-bc7b-d3e8e33f94g1
```

La table suivante présente certaines réponses courantes que vous pouvez obtenir pour les demandes d'API idempotentes et fournit des recommandations pour réessayer.

Réponse	Recommendation	Commentaires
200 (OK)	Ne pas réessayer	La demande d'origine s'est terminée avec succès. Toutes les tentatives suivantes sont renvoyées avec succès.
Codes de réponse de la série 400	Ne pas réessayer	La demande présente un problème, parmi les suivants : • Elle inclut un paramètre ou une combinaison de paramètres invalide. • Elle utilise une action ou une ressource pour laquelle vous n'avez pas les autorisations nécessaires. • Elle utilise une ressource qui est en train de changer d'état. Si la demande concerne une ressource en train de changer d'état, il est possible que la nouvelle tentative aboutisse.
Codes de réponse de la série 500	Réessayer	L'erreur est causée par un problème AWS côté serveur et est généralement transitoire. Répétez la demande avec une stratégie de backoff appropriée.

Pour plus d'informations sur les codes de réponse Amazon Redshift, consultez Common Errors (Erreurs courantes) dans la référence d'API Amazon Redshift.

Exécution d'instructions SQL avec réutilisation de session lors de l'appel à l'API de données Amazon Redshift

Lorsque vous faites une demande d'API pour exécuter une instruction SQL, la session pendant laquelle le SQL s'exécute est généralement interrompue lorsque le SQL est terminé. Pour que la session reste active pendant un certain nombre de secondes, les opérations d'API de données `ExecuteStatement` et `BatchExecuteStatement` ont un paramètre `SessionKeepAliveSeconds` facultatif. Un champ de réponse `SessionId` contient l'identité de la session qui peut ensuite être utilisée dans les opérations `ExecuteStatement` et `BatchExecuteStatement` suivantes. Lors des appels suivants, vous pouvez en spécifier un autre `SessionKeepAliveSeconds` pour modifier le délai d'inactivité. Si le `SessionKeepAliveSeconds` n'est pas modifié, le paramètre de délai d'inactivité initial est conservé. Tenez compte des éléments suivants lorsque vous utilisez la réutilisation de session :

- La valeur maximale de `SessionKeepAliveSeconds` est de 24 heures.
- La session peut durer 24 heures au maximum. Après 24 heures, la session est fermée de force et les requêtes en cours sont interrompues.
- Le nombre maximum de sessions par cluster Amazon Redshift ou groupe de travail Redshift sans serveur est de 500.
- Vous ne pouvez exécuter qu'une seule requête à la fois dans une session. Vous devez attendre la fin de la requête pour exécuter la requête suivante au cours de la même session. En d'autres termes, vous ne pouvez pas exécuter de requêtes en parallèle dans une session donnée.
- L'API de données ne peut pas mettre les requêtes en file d'attente pour une session donnée.

Pour récupérer l'`SessionId` utilisé par les appels aux opérations `ExecuteStatement` et `BatchExecuteStatement`, l'appel `DescribeStatement` et les opérations `ListStatements`. Pour répertorier les sessions et leur statut, utilisez l'`ListSessions`opération. Pour de plus amples informations, veuillez consulter Liste des sessions.

L'exemple suivant montre comment utiliser les paramètres `SessionKeepAliveSeconds` et `SessionId` pour maintenir une session active et la réutiliser. Tout d'abord, appelez la `execute-statement` AWS CLI commande avec le `session-keep-alive-seconds` paramètre facultatif défini sur2.

```
aws redshift-data execute-statement
```

```
    --session-keep-alive-seconds 2
    --sql "select 1"
    --database dev
    --workgroup-name mywg
```

La réponse contient l'identifiant de session.

```
{
    "WorkgroupName": "mywg",
    "CreatedAt": 1703022996.436,
    "Database": "dev",
    "DbUser": "awsuser",
    "Id": "07c5ffea-76d6-4786-b62c-4fe3ef529680",
    "SessionId": "5a254dc6-4fc2-4203-87a8-551155432ee4"
}
```

Ensuite, appelez la `execute-statement` AWS CLI commande avec `SessionId` le résultat du premier appel. Et éventuellement, spécifiez le paramètre `session-keep-alive-seconds` défini sur `10` pour modifier la valeur du délai d'inactivité.

```
aws redshift-data execute-statement
    --sql "select 1"
    --session-id 5a254dc6-4fc2-4203-87a8-551155432ee4
    --session-keep-alive-seconds 10
```

Récupération des résultats des instructions SQL

Vous utilisez différentes opérations de l'API de données pour récupérer les résultats SQL en fonction du format des résultats. Lorsque vous appelez `ExecuteStatement` et effectuez les opérations `BatchExecuteStatement`, vous pouvez spécifier si les résultats sont au format JSON ou CSV. Si vous ne spécifiez rien, le format par défaut est JSON. Pour récupérer les résultats JSON, utilisez l'opération `GetStatementResult`. Pour récupérer les résultats CSV, utilisez l'opération `GetStatementResultV2`.

Les résultats renvoyés au format JSON sont des enregistrements qui incluent des métadonnées relatives à chaque colonne. Chaque enregistrement est au format JSON. Par exemple, la réponse de `GetStatementResult` ressemble à ceci :

```
{
```

```
   "ColumnMetadata": [
      {
         "isCaseSensitive": false,
         "isCurrency": false,
         "isSigned": true,
         "label": "?column?",
         "name": "?column?",
         "nullable": 1,
         "precision": 10,
         "scale": 0,
         "schemaName": "",
         "tableName": "",
         "typeName": "int4",
         "length": 0
      }
   ],
   "NextToken": "<token>",
   "Records": [
        [
            {
                "longValue": 1
            }
        ]
    ],
   "TotalNumRows": <number>
}
```

Les résultats renvoyés au format CSV sont des enregistrements qui incluent des métadonnées relatives à chaque colonne. Les résultats sont renvoyés sous forme de blocs de 1 Mo, chaque bloc pouvant stocker un nombre illimité de lignes au format CSV. Chaque requête renvoie jusqu'à 15 Mo de résultats. Si les résultats sont supérieurs à 15 Mo, un jeton de page suivante est renvoyé pour continuer à récupérer les résultats. Par exemple, la réponse de `GetStatementResultV2` ressemble à ceci :

```
{
    "ColumnMetadata": [
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "?column?",
            "name": "?column?",
```

```
            "nullable": 1,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "",
            "typeName": "int4",
            "length": 0
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "?column?",
            "name": "?column?",
            "nullable": 1,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "",
            "typeName": "int4",
            "length": 0
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "?column?",
            "name": "?column?",
            "nullable": 1,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "",
            "typeName": "int4",
            "length": 0
        }
    ],
    "NextToken": "<token>",
    "Records": [
        [
            {
                "CSVRecords":"1,2,3\r\n4,5,6\r\n7,8,9\r\n, ... 1MB" // First 1MB Chunk
            },
            {
```

```
                "CSVRecords":"1025,1026,1027\r\n1028,1029,1030\r\n...2MB" // Second 1MB
 chunk
            }
            ...
        ]
    ],
    "ResultFormat" : "CSV",
    "TotalNumRows": <number>
}
```

Autorisation de l'accès à l'API de données Amazon Redshift

Pour accéder à l'API de données, un utilisateur doit recevoir une autorisation. Vous pouvez autoriser un utilisateur à accéder à l'API de données en ajoutant une politique gérée, qui est une politique Gestion des identités et des accès AWS (IAM) prédéfinie, à l'utilisateur concerné. Il est recommandé d'associer des politiques d'autorisation à un rôle IAM, puis de l'attribuer à des utilisateurs et à des groupes, le cas échéant. Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift. Pour voir les autorisations autorisées et refusées par les politiques gérées, consultez la console IAM (https://console.aws.amazon.com/iam/).

Configuration des autorisations IAM

Amazon Redshift fournit la politique gérée par `AmazonRedshiftDataFullAccess`. Cette politique fournit un accès complet aux fonctions de l'API de données Amazon Redshift. Cette politique permet également un accès limité à des opérations spécifiques d'API Amazon Redshift et IAM nécessaires pour authentifier et accéder à un cluster Amazon Redshift ou à un groupe de travail Redshift Serverless. AWS Secrets Manager

Vous pouvez également créer votre propre politique IAM qui autorise l'accès à des ressources spécifiques. Pour créer votre politique, utilisez la politique `AmazonRedshiftDataFullAccess` comme modèle de départ. Une fois votre politique créée, ajoutez-la à chaque utilisateur ayant besoin d'accéder à l'API de données.

Prenez les exigences suivantes de la politique IAM associée à l'utilisateur :

- Si vous l'utilisez AWS Secrets Manager pour vous authentifier, vérifiez que la politique autorise l'utilisation de l'`secretsmanager:GetSecretValue`action pour récupérer le secret associé à la clé`RedshiftDataFullAccess`.
- Si vous utilisez des informations d'identification temporaires pour vous authentifier auprès d'un cluster, confirmez que la politique autorise l'utilisation de l'action

`redshift:GetClusterCredentials` pour le nom d'utilisateur de la base de données `redshift_data_api_user` pour toute base de données du cluster. Ce nom d'utilisateur doit déjà avoir été créé dans votre base de données.

- Si vous utilisez des informations d'identification temporaires pour vous authentifier auprès d'un groupe de travail sans serveur, confirmez que la politique autorise l'utilisation de l'action `redshift-serverless:GetCredentials` pour récupérer le groupe de travail identifié avec la clé `RedshiftDataFullAccess`. L'utilisateur de la base de données est mappé 1:1 à l'identité de la source Gestion des identités et des accès AWS (IAM). Par exemple, l'utilisateur sample_user est mappé à l'utilisateur de la base de données `IAM:sample_user`, et le rôle IAM sample_role est mappé à `IAMR:sample_role`. Pour plus d'informations sur les identités IAM, consultez Identités IAM (utilisateurs, groupes d'utilisateurs et rôles) dans le Guide de l'utilisateur IAM.
- L'action IAM `redshift-data:GetStatementResult` permet d'accéder à la fois aux opérations d'API `GetStatementResult` et `GetStatementResultV2`.

Les liens suivants fournissent des informations supplémentaires sur Gestion des identités et des accès AWS le Guide de l'utilisateur IAM.

- Pour plus d'informations sur la création de rôles IAM, consultez Création de rôles IAM.
- Pour plus d'informations sur la création de politiques IAM, consultez Création de politiques IAM.
- Pour en savoir plus sur l'ajout d'une politique IAM à un utilisateur, consultez Ajout et suppression d'autorisations basées sur l'identité IAM.

Exécution d'une requête sur un cluster appartenant un autre compte

Pour exécuter une requête sur un cluster appartenant à un autre compte, le compte propriétaire doit fournir un rôle IAM que l'API de données peut assumer dans le compte appelant. Par exemple, supposons que le compte B possède un cluster auquel le compte A doit accéder. Le compte B peut associer la politique AWS gérée `AmazonRedshiftDataFullAccess` au rôle IAM du compte B. Ensuite, le compte B approuve le compte A à l'aide d'une politique de confiance telle que la suivante :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/someRoleA"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Enfin, le rôle IAM du compte A doit être en mesure d'assumer le rôle IAM du compte B.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "arn:aws:iam::111122223333:role/someRoleB"
    }
}
```

Spécifiez un rôle IAM qui limite les ressources aux groupes de travail Redshift Serverless et aux clusters Amazon Redshift dans un Compte AWS

Vous pouvez spécifier des ARN de ressources dans votre politique basée sur l'identité pour contrôler l'accès aux groupes de travail Redshift sans serveur et aux clusters Amazon Redshift dans un Compte AWS. Cet exemple montre comment créer une politique qui autorise l'accès à l'API de données uniquement pour le groupe de travail et les clusters spécifiés Compte AWS.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "redshift-data:CancelStatement",
                "redshift-data:DescribeStatement",
                "redshift-data:GetStatementResult",
                "redshift-data:ListStatements"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "redshift-data:*",
            "Resource": [
                "arn:aws:redshift:us-east-1:111122223333:workgroup/*",
                "arn:aws:redshift:us-east-1:111122223333:cluster:*"
            ]
        }
    ]
}
```

Configurer une politique IAM qui restreint l'accès aux informations des instructions SQL au seul propriétaire de l'instruction

Par défaut, l'API de données Amazon Redshift considère le rôle IAM utilisé lors de l'appel `ExecuteStatement` et `BatchExecuteStatement` comme le propriétaire de l'instruction SQL. Toute personne autorisée à assumer ce rôle peut accéder aux informations relatives à l'instruction SQL, notamment à ses résultats. Pour restreindre l'accès aux informations des instructions SQL à une session de rôle IAM avec un propriétaire particulier, ajoutez une condition `redshift-data:statement-owner-iam-userid: "${aws:userid}"`. La politique IAM suivante restreint l'accès.

JSON

```
{
"Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "redshift-data:CancelStatement",
```

```
                "redshift-data:DescribeStatement",
                "redshift-data:GetStatementResult",
                "redshift-data:ListStatements"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "redshift-data:statement-owner-iam-userid": "${aws:userid}"
                }
            }
        }
    ]
}
```

Vous pouvez utiliser la condition `statement-owner-iam-userid` avec `CancelStatement`, `DescribeStatement`, `GetStatementResult` et `ListStatements`. Pour plus d'informations, consultez Actions définies par l'API de données Amazon Redshift.

Configurer une politique IAM qui limite l'accès aux résultats SQL au seul propriétaire de la session

Par défaut, l'API de données Amazon Redshift considère le rôle IAM utilisé lors de l'appel `ExecuteStatement` et `BatchExecuteStatement` comme le propriétaire de la session de base de données qui exécute l'instruction SQL. Toute personne autorisée à assumer ce rôle peut soumettre des requêtes à la session de base de données. Pour restreindre l'accès à la session à une session de rôle IAM avec un propriétaire particulier, ajoutez une condition `redshift-data:session-owner-iam-userid: "${aws:userid}"`. La politique IAM suivante restreint l'accès.

La politique IAM suivante permet uniquement au propriétaire de la session d'obtenir les résultats des instructions. La condition `session-owner-iam-userid` est utilisée pour limiter l'accès aux ressources au `userid` spécifié.

JSON

```
{
"Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "redshift-data:ExecuteStatement",
```

```
                "redshift-data:BatchExecuteStatement"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "redshift-data:session-owner-iam-userid": "${aws:userid}"
                }
            }
        }
    ]
}
```

Vous pouvez utiliser la condition `session-owner-iam-userid` avec `ExecuteStatement` et `BatchExecuteStatement`. Pour plus d'informations, consultez Actions définies par l'API de données Amazon Redshift.

Stockage des informations d'identification de base de données AWS Secrets Manager

Lorsque vous appelez l'API de données, vous pouvez utiliser un secret dans AWS Secrets Manager pour transmettre les informations d'identification du cluster ou du groupe de travail sans serveur. Pour ce faire, vous devez spécifier le nom du secret ou son ARN (Amazon Resource Name).

Pour stocker des informations d'identification avec Secrets Manager, vous devez disposer d'une autorisation de politique gérée par `SecretManagerReadWrite`. Pour plus d'informations sur les autorisations minimales, consultez la section Création et gestion de AWS secrets avec Secrets Manager dans le Guide de AWS Secrets Manager l'utilisateur.

Pour sauvegarder vos informations d'identification dans un secret pour un cluster Amazon Redshift

1. Utilisez la AWS Secrets Manager console pour créer un secret contenant les informations d'identification de votre cluster :
   - Lorsque vous choisissez Store a new secret (Sauvegarder un nouveau secret), sélectionnez Credentials for Redshift cluster (Informations d'identification du cluster Redshift).
   - Sauvegardez les valeurs User name (Nom d'utilisateur) (utilisateur de la base de données), Password (Mot de passe) et DB cluster (Cluster de base de données) (identifiant du cluster) dans votre secret.
   - Étiquetez le secret avec la clé `RedshiftDataFullAccess`. La politique AWS gérée `AmazonRedshiftDataFullAccess` n'autorise l'action que

`secretsmanager:GetSecretValue` pour les secrets marqués par la cléRedshiftDataFullAccess.

Pour obtenir des instructions, consultez Création d'un secret basique dans le Guide de l'utilisateur AWS Secrets Manager .

2. Utilisez la AWS Secrets Manager console pour afficher les détails du secret que vous avez créé ou exécutez la `aws secretsmanager describe-secret` AWS CLI commande.

   Notez le nom et l'ARN du secret. Vous pouvez les utiliser dans les appels à l'API de données.

Pour stocker vos informations d'identification dans un secret pour un groupe de travail sans serveur

1. Utilisez AWS Secrets Manager AWS CLI des commandes pour stocker un secret contenant les informations d'identification de votre groupe de travail sans serveur :

   - Créez votre secret dans un fichier, par exemple, un fichier JSON nommé `mycreds.json`. Fournissez les valeurs du champ User name (Nom d'utilisateur), à savoir l'utilisateur de la base de données, et du champ Password (Mot de passe) dans le fichier.

     ```
     {
           "username": "myusername",
           "password": "mypassword"
     }
     ```

   - Stockez vos valeurs dans votre secret et étiquetez le secret avec la clé `RedshiftDataFullAccess`.

     ```
     aws secretsmanager create-secret --name MyRedshiftSecret  --tags
      Key="RedshiftDataFullAccess",Value="serverless" --secret-string file://
     mycreds.json
     ```

     Le résultat est présenté ci-dessous :

     ```
     {
         "ARN":
      "arn:aws:secretsmanager:region:accountId:secret:MyRedshiftSecret-mvLHxf",
         "Name": "MyRedshiftSecret",
         "VersionId": "a1603925-e8ea-4739-9ae9-e509eEXAMPLE"
     ```

```
}
```

Pour plus d'informations, consultez Création d'un secret basique avec AWS CLI dans le Guide de l'utilisateur AWS Secrets Manager .

2. Utilisez la AWS Secrets Manager console pour afficher les détails du secret que vous avez créé ou exécutez la `aws secretsmanager describe-secret` AWS CLI commande.

   Notez le nom et l'ARN du secret. Vous pouvez les utiliser dans les appels à l'API de données.

Création d'un point de terminaison Amazon VPC (AWS PrivateLink) pour l'API Data

Amazon Virtual Private Cloud (Amazon VPC) vous permet de lancer AWS des ressources, telles que des clusters et des applications Amazon Redshift, dans un cloud privé virtuel (VPC). AWS PrivateLink fournit une connectivité privée entre les clouds privés virtuels (VPC) et les AWS services en toute sécurité sur le réseau Amazon. À l'aide de AWS PrivateLink, vous pouvez créer des points de terminaison VPC, que vous pouvez utiliser pour vous connecter à des services sur différents comptes et VPC basés sur Amazon VPC. Pour plus d'informations à ce sujet AWS PrivateLink, consultez VPC Endpoint Services (AWS PrivateLink) dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.

Vous pouvez appeler l'API de données avec des points de terminaison Amazon VPC. L'utilisation d'un point de terminaison Amazon VPC permet de maintenir le trafic entre les applications de votre Amazon VPC et l'API de données dans le réseau AWS , sans utiliser d'adresses IP publiques. Les points de terminaison Amazon VPC peuvent vous aider à respecter les exigences réglementaires et de conformité liées à la limitation de la connectivité Internet publique. Par exemple, si vous utilisez un point de terminaison Amazon VPC, vous pouvez maintenir le trafic entre une application exécutée sur une instance Amazon EC2 et l'API de données dans les VPC qui les hébergent.

Une fois que vous avez créé le point de terminaison Amazon VPC, vous pouvez commencer à l'utiliser sans modifier le code ou la configuration de votre application.

Pour créer un point de terminaison Amazon VPC pour l'API de données

1. Connectez-vous au Console de gestion AWS et ouvrez la console Amazon VPC à https://console.aws.amazon.com/vpc/ l'adresse.
2. Choisissez Points de terminaison, puis Créer un point de terminaison.

3. Sur la page Créer un point de terminaison, pour Catégorie de services, choisissez Services AWS . Pour Service Name (Nom de service), choisissez redshift-data(`com.amazonaws.region.redshift-data`).
4. Pour VPC, choisissez le VPC dans lequel créer le point de terminaison.

   Choisissez le VPC contenant l'application qui effectue des appels de l'API de données.
5. Pour les sous-réseaux, choisissez le sous-réseau pour chaque zone de disponibilité (AZ) utilisée par le AWS service qui exécute votre application.

   Pour créer un point de terminaison Amazon VPC, spécifiez la plage d'adresses IP privées dans laquelle le point de terminaison est accessible. Pour ce faire, choisissez le sous-réseau de chaque zone de disponibilité. Cela limite le point de terminaison de VPC à la plage d'adresses IP privées spécifique à chaque zone de disponibilité et crée également un point de terminaison Amazon VPC dans chaque zone de disponibilité.
6. Pour Enable DNS Name (Activer le nom DNS), sélectionnez Activer pour ce point de terminaison.

   Private DNS résout le nom d'hôte DNS standard de l'API de données (`https://redshift-data.region.amazonaws.com`) par les adresses IP privées associées au nom d'hôte DNS spécifique à votre point de terminaison Amazon VPC. Par conséquent, vous pouvez accéder au point de terminaison Data API VPC à l'aide des AWS kits SDK AWS CLI ou des kits SDK sans apporter de modifications de code ou de configuration pour mettre à jour l'URL du point de terminaison Data API.
7. Pour Groupe de sécurité, choisissez un groupe de sécurité à associer au point de terminaison Amazon VPC.

   Choisissez le groupe de sécurité qui autorise l'accès au AWS service qui exécute votre application. Par exemple, si une instance Amazon EC2 exécute votre application, choisissez le groupe de sécurité qui autorise l'accès à cette instance Amazon EC2. Le groupe de sécurité vous permet de contrôler le trafic vers le point de terminaison Amazon VPC à partir des ressources de votre VPC.
8. Choisissez Créer un point de terminaison.

Une fois le point de terminaison créé, cliquez sur le lien dans le Console de gestion AWS pour afficher les détails du point de terminaison.

L'onglet Détails du point de terminaison affiche les noms d'hôte DNS générés lors de la création du point de terminaison Amazon VPC.

Vous pouvez utiliser le point de terminaison standard (`redshift-data.region.amazonaws.com`) ou l'un des VPC-specific points de terminaison pour appeler l'API Data au sein d'Amazon VPC. Le point de terminaison standard de l'API de données effectue automatiquement un routage vers le point de terminaison Amazon VPC. Ce routage se produit car le nom d'hôte DNS privé a été activé lors de la création du point de terminaison Amazon VPC.

Lorsque vous utilisez un point de terminaison Amazon VPC dans un appel de l'API de données, tout le trafic entre votre application et l'API de données reste dans les Amazon VPC qui les contiennent. Vous pouvez utiliser un point de terminaison Amazon VPC pour n'importe quel type d'appel à l'API de données. Pour plus d'informations sur l'appel de l'API de données, consultez Considérations relatives à l'appel à l'API de données Amazon Redshift.

Rejoindre des groupes de base de données lors de la connexion à un cluster

Les groupes de base de données sont des ensembles d'utilisateurs de base de données. Des privilèges de base de données peuvent être accordés aux groupes. Un administrateur peut configurer un rôle IAM de telle sorte que ces groupes de base de données soient pris en compte lorsque votre requête SQL s'exécute avec l'API de données. Pour en savoir plus sur les groupes de base de données, consultez Groupes dans le Guide du développeur de base de données Amazon Redshift.

Vous pouvez configurer le rôle IAM d'un appelant de l'API de données de sorte que l'utilisateur de base de données spécifié dans l'appel rejoigne des groupes de base de données au moment où l'API de données se connecte à un cluster. Cette fonctionnalité n'est prise en charge que lors de la connexion à des clusters provisionnés. Elle n'est pas pris en charge lors de la connexion à des groupes de travail Redshift sans serveur. Le rôle IAM de l'appelant de l'API de données doit également autoriser l'action `redshift:JoinGroup`.

Pour configurer cela, vous devez ajouter des balises aux rôles IAM. L'administrateur du rôle IAM de l'appelant ajoute des balises avec la clé `RedshiftDbGroups` et une clé-valeur d'une liste de groupes de base de données. La valeur est une liste de noms de groupes de base de données séparés par deux points (:) d'une longueur totale maximale de 256 caractères. Les groupes de base de données doivent être préalablement définis dans la base de données connectée. Si aucun groupe spécifié n'est trouvé dans la base de données, elle est ignorée. Par exemple, pour les groupes de base de données `accounting` et `retail`, la clé-valeur est `accounting:retail`. La paire clé-valeur de balise `{"Key":"RedshiftDbGroups","Value":"accounting:retail"}` est utilisée

par l’API de données pour identifier les groupes de base de données qui sont associés à l’utilisateur de base de données indiqué dans l’appel à l’API de données.

Pour rejoindre des groupes de base de données

1. Connectez-vous au Console de gestion AWS et ouvrez la console IAM à https://console.aws.amazon.com/iam/ l'adresse.
2. Dans le panneau de navigation de la console, choisissez Roles (Rôles), puis choisissez le nom du rôle que vous souhaitez modifier.
3. Choisissez l’onglet Balises, puis Gérer les balises.
4. Choisissez Ajouter une balise, puis ajoutez la clé RedshiftDbGroups et une valeur qui est une liste de*database-groups-colon-separated*.
5. Sélectionnez Enregistrer les modifications.

   Désormais, lorsqu’un principal IAM (auquel ce rôle IAM est attaché) appelle l’API de données, l’utilisateur de base de données spécifié rejoint les groupes de base de données spécifiés dans le rôle IAM.

Pour plus d’informations sur la procédure d’attachement d’une balise à un principal, y compris les rôles IAM et les utilisateurs IAM, consultez Étiquetage des ressources IAM dans le Guide de l’utilisateur IAM.

Utilisation de l’API de données avec la propagation d’identité de confiance

En tant qu'administrateur de compte Amazon Redshift, vous pouvez intégrer votre cluster ou groupe de travail Amazon Redshift à AWS IAM Identity Center, ce qui permet de gérer l'accès de votre personnel à Amazon Redshift grâce à l'authentification unique. Pour de plus amples informations, veuillez consulter Configuration AWS Intégration d'IAM Identity Center à Amazon Redshift. L'API Amazon Redshift Data permet de propager les identités des utilisateurs d'IAM Identity Center vers un cluster ou un groupe de travail Amazon Redshift et vers d'autres services, tels que, AWS Lake Formation en aval de la chaîne. Vous pouvez configurer et effectuer des requêtes à l'aide de l'API Data en suivant les étapes décrites dans Access AWS services par programmation à l'aide d'une propagation d'identité sécurisée.

Lorsque vous appelez l’API de données à l’aide d’une identité d’utilisateur IAM Identity Center à partir d’une session de rôle IAM à identité améliorée, vous ne pouvez accéder à l’instruction et au résultat de l’instruction qui en résultent qu’en utilisant le même utilisateur IAM Identity Center. Par

exemple, la AWS CLI commande suivante appelle l'`execute-statement`opération pour exécuter une commande SQL avec une propagation d'identité sécurisée.

```
aws redshift-data execute-statement
--sql "select current_user;"
--cluster-id mycluster
--database dev
```

La AWS CLI commande suivante appelle l'`batch-execute-statement`opération pour exécuter deux commandes SQL.

```
aws redshift-data batch-execute-statement
--sqls  "select current_user;"  "select current_date;"
--cluster-id mycluster
--database dev
```

Pour accéder aux instructions avec `cancel-statement`, `describe-statement`, `get-statement-result` et `get-statement-result-v2` soumises par le biais de sessions de rôle IAM à identité améliorée, l'utilisateur IAM Identity Center et le rôle IAM doivent correspondre aux informations d'identification utilisées pour exécuter `execute-statement` ou `batch-execute-statement`. Par exemple, la AWS CLI commande suivante permet d'obtenir les résultats d'une instruction SQL.

```
aws redshift-data get-statement-result
--id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Pour répertorier les instructions, un paramètre `cluster-identifier` ou `workgroup-name` doit être fourni pour garantir que l'utilisateur de l'IAM Identity Center n'a accès qu'aux applications Amazon Redshift IAM Identity Center auxquelles il est affecté. Par exemple, la AWS CLI commande suivante répertorie les instructions relatives à un cluster spécifique.

```
aws redshift-data list-statements
--cluster-identifier mycluster
```

Vous pouvez également appeler les opérations de l'API de données qui accèdent aux objets de base de données d'un cluster ou d'un groupe de travail à l'aide d'une propagation d'identité fiable. Cela inclut les opérations `list-databases`, `list-schemas`, `list-tables` et `describe-table`.

Les appels d'API effectués par l'utilisateur de l'IAM Identity Center peuvent être suivis dans AWS CloudTrail. Une `onBehalfOf` section de l' CloudTrail événement présente l'identifiant utilisateur IAM Identity Center et l'ARN de la banque d'identités. L'exemple suivant montre un extrait d'un CloudTrail événement montrant la `onBehalfOf` section avec l'ID utilisateur IAM Identity Center de `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111` et l'ARN d'Identity Store de. `arn:aws:identitystore::123456789012:identitystore/d-9067bc44d2`

```
{
            "eventVersion":"1.10",
            "userIdentity":{
            "type":"AssumedRole",
            ...
            },
            "onBehalfOf":{
            "userId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "identityStoreArn":"arn:aws:identitystore::123456789012:identitystore/
d-9067bc44d2"
            }
            },
            "eventTime":"2025-01-13T04:46:27Z",
            "eventSource":"redshift-data.amazonaws.com",
            "eventName":"ExecuteStatement",
            "awsRegion":"us-east-1"
            }
```

Vous pouvez exécuter la commande SQL suivante pour vérifier la requête soumise par l'utilisateur IAM Identity Center. Dans cet exemple, l'e-mail enregistré dans Identity Center est `username@example.com`.

```
SELECT
    h.query_id,
    h.database_name,
    h.status,
    h.query_text,
    u.usename,
    h.start_time,
    h.end_time
FROM
    sys_query_history h
LEFT JOIN
    pg_user u
ON
```

```
    h.user_id = u.usesysid
where u.usename='awsidc:username@example.com'
ORDER BY
    h.start_time DESC;
```

Appel à l'API de données

Vous pouvez appeler l'API Data ou AWS CLI exécuter des instructions SQL sur votre cluster ou groupe de travail sans serveur. Les principales opérations pour exécuter des instructions SQL sont `ExecuteStatement` et `BatchExecuteStatement` dans la Référence de l'API de données Amazon Redshift. L'API Data prend en charge les langages de programmation pris en charge par le AWS SDK. Pour plus d'informations sur ces derniers, consultez Outils pour créer sur AWS.

Pour voir des exemples de code d'appel de l'API Data, consultez la section Démarrage avec l'API Redshift Data dans GitHub. Ce référentiel contient des exemples d'utilisation AWS Lambda pour accéder aux données Amazon Redshift depuis Amazon EC2 et Amazon AWS Glue Data Catalog SageMaker Runtime. Les langages de programmation incluent Python, Go, Java et Javascript.

Vous pouvez appeler l'API de données avec la AWS CLI.

Les exemples suivants utilisent le AWS CLI pour appeler l'API Data. Pour exécuter les exemples, modifiez les valeurs des paramètres de manière à les adapter à votre environnement. Dans de nombreux exemples, un `cluster-identifier` est fourni pour être exécutée sur un cluster. Lorsque vous exécutez une opération sur un groupe de travail sans serveur, vous fournissez un `workgroup-name` à la place. Ces exemples illustrent quelques-unes des opérations de l'API de données. Pour plus d'informations, consultez la référence des commandes de l'AWS CLI .

Les commandes des exemples suivants ont été scindées et formatées pour être plus lisibles. Tous les paramètres et réponses ne sont pas présentés dans tous les exemples. Pour la définition API de la syntaxe complète de la demande, des paramètres de demande, de la syntaxe de réponse et des éléments de réponse, consultez la Référence de l'API de données Amazon Redshift.

Transmission d'instructions SQL à un entrepôt de données Amazon Redshift

Les exemples présentés dans cette page présentent différentes manières de transmettre une instruction SQL à votre entrepôt de données.

Exécuter une instruction SQL

Pour exécuter une instruction SQL, utilisez la `aws redshift-data execute-statement` AWS CLI commande.

Vous pouvez éventuellement utiliser le `WaitTimeSeconds` paramètre pour laisser plus de temps à l'instruction pour se terminer avant que l'API ne renvoie une réponse. Lorsque l'instruction est terminée, la réponse inclut également `StatusRedshiftPid`, et`HasResultSet`. Pour de plus amples informations, veuillez consulter Réduisez les appels d'API grâce à de longues interrogations.

La AWS CLI commande suivante exécute une instruction SQL sur un cluster et renvoie un identifiant pour récupérer les résultats. Cet exemple utilise la méthode d'authentification AWS Secrets Manager .

```
aws redshift-data execute-statement
    --secret-arn arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-
hKgPWn
    --cluster-identifier mycluster-test
    --sql "select * from stl_query limit 1"
    --database dev
```

Voici un exemple de réponse.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598323175.823,
    "Database": "dev",
    "Id": "c016234e-5c6c-4bc5-bb16-2c5b8ff61814",
    "SecretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-
hKgPWn"
}
```

La AWS CLI commande suivante exécute une instruction SQL sur un cluster et renvoie un identifiant pour récupérer les résultats. Cet exemple utilise la méthode d'authentification par informations d'identification temporaires.

```
aws redshift-data execute-statement
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
    --sql "select * from stl_query limit 1"
```

Voici un exemple de réponse.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598306924.632,
    "Database": "dev",
    "DbUser": "myuser",
    "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

La AWS CLI commande suivante exécute une instruction SQL sur un groupe de travail sans serveur et renvoie un identifiant pour récupérer les résultats. Cet exemple utilise la méthode d'authentification par informations d'identification temporaires.

```
aws redshift-data execute-statement
    --database dev
    --workgroup-name myworkgroup
    --sql "select 1;"
```

Voici un exemple de réponse.

```
{
 "CreatedAt": "2022-02-11T06:25:28.748000+00:00",
 "Database": "dev",
 "DbUser": "IAMR:RoleName",
 "Id": "89dd91f5-2d43-43d3-8461-f33aa093c41e",
 "WorkgroupName": "myworkgroup"
}
```

La AWS CLI commande suivante exécute une instruction SQL sur un cluster et renvoie un identifiant pour récupérer les résultats. Cet exemple utilise la méthode d'authentification AWS Secrets Manager et un jeton d'idempotence.

```
aws redshift-data execute-statement
    --secret-arn arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-
hKgPWn
    --cluster-identifier mycluster-test
    --sql "select * from stl_query limit 1"
    --database dev
    --client-token b855dced-259b-444c-bc7b-d3e8e33f94g1
```

Voici un exemple de réponse.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598323175.823,
    "Database": "dev",
    "Id": "c016234e-5c6c-4bc5-bb16-2c5b8ff61814",
    "SecretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-
hKgPWn"
}
```

Exécuter plusieurs instructions SQL

Pour exécuter plusieurs instructions SQL avec une seule commande, utilisez la `aws redshift-data batch-execute-statement` AWS CLI commande.

Vous pouvez éventuellement utiliser le `WaitTimeSeconds` paramètre pour laisser plus de temps à l'ensemble du lot pour se terminer avant que l'API ne renvoie une réponse. Pour de plus amples informations, veuillez consulter Réduisez les appels d'API grâce à de longues interrogations.

La AWS CLI commande suivante exécute trois instructions SQL sur un cluster et renvoie un identifiant pour récupérer les résultats. Cet exemple utilise la méthode d'authentification par informations d'identification temporaires.

```
aws redshift-data batch-execute-statement
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
    --sqls "set timezone to BST" "select * from mytable" "select * from another_table"
```

Voici un exemple de réponse.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598306924.632,
    "Database": "dev",
    "DbUser": "myuser",
    "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

La AWS CLI commande suivante exécute trois instructions SQL dans des transactions distinctes en mode `AUTO_COMMIT` d'exécution. Chaque instruction est validée indépendamment : l'échec d'une instruction n'empêche pas l'exécution des autres instructions et n'affecte pas les instructions déjà terminées.

```
aws redshift-data batch-execute-statement
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
    --sqls "insert into mytable values (1)" "invalid sql statement" "insert into
 mytable values (3)"
    --execution-mode AUTO_COMMIT
```

Voici un exemple de réponse.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1623979777.126,
    "Duration": 6591877,
    "HasResultSet": false,
    "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652",
    "RedshiftPid": 31459,
    "RedshiftQueryId": 0,
    "Status": "FAILED",
    "SubStatements": [
        {
            "CreatedAt": 1623979777.274,
            "Duration": 3396637,
            "HasResultSet": false,
            "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:1",
            "QueryString": "insert into mytable values (1)",
            "RedshiftQueryId": -1,
            "Status": "FINISHED",
            "UpdatedAt": 1623979777.903
        },
        {
            "CreatedAt": 1623979777.274,
            "Duration": 1195240,
            "HasResultSet": false,
            "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2",
            "QueryString": "invalid sql statement",
```

```
            "RedshiftQueryId": -1,
            "Error": "ERROR: syntax error at or near \"invalid\"",
            "Status": "FAILED",
            "UpdatedAt": 1623979777.503
        },
        {
            "CreatedAt": 1623979777.274,
            "Duration": 1095981,
            "HasResultSet": false,
            "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:3",
            "QueryString": "insert into mytable values (3)",
            "RedshiftQueryId": -1,
            "Status": "FINISHED",
            "UpdatedAt": 1623979777.903
        }
    ],
    "UpdatedAt": 1623979778.183
}
```

Exécuter des instructions avec des paramètres

Vous pouvez utiliser des paramètres nommés à la fois avec les `batch-execute-statement` opérations `execute-statement` et. Lors de l'utilisation`batch-execute-statement`, les paramètres sont partagés entre toutes les instructions SQL du lot. Chaque instruction SQL peut faire référence à un sous-ensemble des paramètres fournis, mais chaque paramètre doit être utilisé par au moins une instruction SQL.

La AWS CLI commande suivante exécute une instruction SQL sur un cluster et renvoie un identifiant pour récupérer les résultats. Cet exemple utilise la méthode d'authentification AWS Secrets Manager . Le texte SQL a un paramètre nommé `distance`. Dans ce cas, la distance utilisée dans le prédicat est `5`. Dans une instruction SELECT, les paramètres nommés pour les noms de colonnes ne peuvent être utilisés que dans le prédicat. Les valeurs des paramètres nommés pour l'instruction SQL sont spécifiées dans l'option `parameters`.

```
aws redshift-data execute-statement
    --secret-arn arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-
hKgPWn
    --cluster-identifier mycluster-test
    --sql "SELECT ratecode FROM demo_table WHERE trip_distance > :distance"
    --parameters "[{\"name\": \"distance\", \"value\": \"5\"}]"
```

```
    --database dev
```

Voici un exemple de réponse.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598323175.823,
    "Database": "dev",
    "Id": "c016234e-5c6c-4bc5-bb16-2c5b8ff61814",
    "SecretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-
hKgPWn"
}
```

L'exemple de requête suivant utilise la table EVENT de l'exemple de base de données. Pour plus d'informations, consultez Table EVENT dans le Manuel du développeur de bases de données Amazon Redshift.

Si la table EVENT n'existe pas encore dans votre base de données, vous pouvez en créer une à l'aide de l'API de données comme suit :

```
aws redshift-data execute-statement
--database dev
--cluster-id mycluster-test
--db-user awsuser
--sql "create table event( eventid integer not null distkey,
                           venueid smallint not null,
                           catid smallint not null,
                           dateid smallint not null sortkey,
                           eventname varchar(200),
                           starttime timestamp)"
```

L'instruction suivante insère une ligne dans la table EVENT.

```
aws redshift-data execute-statement
--database dev
--cluster-id mycluster-test
--db-user awsuser
--sql "insert into event
 values(:eventid, :venueid::smallint, :catid, :dateid, :eventname, :starttime)"
```

```
--parameters "[{\"name\": \"eventid\", \"value\": \"1\"}, {\"name\": \"venueid\",
 \"value\": \"1\"},
              {\"name\": \"catid\", \"value\": \"1\"},
              {\"name\": \"dateid\", \"value\": \"1\"},
              {\"name\": \"eventname\", \"value\": \"event 1\"},
              {\"name\": \"starttime\", \"value\": \"2022-02-22\"}]"
```

L'instruction suivante insère une deuxième ligne dans la table EVENT. Cet exemple illustre ce scénario :

- Le paramètre nommé `id` est utilisé quatre fois dans le texte SQL.
- La conversion de type implicite est appliquée automatiquement lors de l'insertion d'un paramètre `starttime`.
- La colonne `venueid` est convertie en type de données SMALLINT.
- Les chaînes de caractères qui représentent le type de données DATE sont implicitement converties en type de données TIMESTAMP.
- Les commentaires peuvent être utilisés dans le texte SQL.

```
aws redshift-data execute-statement
--database dev
--cluster-id mycluster-test
--db-user awsuser
--sql "insert into event values(:id, :id::smallint, :id, :id, :eventname, :starttime) /
*this is comment, and it won't apply parameterization for :id, :eventname or :starttime
 here*/"
--parameters "[{\"name\": \"eventname\", \"value\": \"event 2\"},
              {\"name\": \"starttime\", \"value\": \"2022-02-22\"},
              {\"name\": \"id\", \"value\": \"2\"}]"
```

Voici les deux lignes insérées :

```
 eventid | venueid | catid | dateid | eventname |      starttime
---------+---------+-------+--------+-----------+---------------------
       1 |       1 |     1 |      1 | event 1   | 2022-02-22 00:00:00
       2 |       2 |     2 |      2 | event 2   | 2022-02-22 00:00:00
```

La commande suivante utilise un paramètre nommé dans une clause WHERE pour récupérer la ligne où `eventid` est 1.

```
aws redshift-data execute-statement
--database dev
--cluster-id mycluster-test
--db-user awsuser
--sql "select * from event where eventid=:id"
--parameters "[{\"name\": \"id\", \"value\": \"1\"}]"
```

Exécutez l'instruction suivante pour obtenir les résultats SQL de l'instruction SQL précédente :

```
aws redshift-data get-statement-result --id 7529ad05-b905-4d71-9ec6-8b333836eb5a
```

Fournit les résultats suivants :

```
{
    "Records": [
        [
            {
                "longValue": 1
            },
            {
                "longValue": 1
            },
            {
                "longValue": 1
            },
            {
                "longValue": 1
            },
            {
                "stringValue": "event 1"
            },
            {
                "stringValue": "2022-02-22 00:00:00.0"
```

```
            }
        ]
    ],
    "ColumnMetadata": [
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "eventid",
            "length": 0,
            "name": "eventid",
            "nullable": 0,
            "precision": 10,
            "scale": 0,
            "schemaName": "public",
            "tableName": "event",
            "typeName": "int4"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "venueid",
            "length": 0,
            "name": "venueid",
            "nullable": 0,
            "precision": 5,
            "scale": 0,
            "schemaName": "public",
            "tableName": "event",
            "typeName": "int2"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "catid",
            "length": 0,
            "name": "catid",
            "nullable": 0,
            "precision": 5,
            "scale": 0,
            "schemaName": "public",
            "tableName": "event",
```

```
            "typeName": "int2"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "dateid",
            "length": 0,
            "name": "dateid",
            "nullable": 0,
            "precision": 5,
            "scale": 0,
            "schemaName": "public",
            "tableName": "event",
            "typeName": "int2"
        },
        {
            "isCaseSensitive": true,
            "isCurrency": false,
            "isSigned": false,
            "label": "eventname",
            "length": 0,
            "name": "eventname",
            "nullable": 1,
            "precision": 200,
            "scale": 0,
            "schemaName": "public",
            "tableName": "event",
            "typeName": "varchar"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "label": "starttime",
            "length": 0,
            "name": "starttime",
            "nullable": 1,
            "precision": 29,
            "scale": 6,
            "schemaName": "public",
            "tableName": "event",
            "typeName": "timestamp"
        }
```

```
    ],
    "TotalNumRows": 1
}
```

La AWS CLI commande suivante exécute deux instructions SQL avec des paramètres nommés partagés sur un cluster utilisant`batch-execute-statement`. Le texte SQL a les paramètres nommés `id` et `name`. La première instruction SQL utilise le `id` paramètre et la seconde utilise le `name` paramètre.

```
aws redshift-data batch-execute-statement
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
    --sqls "SELECT * FROM mytable WHERE id = :id" "SELECT * FROM mytable WHERE name
 = :name"
    --parameters "[{\"name\": \"id\", \"value\": \"1\"},{\"name\": \"name\", \"value\":
 \"Alice\"}]"
```

Voici un exemple de réponse.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598306924.632,
    "Database": "dev",
    "DbUser": "myuser",
    "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

La AWS CLI commande suivante exécute deux instructions SQL dans lesquelles le même paramètre est utilisé dans les deux instructions. Le paramètre nommé `id` est utilisé dans une instruction INSERT et une instruction SELECT.

```
aws redshift-data batch-execute-statement
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
    --sqls "INSERT INTO mytable VALUES(:id, :name, :address)" "SELECT * FROM mytable
 WHERE id = :id"
```

```
    --parameters "[{\"name\": \"id\", \"value\": \"1\"},{\"name\": \"name\", \"value\":
 \"Alice\"},{\"name\": \"address\", \"value\": \"Seattle\"}]"
```

Voici un exemple de réponse.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598306924.632,
    "Database": "dev",
    "DbUser": "myuser",
    "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

Répertorier les métadonnées sur les instructions SQL

Pour répertorier les métadonnées relatives aux instructions SQL, utilisez la `aws redshift-data list-statements` AWS CLI commande. L'autorisation d'exécuter cette commande est basée sur les autorisations IAM de l'appelant.

La AWS CLI commande suivante répertorie les instructions SQL exécutées.

```
aws redshift-data list-statements
    --status ALL
```

Voici un exemple de réponse.

```
{
    "Statements": [
        {
            "CreatedAt": 1598306924.632,
            "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766",
            "QueryString": "select * from stl_query limit 1",
            "Status": "FINISHED",
            "UpdatedAt": 1598306926.667
        },
        {
            "CreatedAt": 1598311717.437,
            "Id": "e0ebd578-58b3-46cc-8e52-8163fd7e01aa",
            "QueryString": "select * from stl_query limit 1",
            "Status": "FAILED",
```

```
            "UpdatedAt": 1598311719.008
        },
        {
            "CreatedAt": 1598313683.65,
            "Id": "c361d4f7-8c53-4343-8c45-6b2b1166330c",
            "QueryString": "select * from stl_query limit 1",
            "Status": "ABORTED",
            "UpdatedAt": 1598313685.495
        },
        {
            "CreatedAt": 1598306653.333,
            "Id": "a512b7bd-98c7-45d5-985b-a715f3cfde7f",
            "QueryString": "select 1",
            "Status": "FINISHED",
            "UpdatedAt": 1598306653.992
        }
    ]
}
```

Liste des sessions

Pour répertorier les sessions que vous avez créées au cours des dernières 24 heures, utilisez la `aws redshift-data list-sessions` AWS CLI commande. Par défaut, la commande renvoie uniquement les sessions dont le statut est `AVAILABLE` ou`BUSY`. Vous pouvez filtrer les résultats par état de session, cible de calcul (cluster ou groupe de travail sans serveur) ou base de données. Vos autorisations IAM déterminent si vous pouvez exécuter cette commande. Pour en savoir plus sur les sessions, consultez Exécution d'instructions SQL avec réutilisation de session lors de l'appel à l'API de données Amazon Redshift.

La AWS CLI commande suivante répertorie les sessions exécutées sur un cluster :

```
aws redshift-data list-sessions
   --cluster-identifier mycluster-test
```

Voici un exemple de réponse :

```
{
    "Sessions": [
        {
            "SessionId": "5a254dc6-4fc2-4203-87a8-551155432ee4",
```

```
            "Status": "AVAILABLE",
            "CreatedAt": 1703022996.436,
            "UpdatedAt": 1703023010.221,
            "Database": "dev",
            "DbUser": "awsuser",
            "ClusterIdentifier": "mycluster-test",
            "SessionAliveSeconds": 10,
            "SessionTtl": 1703023020.436
        },
        {
            "SessionId": "8b365ed7-5gd7-5314-98b9-662266543ff5",
            "Status": "BUSY",
            "CreatedAt": 1703023100.512,
            "UpdatedAt": 1703023150.874,
            "Database": "dev",
            "DbUser": "awsuser",
            "ClusterIdentifier": "mycluster-test",
            "SessionAliveSeconds": 60,
            "SessionTtl": 1703023210.512,
            "CurrentStatementId": "c016234e-5c6c-4bc5-bb16-2c5b8ff61814"
        }
    ]
}
```

La AWS CLI commande suivante répertorie les `CLOSED` sessions d'un groupe de travail sans serveur en filtrant en fonction de l'état de la session :

```
aws redshift-data list-sessions
    --workgroup-name myworkgroup
    --status CLOSED
```

Voici un exemple de réponse :

```
{
    "Sessions": [
        {
            "SessionId": "07c5ffea-76d6-4786-b62c-4fe3ef529680",
            "Status": "CLOSED",
            "CreatedAt": 1703019996.436,
            "UpdatedAt": 1703020056.436,
            "Database": "dev",
            "DbUser": "IAMR:RoleName",
```

```
            "WorkgroupName": "myworkgroup",
            "SessionAliveSeconds": 60,
            "SessionTtl": 1703020056.436
        }
    ]
}
```

> **Note**
>
> Si vous utilisez des sessions de rôles IAM à identité améliorée, vous devez fournir le `cluster-identifier` paramètre ou. `workgroup-name` Avec ce paramètre, vous vous assurez que l' AWS IAM Identity Center utilisateur peut accéder uniquement aux applications Amazon Redshift IAM Identity Center auxquelles il est affecté. Pour de plus amples informations, veuillez consulter Utilisation de l'API de données avec la propagation d'identité de confiance.

Décrire des métadonnées à propos d'une instruction SQL

Pour obtenir la description des métadonnées d'une instruction SQL, utilisez la `aws redshift-data describe-statement` AWS CLI commande. Vous pouvez également utiliser cette commande pour décrire des sous-instructions individuelles au sein d'un lot en fournissant l'ID de sous-déclaration. L'autorisation d'exécuter cette commande est basée sur les autorisations IAM de l'appelant.

Facultativement, pour réduire le nombre de demandes de sondage, utilisez le `WaitTimeSeconds` paramètre pour donner plus de temps pour que l'état d'une opération soit mis à jour dans le cadre de cet appel d'API. Pour de plus amples informations, veuillez consulter Réduisez les appels d'API grâce à de longues interrogations.

La AWS CLI commande suivante décrit une instruction SQL.

```
aws redshift-data describe-statement
    --id d9b6c0c9-0747-4bf4-b142-e8883122f766
```

Voici un exemple de réponse.

```
{
    "ClusterIdentifier": "mycluster-test",
```

```
    "CreatedAt": 1598306924.632,
    "Duration": 1095981511,
    "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766",
    "QueryString": "select * from stl_query limit 1",
    "RedshiftPid": 20859,
    "RedshiftQueryId": 48879,
    "ResultRows": 1,
    "ResultSize": 4489,
    "Status": "FINISHED",
    "UpdatedAt": 1598306926.667
}
```

Voici un exemple de réponse de `describe-statement` après l'exécution d'une commande `batch-execute-statement` avec plusieurs instructions SQL.

```
{
    "ClusterIdentifier": "mayo",
    "CreatedAt": 1623979777.126,
    "Duration": 6591877,
    "HasResultSet": true,
    "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652",
    "RedshiftPid": 31459,
    "RedshiftQueryId": 0,
    "ResultRows": 2,
    "ResultSize": 22,
    "Status": "FINISHED",
    "SubStatements": [
        {
            "CreatedAt": 1623979777.274,
            "Duration": 3396637,
            "HasResultSet": true,
            "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:1",
            "QueryString": "select 1;",
            "RedshiftQueryId": -1,
            "ResultRows": 1,
            "ResultSize": 11,
            "Status": "FINISHED",
            "UpdatedAt": 1623979777.903
        },
        {
            "CreatedAt": 1623979777.274,
            "Duration": 3195240,
            "HasResultSet": true,
```

```
            "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2",
            "QueryString": "select 2;",
            "RedshiftQueryId": -1,
            "ResultRows": 1,
            "ResultSize": 11,
            "Status": "FINISHED",
            "UpdatedAt": 1623979778.076
        }
    ],
    "UpdatedAt": 1623979778.183
}
```

La AWS CLI commande suivante décrit une sous-instruction spécifique au sein d'un lot en fournissant l'ID de la sous-instruction.

```
aws redshift-data describe-statement
    --id b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2
```

Voici un exemple de réponse. L'état de la déclaration parent est `STARTED` dû au fait que le lot n'est pas encore terminé. Le `SubStatements` tableau contient uniquement la sous-instruction demandée.

```
{
    "ClusterIdentifier": "mayo",
    "CreatedAt": 1623979777.126,
    "Duration": 0,
    "HasResultSet": false,
    "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652",
    "RedshiftPid": 31459,
    "RedshiftQueryId": 0,
    "Status": "STARTED",
    "SubStatements": [
        {
            "CreatedAt": 1623979777.274,
            "Duration": 3195240,
            "HasResultSet": true,
            "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2",
            "QueryString": "select 2;",
            "RedshiftQueryId": -1,
            "ResultRows": 1,
            "ResultSize": 11,
            "Status": "FINISHED",
```

```
            "UpdatedAt": 1623979778.076
        }
    ],
    "UpdatedAt": 1623979777.503
}
```

Récupérer les résultats d'une instruction SQL

Pour récupérer le résultat d'une instruction SQL exécutée, utilisez la `redshift-data get-statement-result-v2` AWS CLI commande `redshift-data get-statement-result` or. Les résultats de `get-statement-result` sont au format JSON. Les résultats de `get-statement-result-v2` sont au format CSV. Vous pouvez spécifier un `Id` que vous recevez en réponse à `execute-statement` ou `batch-execute-statement`. La valeur `Id` d'une instruction SQL exécutée par `batch-execute-statement` peut être récupéré dans le résultat de `describe-statement` et son suffixe est composé de deux points suivis d'un numéro de séquence tel que `b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2`. Si vous exécutez plusieurs instructions SQL avec `batch-execute-statement`, chaque instruction SQL a une valeur `Id` comme indiqué dans `describe-statement`. L'autorisation d'exécuter cette commande est basée sur les autorisations IAM de l'appelant.

Facultativement, pour réduire le nombre de demandes de sondage, utilisez le `WaitTimeSeconds` paramètre afin de laisser plus de temps à l'instruction pour se terminer avant que l'API ne renvoie un résultat de déclaration. Pour de plus amples informations, veuillez consulter Réduisez les appels d'API grâce à de longues interrogations.

L'instruction suivante renvoie le résultat d'une instruction SQL exécutée par `execute-statement` laissant le `ResultFormat` par défaut sur `JSON`. Pour récupérer les résultats, appelez l'opération `get-statement-result`.

```
aws redshift-data get-statement-result
    --id d9b6c0c9-0747-4bf4-b142-e8883122f766
```

L'instruction suivante renvoie le résultat de la deuxième instruction SQL exécutée par `batch-execute-statement`.

```
aws redshift-data get-statement-result
    --id b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2
```

Voici un exemple de réponse à un appel de `get-statement-result` où le résultat SQL est renvoyé au format JSON dans la clé `Records` de la réponse.


```
{
    "ColumnMetadata": [
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "userid",
            "length": 0,
            "name": "userid",
            "nullable": 0,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "int4"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "query",
            "length": 0,
            "name": "query",
            "nullable": 0,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "int4"
        },
        {
            "isCaseSensitive": true,
            "isCurrency": false,
            "isSigned": false,
            "label": "label",
            "length": 0,
            "name": "label",
            "nullable": 0,
            "precision": 320,
            "scale": 0,
```

```
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "bpchar"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "xid",
            "length": 0,
            "name": "xid",
            "nullable": 0,
            "precision": 19,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "int8"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "pid",
            "length": 0,
            "name": "pid",
            "nullable": 0,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "int4"
        },
        {
            "isCaseSensitive": true,
            "isCurrency": false,
            "isSigned": false,
            "label": "database",
            "length": 0,
            "name": "database",
            "nullable": 0,
            "precision": 32,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
```

```
            "typeName": "bpchar"
        },
        {
            "isCaseSensitive": true,
            "isCurrency": false,
            "isSigned": false,
            "label": "querytxt",
            "length": 0,
            "name": "querytxt",
            "nullable": 0,
            "precision": 4000,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "bpchar"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "label": "starttime",
            "length": 0,
            "name": "starttime",
            "nullable": 0,
            "precision": 29,
            "scale": 6,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "timestamp"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "label": "endtime",
            "length": 0,
            "name": "endtime",
            "nullable": 0,
            "precision": 29,
            "scale": 6,
            "schemaName": "",
            "tableName": "stll_query",
            "type": 93,
            "typeName": "timestamp"
```

```
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "aborted",
            "length": 0,
            "name": "aborted",
            "nullable": 0,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "int4"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "insert_pristine",
            "length": 0,
            "name": "insert_pristine",
            "nullable": 0,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "int4"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "concurrency_scaling_status",
            "length": 0,
            "name": "concurrency_scaling_status",
            "nullable": 0,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "int4"
        }
    ],
```

```
    "Records": [
        [
            {
                "longValue": 1
            },
            {
                "longValue": 3
            },
            {
                "stringValue": "health"
            },
            {
                "longValue": 1023
            },
            {
                "longValue": 15279
            },
            {
                "stringValue": "dev"
            },
            {
                "stringValue": "select system_status from stv_gui_status;"
            },
            {
                "stringValue": "2020-08-21 17:33:51.88712"
            },
            {
                "stringValue": "2020-08-21 17:33:52.974306"
            },
            {
                "longValue": 0
            },
            {
                "longValue": 0
            },
            {
                "longValue": 6
            }
        ]
    ],
    "TotalNumRows": 1
}
```

L'exemple suivant montre une instruction SQL exécutée par `execute-statement` pour renvoyer des résultats au format JSON. La table `testingtable` comporte trois colonnes entières (col1, col2, col3) et trois lignes contenant des valeurs (1, 2, 3), (4, 5, 6) et (7, 8, 9).

```
aws redshift-data execute-statement
    --database dev
    --sql "SELECT col1, col2, col3 FROM testingtable"
    --cluster-id mycluster-test
    --result-format JSON
```

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": "2024-04-02T16:45:25.144000+00:00",
    "Database": "dev",
    "DbUser": "IAMR:Administrator",
    "Id": "d468d942-6df9-4f85-8ae3-bac01a61aec3"
}
```

Voici un exemple de réponse à un appel de `get-statement-result` où le résultat SQL est renvoyé au format JSON dans la clé `Records` de la réponse.

```
aws redshift-data get-statement-result
    --id d468d942-6df9-4f85-8ae3-bac01a61aec3
```

```
{
    "Records": [
        [
            {
                "longValue": 1
            },
            {
                "longValue": 2
            },
            {
                "longValue": 3
            }
        ],
        [
            {
```

```
                "longValue": 4
            },
            {
                "longValue": 5
            },
            {
                "longValue": 6
            }
        ],
        [
            {
                "longValue": 7
            },
            {
                "longValue": 8
            },
            {
                "longValue": 9
            }
        ]
    ],
    "ColumnMetadata": [
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "col1",
            "name": "col1",
            "nullable": 1,
            "precision": 10,
            "scale": 0,
            "schemaName": "public",
            "tableName": "testingtable",
            "typeName": "int4",
            "length": 0
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "col2",
            "name": "col2",
            "nullable": 1,
            "precision": 10,
```

```
            "scale": 0,
            "schemaName": "public",
            "tableName": "testingtable",
            "typeName": "int4",
            "length": 0
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "col3",
            "name": "col3",
            "nullable": 1,
            "precision": 10,
            "scale": 0,
            "schemaName": "public",
            "tableName": "testingtable",
            "typeName": "int4",
            "length": 0
        }
    ],
    "TotalNumRows": 3
}
```

L'exemple suivant montre une instruction SQL exécutée par `execute-statement` pour renvoyer des résultats au format CSV. La table `testingtable` comporte trois colonnes entières (col1, col2, col3) et trois lignes contenant des valeurs (1, 2, 3), (4, 5, 6) et (7, 8, 9).

```
aws redshift-data execute-statement
    --database dev
    --sql "SELECT col1, col2, col3 FROM testingtable"
    --cluster-id mycluster-test
    --result-format CSV
```

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": "2024-04-02T16:45:25.144000+00:00",
    "Database": "dev",
    "DbUser": "IAMR:Administrator",
    "Id": "d468d942-6df9-4f85-8ae3-bac01a61aec3"
}
```

Voici un exemple de réponse à un appel de `get-statement-result-v2` où le résultat SQL est renvoyé au format CSV dans la clé `Records` de la réponse. Les lignes sont séparées par un retour du chariot et par une nouvelle ligne (\r\n). La première ligne renvoyée dans `Records` correspond aux en-têtes de colonne. Les résultats renvoyés au format CSV sont renvoyés dans un format de 1 Mo, chaque bloc pouvant stocker un nombre quelconque de lignes allant jusqu'à 1 Mo.

```
aws redshift-data get-statement-result-v2
    --id d468d942-6df9-4f85-8ae3-bac01a61aec3
```


```
{
    "Records": [
        {
            "CSVRecords": "col1,col2,col3\r\n1,2,3\r\n4,5,6\r\n7,8,9\r\n"
        }
    ],
    "ColumnMetadata": [
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "col1",
            "name": "col1",
            "nullable": 1,
            "precision": 10,
            "scale": 0,
            "schemaName": "public",
            "tableName": "testingtable",
            "typeName": "int4",
            "length": 0
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "col2",
            "name": "col2",
            "nullable": 1,
            "precision": 10,
            "scale": 0,
            "schemaName": "public",
            "tableName": "testingtable",
```

```
            "typeName": "int4",
            "length": 0
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "col3",
            "name": "col3",
            "nullable": 1,
            "precision": 10,
            "scale": 0,
            "schemaName": "public",
            "tableName": "testingtable",
            "typeName": "int4",
            "length": 0
        }
    ],
    "TotalNumRows": 3,
    "ResultFormat": "csv"
}
```

Réduisez les appels d'API grâce à de longues interrogations

Par défaut, les opérations de l'API Data renvoient une réponse immédiate. Si l'opération concerne une instruction en cours, vous devez effectuer plusieurs sondages jusqu'à ce que l'instruction atteigne un état terminal. En cas d'interrogation longue, définissez `WaitTimeSeconds` une valeur comprise entre 1 et 30. L'API retardera le renvoi d'une réponse synchrone jusqu'à ce que l'instruction se termine ou `WaitTimeSeconds` soit atteinte, selon la première éventualité.

Les sondages longs sont pris en charge sur DescribeStatement ExecuteStatement BatchExecuteStatement, GetStatementResult, et GetStatementResultV2.

Lorsqu'une opération a `WaitTimeSeconds` pour but de soumettre une nouvelle déclaration ou d'attendre une déclaration existante :

- Si l'instruction se termine dans le délai d'attente, la réponse inclut l'état du terminal ou les données de résultat, en fonction de l'opération.
- Si l'instruction est toujours en cours à l'expiration du temps d'attente, la réponse renvoie l'état en cours.

- Si la déclaration était déjà terminée avant que la demande de sondage longue ne soit faite, l'API renvoie immédiatement l'état du terminal.
- S'il `WaitTimeSeconds` n'est pas défini, le comportement asynchrone par défaut est conservé.

Cas d'utilisation courants

Voici des exemples de situations dans lesquelles un long sondage peut être utile :

- Soumettez une courte requête et attendez qu'elle soit terminée — À utiliser `ExecuteStatement` avec`WaitTimeSeconds`. Lorsque la requête se termine ou que le temps d'attente expire, la réponse renvoie l'instruction `StatusRedshiftPid`, et`HasResultSet`. Pour obtenir les métadonnées complètes du relevé, appelez`DescribeStatement`. Si `HasResultSet` c'est `true` le cas, appelez `GetStatementResult` pour récupérer les résultats.
- Sondage long pour connaître le statut : utilisez cette option `ExecuteStatement` pour soumettre la requête, puis appelez `DescribeStatement` avec`WaitTimeSeconds`. Lorsque la requête est terminée, `DescribeStatement` renvoie les métadonnées complètes de l'instruction, y compris le statut, la durée et les détails de l'erreur.
- Sondage long pour le résultat : utilisez `ExecuteStatement` cette option pour soumettre la requête, puis appelez `GetStatementResult` avec`WaitTimeSeconds`. Lorsque la requête est terminée, les données de résultat sont renvoyées directement. Si la requête est toujours en cours à l'expiration du temps d'attente, une valeur `ResourceNotFoundException` est renvoyée indiquant qu'aucun résultat n'est encore disponible.
- Soumettez plusieurs requêtes et attendez que l'ensemble du lot soit terminé — À utiliser `BatchExecuteStatement` avec`WaitTimeSeconds`. L'appel reste ouvert jusqu'à ce que toutes les sous-instructions soient terminées et renvoie l'ID du parent du lot et l'état général.
- Soumettez plusieurs requêtes et un statut de sondage long pour une sous-déclaration — Utilisez `DescribeStatement` ou `GetStatementResult` avec l'ID de sous-déclaration et. `WaitTimeSeconds` Renvoie dès que cette sous-instruction est terminée, sans attendre le reste du lot.

Décrire une table

Pour obtenir les métadonnées qui décrivent une table, utilisez la `aws redshift-data describe-table` AWS CLI commande.

La AWS CLI commande suivante exécute une instruction SQL sur un cluster et renvoie des métadonnées qui décrivent une table. Cet exemple utilise la méthode AWS Secrets Manager d'authentification.

```
aws redshift-data describe-table
    --cluster-identifier mycluster-test
    --database dev
    --schema information_schema
    --table sql_features
    --secret-arn arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-
hKgPWn
```

Voici un exemple de réponse.

```
{
    "ColumnList": [
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "feature_id",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "feature_name",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        }
```

```
    ]
}
```

La AWS CLI commande suivante exécute une instruction SQL sur un cluster qui décrit une table. Cet exemple utilise la méthode d'authentification par informations d'identification temporaires.

```
aws redshift-data describe-table
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
    --schema information_schema
    --table sql_features
```

Voici un exemple de réponse.

```
{
    "ColumnList": [
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "feature_id",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "feature_name",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
```

```
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "sub_feature_id",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "sub_feature_name",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "is_supported",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
```

```
            "length": 2147483647,
            "name": "is_verified_by",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "comments",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        }
    ]
}
```

Répertorier les bases de données dans un cluster

Pour répertorier les bases de données d'un cluster, utilisez la `aws redshift-data list-databases` AWS CLI commande.

La AWS CLI commande suivante exécute une instruction SQL sur un cluster pour répertorier les bases de données. Cet exemple utilise la méthode AWS Secrets Manager d'authentification.

```
aws redshift-data list-databases

    --secret-arn arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-
hKgPWn
    --cluster-identifier mycluster-test
    --database dev
```

Voici un exemple de réponse.

```
{
    "Databases": [
        "dev"
    ]
}
```

La AWS CLI commande suivante exécute une instruction SQL sur un cluster pour répertorier les bases de données. Cet exemple utilise la méthode d'authentification par informations d'identification temporaires.

```
aws redshift-data list-databases
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
```

Voici un exemple de réponse.

```
{
    "Databases": [
        "dev"
    ]
}
```

Répertorier les schémas dans une base de données

Pour répertorier les schémas d'une base de données, utilisez la `aws redshift-data list-schemas` AWS CLI commande.

La AWS CLI commande suivante exécute une instruction SQL sur un cluster pour répertorier les schémas d'une base de données. Cet exemple utilise la méthode AWS Secrets Manager d'authentification.

```
aws redshift-data list-schemas
    --secret-arn arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-
hKgPWn
    --cluster-identifier mycluster-test
    --database dev
```

Voici un exemple de réponse.

```
{
    "Schemas": [
        "information_schema",
        "pg_catalog",
        "pg_internal",
        "public"
    ]
}
```

La AWS CLI commande suivante exécute une instruction SQL sur un cluster pour répertorier les schémas d'une base de données. Cet exemple utilise la méthode d’authentification par informations d’identification temporaires.

```
aws redshift-data list-schemas
    --db-user mysuser
    --cluster-identifier mycluster-test
    --database dev
```

Voici un exemple de réponse.

```
{
    "Schemas": [
        "information_schema",
        "pg_catalog",
        "pg_internal",
        "public"
    ]
}
```

Répertorier les tables dans une base de données

Pour répertorier les tables d'une base de données, utilisez la `aws redshift-data list-tables` AWS CLI commande.

La AWS CLI commande suivante exécute une instruction SQL sur un cluster pour répertorier les tables d'une base de données. Cet exemple utilise la méthode AWS Secrets Manager d'authentification.

```
aws redshift-data list-tables
```

```
    --secret-arn arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-
hKgPWn
    --cluster-identifier mycluster-test
    --database dev
    --schema information_schema
```

Voici un exemple de réponse.

```
{
    "Tables": [
        {
            "name": "sql_features",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        },
        {
            "name": "sql_implementation_info",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        }
}
```

La AWS CLI commande suivante exécute une instruction SQL sur un cluster pour répertorier les tables d'une base de données. Cet exemple utilise la méthode d’authentification par informations d’identification temporaires.

```
aws redshift-data list-tables

     --db-user myuser
     --cluster-identifier mycluster-test
     --database dev
     --schema information_schema
```

Voici un exemple de réponse.

```
{
    "Tables": [
        {
            "name": "sql_features",
```

```
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        },
        {
            "name": "sql_implementation_info",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        }
    ]
}
```

Résolution des problèmes liés à l'API de données Amazon Redshift

Utilisez les sections suivantes, dont le titre correspond aux messages d'erreur courants, pour vous aider à résoudre les problèmes que vous rencontrez avec l'API de données.

Rubriques

- Packet for query is too large
- Database Response Exceeded Size Limit

Packet for query is too large

Si vous obtenez une erreur indiquant que le paquet pour une requête est trop grand, cela signifie généralement que l'ensemble de résultats renvoyé pour une ligne est trop grand. La taille de l'API de données ne doit pas dépasser 64 Ko par ligne dans le jeu de résultat renvoyé par la base de données.

Pour résoudre ce problème, assurez-vous que la taille de chaque ligne d'un jeu de résultat est inférieure ou égale à 64 Ko.

Database Response Exceeded Size Limit

Si vous obtenez une erreur indiquant que la réponse de la base de données a dépassé la limite de taille, cela signifie généralement que la taille de l'ensemble de résultats renvoyé par la base de données était trop importante. La limite de l'API Data est de 500 Mo dans le jeu de résultats renvoyé par la base de données.

Pour résoudre ce problème, assurez-vous que les appels à l'API Data renvoient 500 Mo de données ou moins. Si vous devez renvoyer plus de 500 Mo, vous pouvez exécuter plusieurs appels d'instructions avec la `LIMIT` clause dans votre requête.

Planification des opérations de l'API Amazon Redshift Data avec Amazon EventBridge

Vous pouvez créer des règles qui correspondent à des événements sélectionnés et les acheminent vers des cibles pour qu'elles prennent des mesures. Vous pouvez également utiliser des règles pour effectuer des actions sur une planification prédéterminée. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

Pour planifier les opérations de l'API Data avec EventBridge, le rôle IAM associé doit faire confiance au responsable des CloudWatch événements (events.amazonaws.com). Ce rôle doit être assorti de l'équivalent de la politique gérée `AmazonEventBridgeFullAccess`. Il doit également disposer des autorisations de la politique `AmazonRedshiftDataFullAccess` qui sont gérées par l'API de données. Vous pouvez créer un rôle IAM avec ces autorisations sur la console IAM. Lorsque vous créez un rôle sur la console IAM, choisissez l'entité de AWS service sécurisée pour les CloudWatch événements. Spécifiez le rôle IAM dans la valeur `RoleArn` JSON de la EventBridge cible. Pour plus d'informations sur la création d'un rôle IAM, consultez la section Création d'un rôle pour un AWS service (console) dans le Guide de l'utilisateur IAM.

La règle `name` de la règle que vous créez dans Amazon EventBridge doit correspondre `StatementName` à celle du`RedshiftDataParameters`.

Les exemples suivants montrent des variantes de création de EventBridge règles avec une ou plusieurs instructions SQL et avec un cluster Amazon Redshift ou un groupe de travail Amazon Redshift Serverless comme entrepôt de données.

Appel à l'aide d'une seule instruction SQL et d'un cluster

L'exemple suivant utilise le AWS CLI pour créer une EventBridge règle qui permet d'exécuter une instruction SQL sur un cluster Amazon Redshift.

```
aws events put-rule
--name test-redshift-cluster-data
--schedule-expression "rate(1 minute)"
```

Ensuite, une EventBridge cible est créée pour être exécutée selon le calendrier spécifié dans la règle.

```
aws events put-targets
--cli-input-json file://data.json
```

Le fichier d'entrée data.json se présente comme suit. La clé JSON `Sql` indique qu'il y a une seule instruction SQL. La valeur JSON `Arn` contient un identifiant de cluster. La valeur JSON `RoleArn` contient le rôle IAM utilisé pour exécuter le SQL comme décrit précédemment.

```
{
    "Rule": "test-redshift-cluster-data",
    "EventBusName": "default",
    "Targets": [
        {
            "Id": "2",
            "Arn": "arn:aws:redshift:us-east-1:123456789012:cluster:mycluster",
            "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
            "RedshiftDataParameters": {
                "Database": "dev",
                "DbUser": "root",
                "Sql": "select 1;",
                "StatementName": "test-redshift-cluster-data",
                "WithEvent": true
            }
        }
    ]
}
```

Appel à l'aide d'une seule instruction SQL et d'un groupe de travail

L'exemple suivant utilise le AWS CLI pour créer une EventBridge règle qui permet d'exécuter une instruction SQL sur un groupe de travail Amazon Redshift Serverless.

```
aws events put-rule
--name  test-redshift-serverless-workgroup-data
--schedule-expression "rate(1 minute)"
```

Ensuite, une EventBridge cible est créée pour être exécutée selon le calendrier spécifié dans la règle.

```
aws events put-targets
--cli-input-json file://data.json
```

Le fichier d'entrée data.json se présente comme suit. La clé JSON `Sql` indique qu'il y a une seule instruction SQL. La valeur JSON `Arn` contient un nom de groupe de travail.

La valeur JSON `RoleArn` contient le rôle IAM utilisé pour exécuter le SQL comme décrit précédemment.

```
{
    "Rule": "test-redshift-serverless-workgroup-data",
    "EventBusName": "default",
    "Targets": [
        {
            "Id": "2",
            "Arn": "arn:aws:redshift-serverless:us-east-1:123456789012:workgroup/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
            "RedshiftDataParameters": {
                "Database": "dev",
                "Sql": "select 1;",
                "StatementName": "test-redshift-serverless-workgroup-data",
                "WithEvent": true
            }
        }
    ]
}
```

Appel à l’aide de plusieurs instructions SQL et d’un cluster

L'exemple suivant utilise le AWS CLI pour créer une EventBridge règle qui permet d'exécuter plusieurs instructions SQL sur un cluster Amazon Redshift.

```
aws events put-rule
--name  test-redshift-cluster-data
--schedule-expression "rate(1 minute)"
```

Ensuite, une EventBridge cible est créée pour être exécutée selon le calendrier spécifié dans la règle.

```
aws events put-targets
--cli-input-json file://data.json
```

Le fichier d’entrée data.json se présente comme suit. La clé JSON `Sqls` indique qu’il existe plusieurs instructions SQL. La valeur JSON `Arn` contient un identifiant de cluster. La valeur JSON `RoleArn` contient le rôle IAM utilisé pour exécuter le SQL comme décrit précédemment.

```
{
    "Rule": "test-redshift-cluster-data",
    "EventBusName": "default",
    "Targets": [
        {
            "Id": "2",
            "Arn": "arn:aws:redshift:us-east-1:123456789012:cluster:mycluster",
            "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
            "RedshiftDataParameters": {
                "Database": "dev",
                "Sqls": ["select 1;", "select 2;", "select 3;"],
                "StatementName": "test-redshift-cluster-data",
                "WithEvent": true
            }
        }
    ]
}
```

Appel à l’aide de plusieurs instructions SQL et d’un groupe de travail

L'exemple suivant utilise le AWS CLI pour créer une EventBridge règle qui permet d'exécuter plusieurs instructions SQL sur un groupe de travail Amazon Redshift Serverless.

```
aws events put-rule
--name  test-redshift-serverless-workgroup-data
--schedule-expression "rate(1 minute)"
```

Ensuite, une EventBridge cible est créée pour être exécutée selon le calendrier spécifié dans la règle.

```
aws events put-targets
--cli-input-json file://data.json
```

Le fichier d’entrée data.json se présente comme suit. La clé JSON `Sqls` indique qu’il existe plusieurs instructions SQL. La valeur JSON `Arn` contient un nom de groupe de travail.
La valeur JSON `RoleArn` contient le rôle IAM utilisé pour exécuter le SQL comme décrit précédemment.

```
{
    "Rule": "test-redshift-serverless-workgroup-data",
    "EventBusName": "default",
```

```
    "Targets": [
        {
            "Id": "2",
            "Arn": "arn:aws:redshift-serverless:us-east-1:123456789012:workgroup/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
            "RedshiftDataParameters": {
                "Database": "dev",
                "Sqls": ["select 1;", "select 2;", "select 3;"],
                "StatementName": "test-redshift-serverless-workgroup-data",
                "WithEvent": true
            }
        }
    ]
}
```

Surveillance de l’API de données

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de l'API Data et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller l'API Data, signaler tout problème et prendre des mesures automatiques le cas échéant :

- 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 de ressources. Les événements provenant AWS des 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 CloudTrail capture les appels d'API et les événements associés effectués par ou pour le AWS compte de votre compte et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date à laquelle les appels ont eu lieu. Pour en savoir plus sur la manière dont Amazon Redshift est intégré à AWS CloudTrail, consultez Logging with CloudTrail. Pour plus d'informations à ce sujet CloudTrail, consultez le Guide de AWS CloudTrail l'utilisateur.

Rubriques

- Événements de surveillance pour l'API Amazon Redshift Data dans Amazon EventBridge

Événements de surveillance pour l'API Amazon Redshift Data dans Amazon EventBridge

Vous pouvez surveiller les événements de l'API Data dans EventBridge, qui fournit un flux de données en temps réel provenant de vos propres applications, applications SaaS et services. AWS EventBridge achemine ces données vers des cibles telles qu' AWS Lambda Amazon SNS. Ces événements sont les mêmes que ceux qui apparaissent dans CloudWatch Événements, qui fournit un flux en temps quasi réel d'événements système décrivant l'évolution des AWS ressources. Les événements sont envoyés au compte qui contient la base de données Amazon Redshift. Par exemple, si vous assumez un rôle dans un autre compte, les événements sont envoyés à ce compte. Pour plus d'informations, consultez la section EventBridge Événements Amazon dans le guide de EventBridge l'utilisateur Amazon. .

Les événements de l'API de données sont envoyés lorsque l'opération de l'API `ExecuteStatement` ou `BatchExecuteStatement` attribue à l'option `WithEvent` la valeur `true`. Le champ `state` de l'événement peut comporter l'une des valeurs suivantes :

- ABORTED (Abandonné) – L'exécution de la requête a été arrêtée par l'utilisateur.
- FAILED – L'exécution de la requête a échoué.
- FINISHED – L'exécution de la requête est terminée.

Les événements sont fournis sur la base de la garantie. Pour plus d'informations, consultez la section Événements liés AWS aux services dans le guide de EventBridge l'utilisateur Amazon.

Exemple pour l'événement terminé (FINISHED) de l'API de données

L'exemple suivant montre un événement pour l'API de données lorsque l'opération d'API `ExecuteStatement` se termine. Dans cet exemple, une instruction nommée `test.testtable` a terminé son exécution.

```
{
    "version": "0",
    "id": "18e7079c-dd4b-dd64-caf9-e2a31640dab0",
    "detail-type": "Redshift Data Statement Status Change",
    "source": "aws.redshift-data",
    "account": "123456789012",
```

```
    "time": "2020-10-01T21:14:26Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:redshift:us-east-1:123456789012:cluster:redshift-cluster-1"
    ],
    "detail": {
        "principal": "arn:aws:iam::123456789012:user/myuser",
        "statementName": "test.testtable",
        "statementId": "dd2e1ec9-2ee3-49a0-819f-905fa7d75a4a",
        "redshiftQueryId": -1,
        "state": "FINISHED",
        "rows": 1,
        "expireAt": 1601673265
    }
}
```

Utilisation AWS KMS avec l'API Amazon Redshift Data

Lorsque vous chiffrez votre cluster Amazon Redshift ou votre groupe de travail Redshift Serverless avec une clé gérée par le client, l'API Amazon Redshift Data utilise cette même clé gérée par le client pour stocker et chiffrer vos requêtes et vos résultats.

L'API Data chiffre vos données par défaut pour protéger les informations sensibles, telles que le texte et les résultats des requêtes. Il utilise des clés de AWS KMS chiffrement détenues par AWS pour cette protection.

Le chiffrement par défaut pour les données au repos réduit la charge opérationnelle et la complexité lorsque vous protégez des données sensibles. Cette approche vous permet de créer des applications sécurisées qui répondent à des exigences réglementaires et de conformité strictes en matière de chiffrement.

Utilisation des subventions dans AWS KMS

L'API Data nécessite une autorisation pour utiliser votre clé gérée par le client.

Lorsque vous appelez `ExecuteStatement` ou `BatchExecuteStatement` contre un cluster chiffré à l'aide d'une clé gérée par le client, Amazon Redshift crée une subvention en votre nom en envoyant une `CreateGrant` demande à AWS KMS. AWS KMS utilise des autorisations pour donner à l'API Data l'accès à une clé KMS de votre compte.

L'API Data nécessite l'autorisation d'utiliser votre clé gérée par le client pour les opérations suivantes :

- Envoyez `Encrypt` des demandes AWS KMS à pour chiffrer les métadonnées des requêtes à l'aide de la clé gérée par votre client.
- Envoyez `GenerateDataKey` des demandes AWS KMS à pour générer des clés de données chiffrées par la clé gérée par votre client.
- Envoyez `Decrypt` des demandes AWS KMS à pour déchiffrer les clés de données cryptées afin qu'ils puissent crypter vos données.

Vous pouvez révoquer l'accès à l'autorisation ou supprimer l'accès Amazon Redshift à votre clé gérée par le client à tout moment. Dans ce cas, l'API Data ne peut plus accéder aux données chiffrées par la clé gérée par votre client, ce qui affecte les opérations qui dépendent de ces données. Par exemple, si vous essayez de récupérer les résultats d'une requête ou de suivre l'état d'une requête après avoir révoqué l'autorisation, l'API Data renvoie un`AccessDeniedException`.

Politiques clés pour votre clé gérée par le client

Les stratégies de clés contrôlent l’accès à votre clé gérée par le client. Chaque clé gérée par le client doit avoir exactement une stratégie de clé, qui contient des instructions qui déterminent les personnes pouvant utiliser la clé et comment elles peuvent l’utiliser. Lorsque vous créez votre clé gérée par le client, vous pouvez spécifier une stratégie de clé. Pour plus d’informations, consultez Clés gérées par le client dans le Guide du développeur AWS Key Management Service .

Pour utiliser les clés gérées par vos clients avec l'API Data, vous devez d'abord autoriser l'accès à Amazon Redshift. Les opérations d'API suivantes doivent être autorisées dans la politique clé :

- `kms:CreateGrant` : ajoute une attribution à une clé gérée par le client. Les autorisations contrôlent l'accès à une AWS KMS clé spécifiée, ce qui permet d'accéder aux opérations d'autorisation requises par Amazon Redshift. Pour plus d'informations, consultez la section Utilisation des subventions dans AWS KMS.

Voici un exemple de politique clé :

```
"Statement":[
   {
      "Sid":"Allow access to principals authorized to use Amazon Redshift",
      "Effect":"Allow",
      "Principal":{
         "AWS":"*"
      },
```

```
      "Action":[
         "kms:DescribeKey",
         "kms:CreateGrant"
      ],
      "Resource":"*",
      "Condition":{
         "StringEquals":{
            "kms:ViaService":"redshift.amazonaws.com",
            "kms:CallerAccount":"111122223333"
         }
      }
   },
   {
      "Sid":"AllowKeyAdministratorsAccess",
      "Effect":"Allow",
      "Principal":{
         "AWS":"arn:aws:iam::111122223333:role/ExampleAdminRole"
      },
      "Action":"kms:*",
      "Resource":"*"
   },
   {
      "Sid":"AllowKeyUseForExampleRole",
      "Effect":"Allow",
      "Principal":{
         "AWS":"arn:aws:iam::111122223333:role/ExampleUserRole"
      },
      "Action":[
         "kms:Encrypt",
         "kms:Decrypt",
         "kms:ReEncrypt*",
         "kms:GenerateDataKey*",
         "kms:DescribeKey"
      ],
      "Resource":"*"
   }
]
```

Contexte de chiffrement de l'API de données

Un contexte de chiffrement est un ensemble facultatif de paires clé-valeur qui contient des informations contextuelles supplémentaires sur les données. AWS KMS utilise le contexte de chiffrement comme données authentifiées supplémentaires pour prendre en charge le chiffrement

authentifié. Lorsque vous incluez un contexte de chiffrement dans une demande de chiffrement de données, AWS KMS lie le contexte de chiffrement aux données chiffrées. Pour déchiffrer les données, vous devez inclure le même contexte de chiffrement dans la demande.

L'API Data utilise les trois mêmes paires clé-valeur de contexte de chiffrement dans toutes les opérations AWS KMS cryptographiques pour les clusters provisionnés :

- `aws:redshift:arn`— Le nom de ressource Amazon (ARN) du cluster
- `aws:redshift:createtime`— L'horodatage auquel vous avez demandé la création du cluster
- `serviceName` – `RedshiftDataAPI`

```
"EncryptionContextSubset": {
    "aws:redshift:arn": "arn:aws:redshift:us-east-1:123456789012:cluster:redshift-
cluster",
    "aws:redshift:createtime": "20250815T0000Z",
    "serviceName": "RedshiftDataAPI",
}
```

L'API Data utilise deux paires clé-valeur de contexte de chiffrement dans toutes les opérations AWS KMS cryptographiques pour les groupes de travail sans serveur :

- `aws:redshift-serverless:arn`— Le nom de ressource Amazon (ARN) de l'espace de noms
- `serviceName`— RedshiftData API

```
"EncryptionContextSubset": {
    "aws:redshift-serverless:arn": "arn:aws:redshift-serverless:us-
east-1:123456789012:namespace:12345678-1234-1234-1234-123456789012",
    "serviceName": "RedshiftDataAPI"
}
```

Pour plus d'informations sur le chiffrement, voir Introduction aux détails cryptographiques de AWS KMS. Pour plus d'informations sur Amazon Redshift et son AWS KMS intégration, consultez Comment Amazon Redshift l'utilise. AWS KMS

Utilisation d'Amazon Sagemaker Unified Studio pour interroger vos bases de données dans Amazon Redshift and the Lakehouse SageMaker

Amazon SageMaker Unified Studio fournit un environnement de développement hors console et prend en charge les analyses SQL sur les données de SageMaker Lakehouse, Amazon Redshift et Amazon Athena pour les analyses SQL. Accédez à Amazon SageMaker Unified Studio à l'aide de l'URL fournie par votre administrateur et utilisez votre SSO ou vos AWS informations d'identification pour vous connecter. Pour plus d'informations sur la configuration de votre premier projet, consultez Getting started dans le guide de l'utilisateur d'Amazon SageMaker Unified Studio.

Dans Amazon SageMaker Unified Studio, vous pouvez effectuer des analyses SQL en exécutant Amazon Redshift et Amazon Athena avec l'éditeur de requêtes. Utilisez l’éditeur de requête pour écrire et exécuter des requêtes, consulter les résultats et partager votre travail avec votre équipe. Exécutez des requêtes sur vos entrepôts de données Redshift dans votre compte Comptes AWS (au sein du même compte et sur votre autre compte Comptes AWS), créez des requêtes SQL pour Redshift et Athena à l'aide de la même interface et planifiez les requêtes SQL à l'aide d'Amazon Managed Workflows pour Apache Airflow. Vous pouvez également utiliser l’assistant SQL génératif Amazon Q pour générer du SQL à partir de langage naturel.

Groupes de paramètres Amazon Redshift

Dans Amazon Redshift, vous associez un groupe de paramètres avec chaque cluster que vous créez. Un groupe de paramètres est un groupe de paramètres qui s'appliquent à toutes les bases de données que vous créez dans le cluster. Ces paramètres configurent les paramètres de base de données tels que le délai de requête et le style de date. Lorsque vous lancez un cluster, vous devez l'associer à un groupe de paramètres. Si vous voulez modifier le groupe de paramètres par la suite, vous pouvez modifier le cluster et sélectionner un groupe de paramètres différent.

Chaque groupe de paramètres possède plusieurs paramètres pour configurer les paramètres de la base de données. La liste des paramètres disponibles dépend de la famille de groupe de paramètres auquel ce dernier appartient. La famille de groupes de paramètres par défaut est `redshift-2.0`.

Amazon Redshift fournit un groupe de paramètres par défaut pour chaque famille de groupe de paramètres. Le groupe de paramètres par défaut a des valeurs prédéfinies pour chacun de ses paramètres, et ne peut pas être modifié. Le format du nom du groupe de paramètres par défaut est `default.`*`parameter_group_family`*. Par exemple, le groupe de paramètres par défaut pour la famille de groupes de paramètres `redshift-2.0` est `default.redshift-2.0`.

Si vous souhaitez utiliser d'autres valeurs de paramètres que le groupe de paramètres par défaut, vous devez créer un groupe de paramètres personnalisés, puis lui associer votre cluster. A l'origine, les valeurs des paramètres d'un groupe de paramètres personnalisés sont les mêmes que celles du groupe de paramètres par défaut. La `source` initiale de tous les paramètres est `engine-default`, car les valeurs sont prédéfinies par Amazon Redshift. Une fois que vous avez modifié une valeur de paramètre, la `source` se change en `user` pour indiquer que la valeur a été modifiée par rapport à sa valeur par défaut.

> **Note**
>
> La console Amazon Redshift n'affiche pas la `source` de chaque paramètre. Vous devez utiliser l'API Amazon Redshift AWS CLI, le SDK ou l'un des kits de AWS développement logiciel (SDK) pour afficher le. `source`

Pour les groupes de paramètres que vous créez, vous pouvez modifier une valeur de paramètre à tout moment, ou vous pouvez réinitialiser toutes les valeurs des paramètres à leurs valeurs par défaut. Vous pouvez aussi associer un autre groupe de paramètres à un cluster. Dans certains cas,

il se peut que vous modifiiez les valeurs des paramètres d'un groupe de paramètres déjà associé à un cluster ou associiez un autre groupe de paramètres à un cluster. Dans certains cas, il se peut que vous ayez besoin de redémarrer le cluster pour que les valeurs modifiées prennent effet. Si le cluster échoue et est redémarré par Amazon Redshift, vos modifications sont appliquées à ce moment-là. Les modifications ne sont pas appliquées si votre cluster est redémarré au cours de la maintenance. Pour plus d'informations, consultez Propriétés WLM dynamiques et statiques.

Valeurs des paramètres par défaut

> **Note**
>
> Depuis le 10 janvier 2025, la valeur par défaut du paramètre `require_ssl` est true. Si vous ne souhaitez pas que votre cluster nécessite le protocole SSL, vous pouvez utiliser un groupe de paramètres personnalisé lors de sa création, ou modifier le cluster pour l'associer à un groupe de paramètres personnalisé après avoir créé le cluster avec la valeur par défaut.

Le tableau suivant affiche les valeurs des paramètres par défaut en un coup de œil, ainsi que les liens vers des informations plus détaillées pour chaque paramètre. Ce sont les valeurs par défaut pour la famille de groupe de paramètres `redshift-2.0`.

Nom du paramètre	Value	En savoir plus
auto_analyze	true	auto_analyze dans le Manuel du développeur de base de données Amazon Redshift
auto_mv	true	Automated materialized views (Vues matérialisées automatisées) dans le Guide du développeur de base de données Amazon Redshift
datestyle	ISO, MDY	datestyle dans le Manuel du développeur de base de données Amazon Redshift
enable_case_sensitive_identifier	false	enable_case_sensitive_identifier dans le Manuel du développeur de base de données Amazon Redshift

Nom du paramètre	Value	En savoir plus
enable_user_activity_logging	false	Journalisation des audits de base de données dans ce guide
extra_float_digits	0	extra_float_digits dans le Manuel du développeur de base de données Amazon Redshift
max_concurrency_scaling_clusters	1	max_concurrency_scaling_clusters dans le Manuel du développeur de base de données Amazon Redshift
query_group	default	query_group dans le Manuel du développeur de base de données Amazon Redshift
require_ssl	true	Configuration des options de sécurité des connexions dans ce guide
search_path	$user, public	search_path dans le Manuel du développeur de base de données Amazon Redshift
statement_timeout	0	statement_timeout dans le Manuel du développeur de base de données Amazon Redshift
wlm_json_configuration	[{"auto_wlm":true}]	Gestion de la charge de travail dans ce guide
use_fips_ssl	false	Activez le mode FIPS-compliant SSL uniquement si votre système doit l'être FIPS-compliant.

> **Note**
>
> Le paramètre `max_cursor_result_set_size` est obsolète. Pour plus d'informations sur la taille de l'ensemble de résultats du curseur, veuillez consulter la rubrique Contraintes de curseur dans le Manuel du développeur de base de données Amazon Redshift.

Vous pouvez ignorer temporairement un paramètre en utilisant la commande SET de la base de données. La commande SET remplace le paramètre pendant la durée de votre session en cours uniquement. Outre les paramètres répertoriés dans le tableau précédent, vous pouvez aussi ajuster temporairement le nombre d'emplacements en définissant `wlm_query_slot_count` dans la base de données. Le paramètre `wlm_query_slot_count` n'est pas disponible pour la configuration des groupes de paramètres. Pour plus d'informations sur l'ajustement du nombre d'emplacements, veuillez consulter la rubrique wlm_query_slot_count dans le Manuel du développeur de base de données Amazon Redshift. Pour plus d'informations sur le remplacement temporaire des autres paramètres, veuillez consulter la rubrique Modification de la configuration du serveur dans le Manuel du développeur de base de données Amazon Redshift.

Gestion de la charge de travail

Dans Amazon Redshift, vous utilisez la gestion de l'application (WLM) pour définir le nombre de files d'attente de requêtes qui sont disponibles, ainsi que le nombre de requêtes acheminées vers ces files d'attente en vue de leur traitement. WLM fait partie de la configuration du groupe de paramètres. Un cluster utilise la configuration WLM spécifiée dans son groupe de paramètres associé.

Lorsque vous créez un groupe de paramètres, la configuration WLM par défaut contient une seule file d'attente qui peut exécuter jusqu'à cinq requêtes simultanément. Vous pouvez ajouter d'autres files d'attente et configurer les propriétés WLM de chacune d'elles si vous souhaitez plus de contrôle sur le traitement des requêtes. Chaque file d'attente que vous ajoutez possède la même configuration WLM par défaut jusqu'à ce que vous configuriez ses propriétés.

Lorsque vous ajoutez des files d'attente supplémentaires, la dernière file d'attente de la configuration est la file d'attente par défaut. A moins qu'une requête ne soit acheminée vers une autre file d'attente selon les critères de la configuration WLM, elle est traitée par la file d'attente par défaut. Vous pouvez spécifier le mode et le niveau de simultanéité (emplacements de requête) pour la file d'attente par défaut, mais vous ne pouvez pas spécifier de groupes d'utilisateurs ou de groupes de requêtes pour la file d'attente par défaut.

Comme pour d'autres paramètres, vous ne pouvez pas modifier la configuration WLM du groupe de paramètres par défaut. Les clusters associés au groupe de paramètres par défaut utilisent toujours la configuration WLM par défaut. Pour modifier la configuration WLM, créez un nouveau groupe de paramètres, puis associez ce groupe de paramètres aux clusters nécessitant votre configuration WLM personnalisée.

Propriétés WLM dynamiques et statiques

Les propriétés de la configuration WLM sont dynamiques ou statiques. Vous pouvez appliquer des propriétés dynamiques à la base de données sans redémarrage du cluster, mais les propriétés statiques nécessitent un redémarrage du cluster pour que les modifications prennent effet. Pour de plus amples informations sur les propriétés statiques et dynamiques, veuillez consulter Propriétés de configuration dynamiques et statiques WLM.

Propriétés du paramètre de configuration de la gestion de la charge de travail

Vous pouvez configurer WLM à l'aide de la console Amazon Redshift, de l' AWS CLI API Amazon Redshift ou de l'un des kits SDK. AWS La configuration WLM utilise plusieurs propriétés pour définir un comportement de file d'attente, telles que l'allocation mémoire entre les files d'attente, le nombre de requêtes pouvant s'exécuter simultanément dans une file d'attente, et ainsi de suite.

> **Note**
>
> Les propriétés suivantes sont accompagnées de leurs noms Amazon Redshift, avec les noms de propriété JSON correspondants dans les descriptions.

La table suivante résume si une propriété est applicable à la gestion automatique ou manuelle de la charge de travail.

Propriété WLM	Gestion automatique de la charge de travail	Gestion manuelle de la charge de travail
Auto WLM	Oui	Oui
Activer l’accélération des requêtes courtes	Oui	Oui
Durée d'exécution maximale pour les requêtes courtes	Oui	Oui
Priority	Oui	Non
Type de requête	Oui	Oui

Propriété WLM	Gestion automatique de la charge de travail	Gestion manuelle de la charge de travail
Nom de la file d'attente	Oui	Oui
Mode de mise à l’échelle de la simultanéité	Oui	Oui
Concurrency	Non	Oui
Groupes d’utilisateurs	Oui	Oui
Caractère générique de groupe d’utilisateurs	Oui	Oui
Groupes de requêtes	Oui	Oui
Caractère générique de groupe de requêtes	Oui	Oui
Rôles utilisateurs	Oui	Oui
Caractère générique du rôle utilisateur	Oui	Oui
Timeout	Non	Obsolète
Mémoire	Non	Oui
Règles de surveillance de requête	Oui	Oui

La liste suivante décrit les propriétés WLM que vous pouvez configurer.

Auto WLM

Auto WLM défini sur `true` permet une utilisation automatique de WLM. Automatic WLM définit les valeurs Concurrency on main (Simultanéité sur principal) et Memory (%) (Mémoire (%)) sur `Auto`. Amazon Redshift gère la simultanéité des requêtes et l'allocation de mémoire. La valeur par défaut est `true`.

Propriété JSON : `auto_wlm`

Activer l'accélération des requêtes courtes

L’accélération des requêtes courtes (SQA) établit la priorité des requêtes de courte durée sélectionnées sur les requêtes de longue durée. La SQA exécute des requêtes de courte durée dans un espace dédié, afin que les requêtes SQA ne soient pas forcées d'attendre dans des files d'attente derrière les requêtes de longue durée. Avec la SQA, les requêtes de courte durée commencent à s'exécuter plus rapidement et les utilisateurs obtiennent les résultats plus rapidement. Lorsque vous activez la SQA, vous pouvez également spécifier le délai d'exécution maximal des requêtes courtes. Pour activer la SQA, spécifiez `true`. La valeur par défaut est `false`. Ce paramètre est appliqué à chaque groupe de paramètres plutôt qu'à la file d'attente.

Propriété JSON : `short_query_queue`

Durée d'exécution maximale pour les requêtes courtes

Lorsque vous activez SQA, vous pouvez également spécifier la valeur 0 pour permettre à WLM de définir le délai d'exécution maximal des requêtes courtes. Vous pouvez aussi spécifier une valeur comprise entre 1 et 20 secondes, en millisecondes. La valeur par défaut est `0`.

Propriété JSON : `max_execution_time`

Priorité

La priorité définit la priorité des requêtes qui s'exécutent dans une file d'attente. Pour définir la priorité, le mode WLM doit être défini sur Auto WLM ; c'est-à-dire que `auto_wlm` doit être `true`. Les valeurs de priorité peuvent être `highest`, `high`, `normal`, `low` et `lowest`. La valeur par défaut est `normal`.

Propriété JSON : `priority`

Type de requête

Le type de file d'attente désigne une file d'attente telle qu'utilisée par la gestion automatique de la charge de travail ou la gestion manuelle de la charge de travail. Définissez `queue_type` sur `auto` ou `manual`. Si aucune valeur n'est spécifiée, la valeur par défaut est `manual`.

Propriété JSON : `queue_type`

Nom de la file d'attente

Nom de la file d'attente. Vous pouvez définir le nom de la file d'attente en fonction des besoins de votre entreprise. Les noms de file d'attente doivent être uniques dans une configuration

WLM, contenir jusqu'à 64 caractères alphanumériques, traits de soulignement ou espaces, et ne peuvent pas contenir de guillemets. Par exemple, si vous avez une file d'attente pour vos requêtes ETL, vous pouvez la nommer `ETL queue`. Ce nom est utilisé dans les mesures, les valeurs des tables système et la console Amazon Redshift pour identifier la file d'attente. Les requêtes et les rapports qui utilisent le nom de ces sources doivent pouvoir gérer les changements de nom. Auparavant, les noms de file d'attente étaient générés par Amazon Redshift. Les noms par défaut des files d'attente sont `Queue 1`, `Queue 2`, jusqu'à la dernière file d'attente nommée `Default queue`.

> **Important**
>
> Si vous modifiez le nom d'une file d'attente, la valeur de `QueueName` dimension des métriques de file d'attente WLM (telles que WLMQueueLength WLMQueueWaitTime WLMQueriesCompletedPerSecond, WLMQueryDuration, WLMRunningQueries,,,, etc.) change également. Ainsi, si vous modifiez le nom d'une file d'attente, vous devrez peut-être modifier CloudWatch les alarmes que vous avez configurées.

Propriété JSON : `name`

Mode de mise à l'échelle de la simultanéité

Pour activer la mise à l'échelle de la simultanéité sur une file d'attente, définissez le mode de mise à l'échelle de la simultanéité sur `auto`. Lorsque le nombre de requêtes acheminées vers une file d'attente dépasse la simultanéité configurée pour la file d'attente, les requêtes éligibles sont envoyées au cluster de mise à l'échelle. Lorsque des emplacements deviennent disponibles, les requêtes s'exécutent sur le cluster principal. La valeur par défaut est `off`.

Propriété JSON : `concurrency_scaling`

Simultanéité

Nombre de requêtes qui peuvent être exécutées simultanément dans une file d'attente WLM manuelle. Cette propriété s'applique uniquement à la gestion manuelle de la charge de travail. Si la mise à l'échelle de la simultanéité est activée, les requêtes éligibles sont envoyées à un cluster de mise à l'échelle lorsqu'une file d'attente atteint le niveau de simultanéité (emplacements de requête). Si la mise à l'échelle de la simultanéité est désactivée, les requêtes attendent en file d'attente jusqu'à ce qu'un emplacement se libère. La plage est comprise entre 1 et 50.

Propriété JSON : `query_concurrency`

Groupes d'utilisateurs

Liste séparée par des virgules de noms de groupes d'utilisateurs. Lorsque les membres du groupe d'utilisateurs exécutent les requêtes de la base de données, leurs requêtes sont acheminées vers la file d'attente associée à leur groupe d'utilisateurs.

Propriété JSON : `user_group`

Caractère générique du groupe d'utilisateurs

Une valeur booléenne qui indique s'il convient d'activer les caractères génériques pour les groupes d'utilisateurs. Si la valeur est 0, les caractères génériques sont désactivés ; si la valeur est 1, les caractères génériques sont activés. Lorsque les caractères génériques sont activés, vous pouvez utiliser « * » ou « ? » pour spécifier plusieurs groupes d'utilisateurs lors de l'exécution des requêtes. Pour plus d’informations, consultez Caractères génériques.

Propriété JSON : `user_group_wild_card`

Groupes de requêtes

Liste séparée par des virgules de groupes de requêtes. Lorsque les membres du groupe de requêtes exécutent les requêtes de la base de données, leurs requêtes sont acheminées vers la file d'attente associée à leur groupe d'utilisateurs.

Propriété JSON : `query_group`

Caractère générique de groupe de requêtes

Valeur booléenne qui indique s’il convient d’activer les caractères génériques pour les groupes de requêtes. Si la valeur est 0, les caractères génériques sont désactivés ; si la valeur est 1, les caractères génériques sont activés. Lorsque les caractères génériques sont activés, vous pouvez utiliser « * » ou « ? » pour spécifier plusieurs groupes de requêtes lors de l’exécution des requêtes. Pour plus d’informations, consultez Caractères génériques.

Propriété JSON : `query_group_wild_card`

Rôles utilisateur

Liste séparée par des virgules de rôles utilisateurs. Lorsque des membres avec ce rôle utilisateur exécutent des requêtes de la base de données, leurs requêtes sont acheminées vers la file d'attente associée à leur rôle utilisateur. Pour plus d'informations sur les rôles des utilisateurs, consultez la section Contrôle Role-based d'accès (RBAC).

Propriété JSON : `user_role`

Caractère générique des rôles utilisateurs

Valeur booléenne qui indique s'il convient d'activer les caractères génériques pour les groupes de requêtes. Si la valeur est 0, les caractères génériques sont désactivés ; si la valeur est 1, les caractères génériques sont activés. Lorsque les caractères génériques sont activés, vous pouvez utiliser « * » ou « ? » pour spécifier plusieurs groupes de requêtes lors de l'exécution des requêtes. Pour plus d'informations, consultez Caractères génériques.

Propriété JSON : `user_role_wild_card`

Délai (ms)

Le délai WLM (`max_execution_time`) est obsolète. Il n'est pas disponible lors de l'utilisation de la gestion automatique de la charge de travail. Au lieu de cela, créez une règle de surveillance de requête (QRM) `query_execution_time` pour limiter le temps d'exécution écoulé d'une requête. Pour de plus amples informations, consultez Règles de surveillance de requête WLM.

Durée maximale, en millisecondes, pendant laquelle les requêtes peuvent s'exécuter avant d'être annulées. Dans certains cas, une requête en lecture seule, telle qu'une instruction SELECT peut être annulée en raison d'une expiration WLM. Dans ces cas-là, WLM tente d'acheminer la requête vers la file d'attente correspondante suivante en fonction des règles d'affectation de file d'attente de WLM. Si la requête ne correspond pas à une autre définition de file d'attente, la requête est annulée ; elle n'est pas affectée à la file d'attente par défaut. Pour de plus amples informations, veuillez consulter WLM Query Queue Hopping (Saut de file d'attente des requêtes WLM). Le délai WLM ne s'applique pas à une requête qui a atteint l'état `returning`. Pour afficher l'état d'une requête, consultez la table système STV_WLM_QUERY_STATE.

Propriété JSON : `max_execution_time`

Memory (%) (Mémoire (%))

Pourcentage de mémoire à allouer à la file d'attente. Si vous spécifiez un pourcentage de mémoire pour une file d'attente au moins, vous devez indiquer un pourcentage pour toutes les autres files d'attente afin d'atteindre un total de 100 %. Si votre allocation mémoire est inférieure à 100 % sur l'ensemble des files d'attente, la mémoire non allouée est gérée par le service. Le service peut temporairement attribuer cette mémoire non allouée à une file d'attente qui demande plus de mémoire pour le traitement.

Propriété JSON : `memory_percent_to_use`

Règles de surveillance de requête

Vous pouvez utiliser les règles de surveillance de requête WLM afin de surveiller en permanence vos files d'attente WLM en fonction de critères ou de prédicats que vous spécifiez. Par exemple, vous pouvez surveiller les requêtes qui tendent à consommer des ressources système excessives, puis initier une action donnée lorsqu'une requête dépasse les limites de performance que vous indiquez.

> **Note**
>
> Si vous créez des règles par programmation, il est recommandé d'utiliser la console afin de générer les données JSON à inclure dans la définition du groupe de paramètres.

Vous associez une règle de surveillance de requête à une file d'attente de requêtes spécifique. Vous pouvez disposer de jusqu'à 25 règles par file d'attente et la limite totale pour toutes les files d'attente est de 25 règles.

Propriété JSON : `rules`

Propriétés de hiérarchie JSON

```
rules
    rule_name
    predicate
        metric_name
        operator
        value
    action
        value
```

Pour chaque règle, vous spécifiez les propriétés suivantes :

- `rule_name` – Les noms de règles doivent être uniques au sein de la configuration WLM. Les noms de règles peut comporter jusqu'à 32 caractères alphanumériques ou traits de soulignement et ne doivent pas contenir d'espaces ni de guillemets.
  - `predicate` – Chaque règle peut comporter jusqu'à trois prédicats. Pour chaque prédicats, vous spécifiez les propriétés suivantes.

    - `metric_name` – Pour connaître la liste des métriques, veuillez consulter la rubrique Métriques de surveillance de requête dans le Manuel du développeur de base de données Amazon Redshift.
    - `operator` – Les opérations sont =, < et >.
    - `value` – La valeur de seuil pour la métrique spécifiée déclenchant une action.
- `action` – Chaque règle est associée à une action. Les actions valides sont :
    - `log`
    - hop (uniquement disponible avec la gestion manuelle de la charge de travail)
    - `abort`
    - `change_query_priority` (uniquement disponible avec la gestion automatique de la charge de travail)

L'exemple suivant présente le fichier JSON pour une règle de surveillance de requête WLM nommée `rule_1`, avec deux prédicats et l'action hop.

```
"rules": [
          {
            "rule_name": "rule_1",
            "predicate": [
              {
                "metric_name": "query_execution_time",
                "operator": ">",
                "value": 100000
              },
              {
                "metric_name": "query_blocks_read",
                "operator": ">",
                "value": 1000
              }
            ],
            "action": "hop"
          }
        ]
```

Pour de plus amples informations sur chacune de ces propriétés et les stratégies de configuration des files d'attente de requête, veuillez consulter Implémentation de la gestion des charges de travail dans le Manuel du développeur de base de données Amazon Redshift.

Configuration du paramètre WLM à l'aide du AWS CLI

Pour configurer WLM, vous modifiez le paramètre `wlm_json_configuration`. La taille maximale de la valeur de la propriété `wlm_json_configuration` est de 8 000 caractères. La valeur est mise en forme au format JSON (JavaScript Object Notation). Si vous configurez WLM à l' AWS CLI aide de l'API Amazon Redshift ou de l'un des AWS kits SDK, consultez le reste de cette section pour apprendre à créer la structure JSON pour le paramètre. `wlm_json_configuration`

> **Note**
>
> Si vous configurez WLM en utilisant la console Amazon Redshift, vous n'avez pas besoin de comprendre le format JSON, car la console offre un moyen simple d'ajouter des files d'attente et de configurer leurs propriétés. Pour plus d'informations sur la configuration de WLM à l'aide de la console, consultez Modification d'un groupe de paramètres.

Exemple

L'exemple suivant illustre la configuration WLM par défaut, qui définit une file d'attente avec Automatic WLM.

```
{
   "auto_wlm": true
}
```

Exemple

L'exemple suivant est une configuration WLM personnalisée, qui définit une file d'attente WLM manuelle avec un niveau de simultanéité (emplacements de requête) égal à cinq.

```
{
   "query_concurrency":5
}
```

Syntaxe

La configuration WLM par défaut est très simple, avec une seule file d'attente et une seule propriété. Vous pouvez ajouter plus de files d'attente et configurer plusieurs propriétés pour chaque file d'attente de la structure JSON. La syntaxe suivante représente la structure JSON que vous utilisez pour configurer plusieurs files d'attente avec plusieurs propriétés :

```
[
   {
      "ParameterName":"wlm_json_configuration", "ParameterValue":
         "[
             {
                "q1_first_property_name":"q1_first_property_value",
                "q1_second_property_name":"q1_second_property_value",
                ...
             },
             {
                "q2_first_property_name":"q2_first_property_value",
                "q2_second_property_name":"q2_second_property_value",
                ...
             }
             ...

         ]"
   }
]
```

Dans l'exemple précédent, les propriétés représentatives qui commencent par q1 sont les objets d'un tableau de la première file d'attente. Chacun de ces objets est une name/value paire ; `name` et `value` ensemble, définissez les propriétés WLM pour la première file d'attente. Les propriétés représentatives qui commencent par q2 sont les objets d'un tableau de la deuxième file d'attente. Si vous avez besoin de plus de files d'attente, vous ajoutez un autre tableau pour chaque file d'attente supplémentaire et définissez les propriétés de chaque objet.

Lorsque vous modifiez la configuration WLM, vous devez y inclure la totalité de la structure de vos files d'attente, même si vous ne voulez modifier qu'une seule propriété au sein d'une file d'attente. La raison en est que toute la structure JSON est passée sous forme de chaîne comme valeur du paramètre `wlm_json_configuration`.

Formatage du AWS CLI command

Le paramètre `wlm_json_configuration` nécessite un format spécifique lorsque vous utilisez l' AWS CLI. Le format que vous utilisez dépend du système d'exploitation de votre client. Comme les systèmes d'exploitation ont différentes façons de joindre la structure JSON, elle est transmise correctement à partir de la ligne de commande. Pour plus de détails sur la création de la commande appropriée dans les systèmes d'exploitation Linux, macOS et Windows, consultez les sections suivantes. Pour plus d'informations sur les différences entre les structures de données JSON incluses

AWS CLI en général, consultez la section Citer des chaînes dans le Guide de l'AWS Command Line Interface utilisateur.

Exemples

L'exemple de commande suivant configure la gestion manuelle de la charge de travail pour un groupe de paramètres appelé `example-parameter-group`. La configuration permet l'accélération des requêtes courtes avec une durée d'exécution maximale pour les requêtes courtes définie sur 0, ce qui nécessite que WLM définisse la valeur dynamiquement. Le paramètre `ApplyType` a la valeur `dynamic`. Cette valeur signifie que toute modification apportée aux propriétés dynamiques du paramètre est appliquée immédiatement, à moins que d'autres modifications statiques n'aient été apportées à la configuration. La configuration définit trois files d'attente avec les éléments suivants :

- La première file d'attente permet aux utilisateurs de spécifier `report` comme étiquette (tel qu'indiqué dans la propriété `query_group`) dans leurs requêtes pour aider à acheminer les requêtes vers cette file d'attente. Comme les recherches par caractères génériques sont activées pour l'étiquette `report*`, l'étiquette n'a pas besoin d'être exacte pour que les requêtes soient acheminées vers la file d'attente. Par exemple, `reports` et `reporting` correspondent également à ce groupe de requêtes. La file d'attente se voit allouer 25 % de la mémoire totale sur toutes les files d'attente et peut exécuter jusqu'à quatre requêtes en même temps. Les requêtes sont limitées à une durée maximum de 20 000 millisecondes (ms). Si le mode est défini sur auto, les requêtes éligibles sont envoyées à un cluster de mise à l'échelle lorsque tous les emplacements de requête de la file d'attente sont occupés.
- La deuxième file d'attente permet aux utilisateurs qui sont membres des groupes `admin` ou `dba` de la base de données d'avoir leurs requêtes acheminées vers la file d'attente en vue de leur traitement. Comme les recherches par caractères génériques sont désactivées pour les groupes d'utilisateurs, les utilisateurs doivent correspondre exactement aux groupes de la base de données pour que leurs requêtes soient acheminées vers la file d'attente. La file d'attente se voit allouer 40 % de la mémoire totale sur toutes les files d'attente et peut exécuter jusqu'à cinq requêtes en même temps. Si le mode est désactivé, toutes les requêtes envoyées par les membres des groupes admin ou dba s'exécutent sur le cluster principal.
- La dernière file d'attente de la configuration est la file d'attente par défaut. Cette file d'attente se voit allouer 35 % de la mémoire totale sur toutes les files d'attente et peut traiter jusqu'à cinq requêtes à la fois. Le mode est défini sur auto.

> **Note**
>
> L'exemple est affiché sur plusieurs lignes à des fins de démonstration. Les commandes réelles ne comportent pas de sauts de ligne.

```
aws redshift modify-cluster-parameter-group
--parameter-group-name example-parameter-group
--parameters
'[
  {
    "query_concurrency": 4,
    "max_execution_time": 20000,
    "memory_percent_to_use": 25,
    "query_group": ["report"],
    "query_group_wild_card": 1,
    "user_group": [],
    "user_group_wild_card": 0,
    "user_role": [],
    "user_role_wild_card": 0,
    "concurrency_scaling": "auto",
    "queue_type": "manual"
  },
  {
    "query_concurrency": 5,
    "memory_percent_to_use": 40,
    "query_group": [],
    "query_group_wild_card": 0,
    "user_group": [
      "admin",
      "dba"
    ],
    "user_group_wild_card": 0,
    "user_role": [],
    "user_role_wild_card": 0,
    "concurrency_scaling": "off",
    "queue_type": "manual"
  },
  {
    "query_concurrency": 5,
    "query_group": [],
    "query_group_wild_card": 0,
```

```
    "user_group": [],
    "user_group_wild_card": 0,
    "user_role": [],
    "user_role_wild_card": 0,
    "concurrency_scaling": "auto",
    "queue_type": "manual"
  },
  {"short_query_queue": true}
]'
```

Voici un exemple de configuration de règle de surveillance de requête WLM pour une configuration de gestion automatique de la charge de travail. L'exemple crée un groupe de paramètres nommé `example-monitoring-rules`. La configuration définit les mêmes trois files d'attente que dans l'exemple précédent, mais `query_concurrency` et `memory_percent_to_use` ne sont plus spécifiés. La configuration ajoute également les règles et les priorités de requête suivantes :

- La première file d'attente définit une règle nommée `rule_1`. La règle a deux prédicats : `query_cpu_time > 10000000` et `query_blocks_read > 1000`. L'action de la règle est `log`. La priorité de cette file d'attente est `Normal`.
- La deuxième file d'attente définit une règle nommée `rule_2`. La règle a deux prédicats : `query_execution_time > 600000000` et `scan_row_count > 1000000000`. L'action de la règle est `abort`. La priorité de cette file d'attente est `Highest`.
- La dernière file d'attente de la configuration est la file d'attente par défaut. La priorité de cette file d'attente est `Low`.

> **Note**
>
> L'exemple est affiché sur plusieurs lignes à des fins de démonstration. Les commandes réelles ne comportent pas de sauts de ligne.

```
aws redshift modify-cluster-parameter-group
--parameter-group-name example-monitoring-rules
--parameters
'[ {
  "query_group" : [ "report" ],
  "query_group_wild_card" : 1,
  "user_group" : [ ],
  "user_group_wild_card" : 0,
```

```
  "user_role": [ ],
  "user_role_wild_card": 0,
  "concurrency_scaling" : "auto",
  "rules" : [{
    "rule_name": "rule_1",
    "predicate": [{
      "metric_name": "query_cpu_time",
      "operator": ">",
      "value": 1000000 },
      { "metric_name": "query_blocks_read",
      "operator": ">",
      "value": 1000
    } ],
    "action" : "log"
  } ],
   "priority": "normal",
   "queue_type": "auto"
}, {
  "query_group" : [ ],
  "query_group_wild_card" : 0,
  "user_group" : [ "admin", "dba" ],
  "user_group_wild_card" : 0,
  "user_role": [ ],
  "user_role_wild_card": 0,
  "concurrency_scaling" : "off",
  "rules" : [ {
    "rule_name": "rule_2",
    "predicate": [
      {"metric_name": "query_execution_time",
      "operator": ">",
      "value": 600000000},
      {"metric_name": "scan_row_count",
      "operator": ">",
      "value": 1000000000}],
      "action": "abort"}],
   "priority": "high",
   "queue_type": "auto"

}, {
  "query_group" : [ ],
  "query_group_wild_card" : 0,
  "user_group" : [ ],
  "user_group_wild_card" : 0,
  "user_role": [ ],
```

```
  "user_role_wild_card": 0,
  "concurrency_scaling" : "auto",
  "priority": "low",
  "queue_type": "auto",
  "auto_wlm": true
}, {
  "short_query_queue" : true
} ]'
```

Configuration de WLM à l'aide du AWS CLI en ligne de commande avec un fichier JSON

Vous pouvez modifier le paramètre `wlm_json_configuration` à l'aide de l' AWS CLI et transmettre la valeur de l'argument `parameters` en tant que fichier JSON.

```
aws redshift modify-cluster-parameter-group --parameter-group-name
 myclusterparaametergroup --parameters file://modify_pg.json
```

Les arguments pour `--parameters` sont stockés dans le fichier `modify_pg.json` : L'emplacement du fichier est spécifié dans le format de votre système d'exploitation. Pour de plus amples informations, veuillez consulter Chargement des paramètres à partir d'un fichier. Voici les exemples de contenu du `modify_pg.json` fichier JSON.

```
[
    {
        "ParameterName": "wlm_json_configuration",
        "ParameterValue": "[{\"user_group\":\"example_user_group1\",\"query_group\":
 \"example_query_group1\", \"query_concurrency\":7},{\"query_concurrency\":5}]"
    }
]
```

```
[
    {
        "ParameterName": "wlm_json_configuration",
        "ParameterValue": "[{\"query_group\":[\"reports\"],\"query_group_wild_card\":0,
\"query_concurrency\":4,\"max_execution_time\":20000,\"memory_percent_to_use\":25},
{\"user_group\":[\"admin\",\"dba\"],\"user_group_wild_card\":1,\"query_concurrency\":5,
\"memory_percent_to_use\":40},{\"query_concurrency\":5,\"memory_percent_to_use\":35},
{\"short_query_queue\": true, \"max_execution_time\": 5000 }]",
        "ApplyType": "dynamic"
```

```
    }
]
```

Règles de configuration du WLM à l'aide du AWS CLI en ligne de commande sur les systèmes d'exploitation Linux et macOS

Suivez ces règles pour exécuter une AWS CLI commande avec des paramètres sur une seule ligne :

- Toute la structure JSON doit être placée entre guillemets simples (') et entre crochets ([ ]).
- Tous les noms de paramètre et valeurs de paramètre doivent se trouver entre guillemets doubles (").
- Au sein de la valeur `ParameterValue`, vous devez placer toute la structure imbriquée entre guillemets doubles (") et entre crochets ([ ]).
- Au sein de la structure imbriquée, chacune des propriétés et des valeurs de chaque file d'attente doivent être placées entre accolades ({}).
- Au sein de la structure imbriquée, vous devez utiliser le caractère d'échappement barre oblique inverse (\) avant chaque guillemet double (").
- Pour les name/value paires, deux points (:) séparent chaque propriété de sa valeur.
- Chaque name/value paire est séparée de l'autre par une virgule (,).
- Plusieurs files d'attente sont séparées par une virgule (,) entre la fin d'accolade d'une file d'attente (}) et le début d'accolade de la file d'attente suivante ({).

Règles de configuration du WLM à l'aide du AWS CLI sous Windows PowerShell sur les systèmes d'exploitation Microsoft Windows

Suivez ces règles pour exécuter une AWS CLI commande avec des paramètres sur une seule ligne :

- Toute la structure JSON doit être placée entre guillemets simples (') et entre crochets ([ ]).
- Tous les noms de paramètre et valeurs de paramètre doivent se trouver entre guillemets doubles (").
- Au sein de la valeur `ParameterValue`, vous devez placer toute la structure imbriquée entre guillemets doubles (") et entre crochets ([ ]).
- Au sein de la structure imbriquée, chacune des propriétés et des valeurs de chaque file d'attente doivent être placées entre accolades ({}).
- Au sein de la structure imbriquée, vous devez utiliser le caractère d'échappement de barre oblique inverse (\) avant chaque guillemet double (") et son caractère d'échappement de barre oblique

inverse (\). Cette exigence signifie que vous utiliserez trois barres obliques et un guillemet double pour vous assurer que les propriétés sont correctement transmises (\\\").

- Pour les name/value paires, deux points (:) séparent chaque propriété de sa valeur.
- Chaque name/value paire est séparée de l'autre par une virgule (,).
- Plusieurs files d'attente sont séparées par une virgule (,) entre la fin d'accolade d'une file d'attente (}) et le début d'accolade de la file d'attente suivante ({).

Règles de la configuration WLM à l'aide de l'invite de commande sur les systèmes d'exploitation Windows

Suivez ces règles pour exécuter une AWS CLI commande avec des paramètres sur une seule ligne :

- Toute la structure JSON doit être placée entre guillemets doubles (") et entre crochets ([ ]).
- Tous les noms de paramètre et valeurs de paramètre doivent se trouver entre guillemets doubles (").
- Au sein de la valeur `ParameterValue`, vous devez placer toute la structure imbriquée entre guillemets doubles (") et entre crochets ([ ]).
- Au sein de la structure imbriquée, chacune des propriétés et des valeurs de chaque file d'attente doivent être placées entre accolades ({}).
- Au sein de la structure imbriquée, vous devez utiliser le caractère d'échappement de barre oblique inverse (\) avant chaque guillemet double (") et son caractère d'échappement de barre oblique inverse (\). Cette exigence signifie que vous utiliserez trois barres obliques et un guillemet double pour vous assurer que les propriétés sont correctement transmises (\\\").
- Pour les name/value paires, deux points (:) séparent chaque propriété de sa valeur.
- Chaque name/value paire est séparée de l'autre par une virgule (,).
- Plusieurs files d'attente sont séparées par une virgule (,) entre la fin d'accolade d'une file d'attente (}) et le début d'accolade de la file d'attente suivante ({).

Création d'un groupe de paramètres

Si vous souhaitez définir des valeurs de paramètres différentes du groupe de paramètres par défaut, vous pouvez créer votre propre groupe de paramètres.

Pour créer un groupe de paramètres

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Configurations, puis choisissez Gestion des charges de travail pour afficher la page Gestion des charges de travail.
3. Choisissez Créer pour afficher la fenêtre Créer un groupe de paramètres.
4. Entrez une valeur pour Nom du groupe de paramètres et Description.
5. Choisissez Créer pour créer le groupe de paramètres.

Modification d'un groupe de paramètres

Vous pouvez visualiser votre groupe de paramètres pour afficher un résumé des valeurs des paramètres et de la configuration de la charge de travail (WLM). Vous pouvez modifier les paramètres pour changer leurs valeurs et les propriétés de la configuration WLM.

> **Note**
>
> Vous ne pouvez pas modifier le groupe de paramètres par défaut.

Console de gestion AWS

Dans la console, les paramètres de groupes apparaissent dans l'onglet Paramètres et les Files d'attente de charges de travail apparaissent dans l'onglet Gestion des charges de travail.

Pour modifier un groupe de paramètres

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Configurations, puis choisissez Gestion des charges de travail pour afficher la page Gestion des charges de travail.
3. Choisissez le groupe de paramètres que vous souhaitez modifier pour afficher la page des détails avec des onglets pour Paramètres et Gestion des charges de travail.
4. Choisissez l'onglet Paramètres pour afficher les valeurs de paramètre en cours.
5. Choisissez Modifier les paramètres pour permettre la modification de la définition de ces paramètres.

- auto_analyze
- auto_mv
- datestyle
- enable_case_sensitive_identifier
- enable_user_activity_logging
- extra_float_digits
- max_concurrency_scaling_clusters
- max_cursor_result_set_size
- query_group
- require_ssl
- search_path
- statement_timeout
- use_fips_ssl

Pour obtenir plus d'informations sur ces paramètres, consultez Groupes de paramètres Amazon Redshift.

6. Entrez les modifications, puis choisissez Enregistrer pour mettre à jour le groupe de paramètres.

Pour modifier la configuration WLM d'un groupe de paramètres

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Configurations, puis choisissez Gestion des charges de travail pour afficher la page Gestion des charges de travail.
3. Choisissez le groupe de paramètres que vous souhaitez modifier pour afficher la page des détails avec des onglets pour Paramètres et Gestion des charges de travail.
4. Choisissez l'onglet Gestion des charges de travail afin d'afficher la configuration WLM actuelle.
5. Choisissez Modifier les files d'attente des charges de travail pour modifier la configuration de la gestion de la charge de travail.

6. (Facultatif) Sélectionnez Activer l'accélération des requêtes courtes pour activer l'accélération des requêtes courtes (SQA).

   Lorsque vous activez SQA, Maximum run time for short queries (1 to 20 seconds) (Durée maximale d'exécution pour les courtes requêtes (1 à 20 secondes) a par défaut la valeur Dynamic. Pour définir la durée maximale d'exécution à une valeur fixe, choisissez une valeur comprise entre 1 et 20.

7. Effectuez une ou plusieurs des actions suivantes pour modifier la configuration de la file d'attente :

   - Choisissez Basculer en mode WLM pour choisir entre WLM automatique et WLM manuel.

     Avec WLM automatique, les valeurs Mémoire et Simultanéité sur principal sont définies sur automatique.
   - Pour créer une file d'attente, choisissez Modifier les files d'attente de charges de travail, puis choisissez Ajouter une file d'attente.
   - Pour modifier une file d'attente, modifiez les valeurs de propriété de la table. En fonction du type de file d'attente, les propriétés peuvent inclure :
     - Le nom de la file d'attente peut être modifié.
     - Memory (%) (Mémoire (%))
     - Concurrency on main cluster (Simultanéité sur cluster principal)
     - Concurrency Scaling mode (Mode de mise à l'échelle de la simultanéité) peut être défini sur off ou auto.
     - Délai (ms)
     - User groups (Groupes d'utilisateurs)
     - Query groups (Groupes de requêtes)
     - Rôles utilisateurs

     Pour de plus amples informations sur ces propriétés, veuillez consulter Propriétés du paramètre de configuration de la gestion de la charge de travail.

     > **Important**
     >
     > Si vous modifiez le nom d'une file d'attente, la valeur de `QueueName` dimension des métriques de file d'attente WLM (telles que WLMQueueLength WLMQueueWaitTime WLMQueriesCompletedPerSecond, WLMQueryDuration,

WLMRunningQueries,,,, etc.) change également. Par conséquent, si vous modifiez le nom d'une file d'attente, vous devrez peut-être modifier les alarmes CloudWatch que vous avez configurées.

- Pour modifier l'ordre des files d'attente, sélectionnez les boutons fléchés Haut et Bas.
- Pour supprimer une file d'attente, choisissez Delete (Supprimer) dans la ligne de la file d'attente de la table.

8. (Facultatif) Sélectionnez Reporter les modifications dynamiques jusqu'au redémarrage pour appliquer les modifications aux clusters après leur prochain redémarrage.

> **Note**
>
> Certaines modifications nécessitent un redémarrage du cluster, quel que soit le paramètre. Pour plus d'informations, consultez Propriétés WLM dynamiques et statiques.

9. Choisissez Enregistrer.

AWS CLI

Pour configurer les paramètres Amazon Redshift à l'aide de AWS CLI, vous devez utiliser la commande https://docs.aws.amazon.com/cli/latest/reference/redshift/modify-cluster-parameter-group.html modify-cluster-parameter-group pour un groupe de paramètres spécifique. Vous spécifiez le groupe de paramètres à modifier dans `parameter-group-name`. Vous utilisez le `parameters` paramètre (pour la `modify-cluster-parameter-group` commande) pour spécifier des name/value paires pour chaque paramètre que vous souhaitez modifier dans le groupe de paramètres.

> **Note**
>
> Il existe des considérations particulières lors de la configuration du paramètre `wlm_json_configuration` à l'aide de l' AWS CLI. Les exemples de cette section s'appliquent à tous les paramètres, à l'exception de `wlm_json_configuration`. Pour plus d'informations sur la configuration `wlm_json_configuration` à l'aide du AWS CLI, consultezGestion de la charge de travail.

Une fois que vous avez modifié les valeurs des paramètres, vous devez redémarrer les clusters qui sont associées au groupe de paramètres modifié. L'état du cluster affiche `applying` pour `ParameterApplyStatus`, tandis que les valeurs sont appliquées, puis `pending-reboot` une fois que les valeurs ont été appliquées. Après le redémarrage, les bases de données de votre cluster commencent à utiliser les nouvelles valeurs des paramètres. Pour plus d'informations sur le redémarrage des clusters, consultez Redémarrage d'un cluster.

> **Note**
>
> Le paramètre `wlm_json_configuration` contient certaines propriétés qui sont dynamiques et qui ne nécessitent pas de redémarrer les clusters associés pour que les modifications soient appliquées. Pour plus d'informations sur les propriétés dynamiques et statiques, consultez Propriétés WLM dynamiques et statiques.

La syntaxe suivante montre comment utiliser la commande `modify-cluster-parameter-group` pour configurer un paramètre. Vous spécifiez *`parameter_group_name`* et remplacez les deux *`parameter_name parameter_value`* par un paramètre réel à modifier et une valeur pour ce paramètre. Si vous voulez modifier plusieurs paramètres en même temps, séparez chaque ensemble de paramètre et de valeur du suivant avec un espace.

```
aws redshift modify-cluster-parameter-group --parameter-group-
name parameter_group_name --parameters
 ParameterName=parameter_name,ParameterValue=parameter_value
```

L'exemple suivant montre comment configurer les paramètres `statement_timeout` et `enable_user_activity_logging` pour le groupe de paramètres `myclusterparametergroup`.

> **Note**
>
> Pour des raisons de lisibilité, l'exemple est affiché sur plusieurs lignes, mais dans la réalité, il ne s' AWS CLI agit que d'une seule ligne.

```
aws redshift modify-cluster-parameter-group
--parameter-group-name myclusterparametergroup
```

```
--parameters ParameterName=statement_timeout,ParameterValue=20000
 ParameterName=enable_user_activity_logging,ParameterValue=true
```

Création d’une règle de surveillance de requête

Vous pouvez utiliser la console Amazon Redshift pour créer et modifier les règles de surveillance des requêtes WLM. Les règles de surveillance de requête font partie du paramètre de configuration WLM pour un groupe de paramètres. Si vous modifiez une règle de surveillance des requêtes (QMR), le changement se fait automatiquement sans qu'il soit nécessaire de modifier le cluster. Pour de plus amples informations, consultez Règles de surveillance de requête WLM.

Lorsque vous créez une règle, vous définissez son nom, un ou plusieurs prédicats, puis une action.

Lorsque vous enregistrez une configuration WLM qui comprend une règle, vous pouvez afficher le code JSON correspondant à la définition de règle dans le cadre du code JSON relatif au paramètre de configuration WLM.

Pour créer une règle de surveillance de requête

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Configurations, puis choisissez Gestion des charges de travail pour afficher la page Gestion des charges de travail.
3. Choisissez le groupe de paramètres que vous souhaitez modifier pour afficher la page des détails avec des onglets pour Paramètres et Gestion des charges de travail.
4. Choisissez l’onglet Gestion des charges de travail, puis choisissez Modifier les files d’attente des charges de travail pour modifier la configuration de la gestion de la charge de travail.
5. Ajoutez une nouvelle règle en utilisant un modèle prédéfini ou en la créant totalement.

   Pour utiliser un modèle prédéfini, procédez comme suit :

   1. Choisissez Ajouter une règle en utilisant un modèle dans le groupe Règles de surveillance des requêtes. La liste des modèles de règles s'affiche.
   2. Choisissez un ou plusieurs modèles de règle. Lorsque vous choisissez Enregistrer, WLM crée une règle pour chaque modèle que vous choisissez.
   3. Entrez ou validez les valeurs de la règle, notamment Noms des règles, Prédicats et Actions.

4. Choisissez Enregistrer.

Pour ajouter une nouvelle règle créée à partir de zéro, procédez comme suit :

1. Pour ajouter des prédicats supplémentaires, choisissez Ajouter un prédicat. Vous pouvez avoir jusqu'à trois prédicats pour chaque règle. Si l'ensemble des prédicats sont respectés, WLM déclenche l'action associée.
2. Choisissez une Action. A chaque règle correspond une action.
3. Choisissez Enregistrer.

Amazon Redshift génère votre paramètre de configuration WLM au format JSON et l'affiche dans la section JSON.

Suppression d'un groupe de paramètres

Vous pouvez supprimer un groupe de paramètres si vous n'en avez plus besoin et s'il n'est pas associé à un cluster. Vous ne pouvez supprimer que des groupes de paramètres personnalisés.

Pour supprimer un groupe de paramètres

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Configurations, puis choisissez Gestion des charges de travail pour afficher la page Gestion des charges de travail.
3. Dans le champ Groupes de paramètres, sélectionnez le groupe de paramètres à modifier.

> **Note**
>
> Vous ne pouvez pas supprimer le groupe de paramètres par défaut.

4. Choisissez Supprimer et confirmez la suppression du groupe de paramètres.

Intégrez Amazon Redshift à un AWS Partenaire

En utilisant Amazon Redshift, vous pouvez intégrer les AWS partenaires sur la console Amazon Redshift. Sur la page de détails du cluster, vous pouvez accélérer l'intégration de vos données dans votre entrepôt de données Amazon Redshift AWS grâce aux applications partenaires. Vous pouvez également joindre et analyser des données provenant de différentes sources avec les données existantes de votre cluster. Avant de terminer l'intégration avec Informatica, vous devez ajouter les adresses IP du partenaire à la liste du trafic entrant autorisé. Les AWS partenaires suivants peuvent s'intégrer à Amazon Redshift :

- Datacoral
- Etleap
- Fivetran
- SnapLogic
- Stitch
- Upsolver
- Matillion (aperçu)
- Sisense (aperçu)
- Thoughtspot

AWS Les partenaires peuvent s'intégrer à Amazon Redshift à l'aide des opérations d'API AWS CLI ou d'Amazon Redshift. Pour plus d'informations, consultez la référence de la commande AWS CLI ou la référence de l'API Amazon Redshift.

Utilisez la procédure suivante pour intégrer un cluster à un AWS partenaire.

Pour intégrer un cluster Amazon Redshift à un AWS Partenaire

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters.
3. Choisissez le cluster de bases de données à utiliser.
4. Choisissez Add partner integration (Ajouter une intégration partenaire). La page Choisir un partenaire s'ouvre avec des informations sur les AWS partenaires disponibles.

5. Choisissez un AWS partenaire, puis cliquez sur Suivant.

   Plus de détails sur le AWS partenaire choisi apparaissent, ainsi que des détails sur le cluster que vous intégrez. La section Détails du cluster inclut les informations que vous fournissez sur le site Web du AWS partenaire, telles que l'identifiant du cluster, le point de terminaison, le nom de la base de données et le nom d'utilisateur (qui est un nom d'utilisateur de base de données). Ces informations sont transmises au partenaire que vous avez choisi.
6. Choisissez Ajouter un partenaire pour ouvrir le site Web du AWS partenaire.
7. Configurez l'intégration de votre cluster Amazon Redshift sur le site web du partenaire. Sur le site web du partenaire, vous pouvez sélectionner et configurer les sources de données chargées dans votre cluster Amazon Redshift. Vous pouvez également définir des transformations supplémentaires d'extraction, de chargement et de transformation pour traiter vos données d'entreprise, les joindre à d'autres jeux de données et créer des vues consolidées pour l'analyse et les rapports.

Vous pouvez consulter et gérer les intégrations de AWS partenaires depuis l'onglet Propriétés des détails du cluster. La section Intégrations répertorie le nom du partenaire que vous pouvez utiliser pour créer un lien vers le site Web du AWS partenaire, le statut de l'intégration, la base de données qui reçoit les données et la dernière connexion réussie susceptible d'avoir mis à jour le cluster.

Les valeurs de statut possibles sont les suivantes :

- Actif : le AWS partenaire peut se connecter au cluster et effectuer les tâches configurées.
- Inactif : l'intégration AWS Partner n'existe pas.
- Échec de l'exécution : le AWS partenaire peut se connecter au cluster mais ne peut pas effectuer les tâches configurées.
- Échec de connexion : le AWS partenaire ne peut pas se connecter au cluster.

Une fois que vous avez supprimé une intégration de AWS partenaire d'Amazon Redshift, les données continuent de circuler dans votre cluster. Achevez la suppression sur le site web du partenaire.

Chargement de données avec AWS partenaires

Outre l'intégration d'un partenaire à un cluster Amazon Redshift, vous pouvez également déplacer des données provenant de plus de 30 sources vers votre cluster Amazon Redshift à l'aide des outils de chargement de données de notre partenaire. Auparavant, vous devez ajouter les adresses IP

du partenaire (ci-dessous) à la liste des règles entrantes autorisées. Pour plus d'informations sur l'ajout de règles à un groupe de sécurité Amazon EC2, consultez Autorisation du trafic entrant pour vos instances dans le Guide de l'utilisateur Amazon EC2. Notez que bien que l'outil Informatica Data Loader soit gratuit, des frais d'entrée de données peuvent s'appliquer en fonction des sources de données et des cibles que vous choisissez.

Vous pouvez charger des données à partir des partenaires suivants :

- Informatica

Pour charger des données dans un cluster Amazon Redshift avec un partenaire

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez AWS l'intégration des partenaires, puis le partenaire avec lequel vous souhaitez intégrer votre cluster.
3. Choisissez Complete <partner-name> integration (Terminer l'intégration de <nom-du-partenaire>). Vous serez redirigé vers le site d'intégration du partenaire.
4. Saisissez les informations nécessaires sur le site du partenaire et terminez l'intégration.

Nœuds réservés

Dans AWS, les frais que vous facturez pour utiliser Amazon Redshift sont basés sur les nœuds de calcul. Chaque nœud de calcul est facturé à un taux horaire. Le taux horaire varie en fonction de critères tels que la région, le type de nœud et si le nœud reçoit une tarification de nœud à la demande ou une tarification de nœud réservé.

On-demand la tarification des nœuds est l'option la plus onéreuse mais la plus flexible d'Amazon Redshift. Avec les tarifs à la demande, vous ne payez que les nœuds de calcul que vous avez dans un cluster en cours d'exécution. Si vous arrêtez ou supprimez un cluster, vous n'êtes plus facturé pour les nœuds de calcul qui étaient dans ce cluster. Vous êtes facturé uniquement pour les nœuds de calcul que vous utilisez, et pas plus. Le taux horaire qui vous est facturé pour chaque nœud de calcul varie en fonction de facteurs tels que la région et le type de nœud.

La tarification de nœud réservé est moins onéreuse que la tarification à la demande, car les nœuds de calcul sont facturés à des tarifs horaires réduits. Cependant, pour recevoir ces tarifs réduits, vous devez acheter des offres de nœuds réservés. Lorsque vous achetez une offre, vous faites une réservation. La réservation définit un tarif réduit pour chaque nœud que vous réservez pour la durée de la réservation. Le tarif réduit d'une offre varie en fonction de critères tels que la région, le type de nœud, la durée et l'option de paiement.

Vous pouvez désigner un nœud comme nœud réservé en appelant l'opération d'API `PurchaseReservedNodeOffering` ou en choisissant Acheter des nœuds réservés sur la console Amazon Redshift. Lorsque vous achetez un nœud réservé, vous devez spécifier une AWS région, un type de nœud, une durée, une quantité de nœuds et un type d'offre pour le type de nœud réservé applicable. Le nœud réservé ne peut être utilisé que dans la AWS région désignée.

Cette rubrique explique ce que sont les offres de nœuds réservés et comment vous pouvez les acheter afin de réduire le coût d'exécution de vos clusters Amazon Redshift. Cette rubrique présente les tarifs en termes généraux tels que les tarifs à la demande ou les tarifs réduits afin que vous puissiez comprendre les concepts de tarification et la façon dont la tarification affecte la facturation. Pour plus d'informations sur les tarifs spécifiques, consultez la tarification Amazon Redshift.

Offres relatives aux nœuds réservés

Si vous prévoyez que votre cluster Amazon Redshift s'exécute en continu pendant une période prolongée, envisagez d'acquérir des offres de nœuds réservés. Ces offres fournissent des économies

importantes sur la tarification à la demande, mais nécessitent que vous réserviez des nœuds de calcul et que vous vous engagiez à payer ces nœuds pendant une durée d'un an ou de trois ans.

Les nœuds réservés sont un concept de facturation strictement utilisé pour déterminer à quel taux les nœuds vous sont facturés. La réservation d'un nœud ne crée pas de fait de nœuds pour vous. Vous êtes facturé pour les nœuds réservés quelle que soit l'utilisation, ce qui signifie que vous devez payer chaque nœud que vous réservez pour la durée de la réservation, que vous ayez ou pas des nœuds dans un cluster en cours d'exécution auquel le tarif réduit s'applique.

Dans la phase d'évaluation de votre projet ou lorsque vous développez une preuve de concept, la tarification à la demande vous donne la possibilité de payer à la demande, de payer seulement pour ce que vous utilisez et de cesser de payer à tout moment en arrêtant ou en supprimant des clusters. Une fois que vous avez établi les besoins de votre environnement de production et commencé la phase de mise en œuvre, vous devez envisager de réserver des nœuds de calcul en achetant une ou plusieurs offres.

Une offre peut s'appliquer à un ou plusieurs nœuds de calcul. Vous spécifiez le nombre de nœuds de calcul à réserver lorsque vous achetez l'offre. Vous pouvez choisir d'acheter une offre pour plusieurs nœuds de calcul, ou choisir d'acheter plusieurs offres et spécifier un certain nombre de nœuds de calcul dans chaque offre.

Par exemple, les actions suivantes sont des façons valides d'acheter une offre pour les trois nœuds de calcul :

- Acheter une offre et spécifier trois nœuds de calcul.
- Acheter deux offres, et spécifier un nœud de calcul pour la première offre et deux nœuds de calcul pour la deuxième offre.
- Acheter trois offres, et spécifier un nœud de calcul pour chacune des offres.

Comparaison de prix entre les offres de nœuds réservés

Amazon Redshift propose plusieurs options de paiement pour les offres. L'option de paiement que vous choisissez affecte l'échéance et le tarif réduit qui vous est facturé pour la réservation. Plus vous payez à l'avance, plus importantes seront les économies.

Les options de paiement suivantes sont disponibles pour les offres. Les offres sont répertoriées dans l'ordre des économies les moins importantes aux plus importantes par rapport aux tarifs à la demande.

> **Note**
>
> Le taux horaire applicable vous est facturé pour chaque heure de la durée spécifiée de la réservation, que vous utilisiez le nœud réservé ou pas. L'option de paiement détermine simplement la fréquence des paiements et la remise à appliquer. Pour plus d'informations, consultez Offres relatives aux nœuds réservés.

Option de paiement	Calendrier de paiement	Comparaison des économies	Duration	Frais initiaux	Frais mensuels récurrents
Sans frais initiaux	Versements mensuels pendant la durée de la réservation. Aucun paiement initial.	Remise de 20 % environ par rapport aux tarifs à la demande.	One-year ou mandat de trois ans	Aucune	Oui
Frais initiaux partiels	Paiement partiel initial, puis versements mensuels pendant la durée de la réservation.	De 41 % à 73 % de réduction en fonction de la durée.	One-year ou mandat de trois ans	Oui	Oui
Tous les frais initiaux	Paiement initial complet de la réservation. Aucuns frais mensuels.	De 42 % à 76 % de réduction en fonction de la durée.	One-year ou mandat de trois ans	Oui	Aucune

Les options et durées spécifiques sont soumises à disponibilité.

> **Note**
>
> Si vous avez déjà acheté des offres à utilisation intensive pour Amazon Redshift, l'offre comparable est l'offre initiale partielle.

Fonctionnement des nœuds réservés

Avec les offres de nœuds réservés, vous payez selon les conditions de paiement, comme décrit dans la section précédente. Vous payez de cette façon que vous ayez déjà un cluster en cours d'exécution ou que vous lanciez un cluster après avoir effectué une réservation.

Lorsque vous achetez une offre, votre réservation a le statut en attente de paiement jusqu'à ce que la réservation soit traitée. Si le traitement de la réservation échoue, le statut affiché est échec du paiement et vous pouvez réessayer le processus. Une fois que votre réservation a été traitée avec succès, son statut devient active. Le tarif réduit applicable de votre réservation n'est pas appliqué à votre facture tant que le statut n'est pas active. Après expiration de la durée de la réservation, le statut devient retires mais vous pouvez continuer à accéder aux informations sur la réservation à des fins d'historique. Quand une réservation a le statut retired, vos clusters continuent à s'exécuter, mais vous pouvez être facturé au tarif à la demande, sauf si vous avez une autre réservation qui applique une tarification réduite aux nœuds.

Les nœuds réservés sont spécifiques à la région dans laquelle vous achetez l'offre. Si vous achetez une offre à l'aide de la console Amazon Redshift, sélectionnez la AWS région dans laquelle vous souhaitez acheter une offre, puis terminez le processus de réservation. Si vous achetez une offre par programmation, la région est déterminée par le point de terminaison Amazon Redshift auquel vous vous connectez. Pour plus d'informations sur les régions Amazon Redshift, accédez à Régions et points de terminaison dans le Référence générale d'Amazon Web Services.

Pour garantir que le tarif réduit est appliqué à tous les nœuds lorsque vous lancez un cluster, assurez-vous que la région, le type de nœud et le nombre de nœuds que vous sélectionnez correspondent à une ou plusieurs réservations actives. Sinon, vous serez facturé au tarif à la demande pour les nœuds qui ne correspondent pas à une réservation active.

Dans un cluster en cours d'exécution, si vous dépassez le nombre de nœuds que vous avez réservés, vous commencez à accumuler les frais pour ces nœuds supplémentaires au tarif à la demande. Cette accumulation signifie qu'il est possible que différents tarifs vous soient facturés pour les nœuds du même cluster selon le nombre de nœuds que vous avez réservés. Vous pouvez

acheter une autre offre afin de couvrir ces nœuds supplémentaires, et le tarif réduit est alors appliqué à ces nœuds pour le reste de la durée une fois que la réservation a pour statut active.

Si vous redimensionnez votre cluster en un type de nœud différent et que vous n'avez pas réservé de nœuds de ce type, vous serez facturé au tarif à la demande. Vous pouvez acheter une autre offre avec le nouveau type de nœud si vous souhaitez obtenir des tarifs réduits pour votre cluster redimensionné. Cependant, vous continuez à payer pour la réservation d'origine jusqu'à ce que l'expiration de sa durée. Si vous avez besoin de modifier vos réservations avant leur expiration, créez une demande de support à l'aide de la console AWS.

> **Note**
>
> La console indique le nombre de nœuds réservés utilisés et non utilisés. Toutefois, la console indique uniquement le nombre de nœuds utilisés par le compte utilisateur actuel. Si un autre compte utilisateur du même compte payeur utilise des nœuds, la console indique que ces nœuds ne sont pas utilisés.
> Exemple
>
> - Un compte payeur réserve 20 nœuds
> - Le compte utilisateur actuel utilise six nœuds
> - Un autre compte utilisateur sous le même compte payeur utilise également six nœuds
>
> Dans cet exemple, la console affiche uniquement six nœuds utilisés et quatorze nœuds inutilisés.

Nœuds réservés et facturation consolidée

Les avantages de tarification des nœuds réservés sont partagés lorsque le compte d'achat fait partie d'un ensemble de comptes facturés réunis sous un même compte payeur de facturation consolidée. Le coût horaire pour tous les sous-comptes est regroupé dans le compte payeur tous les mois. Cette fonctionnalité est généralement utile pour les sociétés disposant de plusieurs équipes ou groupes fonctionnels. Ensuite, la logique standard des nœuds réservés est appliquée pour calculer le montant de la facture. Pour plus d'informations, consultez la section Facturation consolidée dans le Guide de AWS Billing l'utilisateur.

Points à prendre en compte avant de modifier le type de nœud sur un cluster qui utilise des instances réservées

Vous pouvez modifier le type de nœud d'un cluster en modifiant la famille de nœuds ou la taille des nœuds à l'aide de la fonction de redimensionnement (élastique ou classique). Lorsque vous modifiez le type de nœud, les achats de nœuds réservés associés au cluster ne changent pas automatiquement. Les réservations existantes restent liées au type de nœud d'origine. Ces réservations continuent à vous être facturées jusqu'à la fin de leur durée. En attendant, les nœuds du nouveau type peuvent être facturés au tarif à la demande.

Pour cette raison, pour modifier vos instances réservées, nous vous recommandons de contacter l'équipe chargée de votre AWS compte ou le service d'assistance à la AWS facturation avant de modifier le type de nœud d'un cluster qui utilise des nœuds réservés. Ils peuvent vous guider de manière appropriée.

Exemples de nœuds réservés

Les scénarios de cette section montrent comment les nœuds accumulent les frais en fonction des tarifs à la demande et des tarifs réduits en utilisant les informations de réservation suivantes :

- Région : USA Ouest (Oregon)
- Type de nœuds : ra3.xlplus
- Option de paiement : aucun paiement initial
- Durée : une année
- Nombre de nœuds réservés : 16

Exemple 1

Vous avez un cluster dans la région USA Ouest (Oregon) avec 20 nœuds.

Dans ce scénario, 16 des nœuds reçoivent le tarif réduit de la réservation, mais les 4 autres nœuds du cluster sont facturés au tarif à la demande.

Exemple 2

Vous avez un cluster dans la région USA Ouest (Oregon) avec 12 nœuds.

Dans ce scénario, les 12 nœuds du cluster bénéficient du tarif réduit de la réservation. Cependant, vous payez aussi les nœuds réservés restants de la réservation même si vous n'avez pas actuellement un cluster en cours d'exécution auquel ils s'appliquent.

Exemple 3

Vous avez un cluster dans la région USA Ouest (Oregon) avec 12 nœuds. Vous exécutez le cluster pendant plusieurs mois avec cette configuration, puis avez besoin d'ajouter des nœuds au cluster. Vous redimensionnez le cluster, en choisissant le même type de nœud et en spécifiant un total de 16 nœuds.

Dans ce scénario, vous êtes facturé au tarif réduit de 16 nœuds. Vos coûts demeurent les mêmes pendant la durée totale de l'année, car le nombre de nœuds que vous avez dans le cluster est égal au nombre de nœuds que vous avez réservés.

Exemple 4

Vous avez un cluster dans la région USA Ouest (Oregon) avec 16 nœuds. Vous exécutez le cluster pendant plusieurs mois avec cette configuration, puis avez besoin d'ajouter des nœuds. Vous redimensionnez le cluster, en choisissant le même type de nœud et en spécifiant un total de 20 nœuds.

Dans ce scénario, vous êtes facturé au tarif réduit pour tous les nœuds antérieurs au redimensionnement. Après le redimensionnement, vous êtes facturé au tarif réduit pour 16 des nœuds pendant le reste de l'année et vous êtes facturé au tarif à la demande pour les 4 nœuds supplémentaires que vous avez ajoutés au cluster.

Exemple 5

Vous avez deux clusters dans la région USA Ouest (Oregon). L'un des clusters a 6 nœuds et l'autre 10 nœuds.

Dans ce scénario, vous êtes facturé au tarif réduit pour tous les nœuds, car le nombre total de nœuds des deux clusters est égal au nombre de nœuds que vous avez réservés.

Exemple 6

Vous avez deux clusters dans la région USA Ouest (Oregon). L'un des clusters a 4 nœuds et l'autre 6 nœuds.

Dans ce scénario, vous êtes facturé au tarif réduit pour les 10 nœuds que vous avez dans les clusters en cours d'exécution, et vous payez également le tarif réduit pour les 6 nœuds supplémentaires que vous avez réservés, même si vous n'avez actuellement aucun cluster en cours d'exécution auquel ils s'appliquent.

Achat d’un nœud réservé

Vous pouvez utiliser le Console de gestion AWS ou AWS CLI pour acheter des offres de nœuds réservés et pour consulter les réservations en cours et passées.

Console de gestion AWS

Pour acheter un nœud réservé

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters, puis choisissez Nœuds réservés pour afficher la liste des nœuds réservés.
3. Choisissez Acheter des nœuds réservés pour afficher la page permettant de choisir les propriétés du nœud que vous souhaitez acheter.
4. Entrez les propriétés du nœud, puis choisissez Acheter des nœuds réservés.

Une fois que vous achetez une offre, la liste Reserved Node affiche vos réservations et les détails de chacune d'elles, tels que le type de nœud, le nombre de nœuds et l'état de la réservation. Pour plus d'informations sur les détails de la réservation, consultez Fonctionnement des nœuds réservés.

Pour mettre à niveau un nœud réservé, utilisez l’ AWS CLI.

Vous ne pouvez pas convertir tous les types de nœuds en nœuds réservés, et il est également possible qu'un nœud réservé existant ne soit pas disponible pour le renouvellement. Cela peut être dû au fait que le type de nœud a été abandonné. Contactez le support client pour renouveler un type de nœud abandonné.

AWS CLI

Pour mettre à niveau une réservation de nœud réservé avec le AWS CLI

1. Obtenez la ReservedNodeOfferingID liste des offres qui répondent à vos exigences en matière de type de paiement, de durée et de frais. L'exemple suivant illustre cette étape :

```
aws redshift get-reserved-node-exchange-offerings --reserved-node-id xxxxxxxx-
xxxx-xxxx-xxxx-xxxxxxxxxxxx
{
    "ReservedNodeOfferings": [
        {
            "Duration": 31536000,
            "ReservedNodeOfferingId": "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy",
            "UsagePrice": 0.0,
            "NodeType": "dc2.large",
            "RecurringCharges": [
                {
                    "RecurringChargeFrequency": "Hourly",
                    "RecurringChargeAmount": 0.2
                }
            ],
            "CcurrencyCode": "USD",
            "OfferingType": "No Upfront",
            "ReservedNodeOfferingType": "Regular",
            "FixedPrice": 0.0
        }
    ]
}
```

2. Appelez `accept-reserved-node-exchange` et fournissez l'ID du nœud réservé DC1 que vous souhaitez échanger, ainsi que celui que ReservedNodeOfferingID vous avez obtenu à l'étape précédente.

   L'exemple suivant illustre cette étape :

```
aws redshift accept-reserved-node-exchange --reserved-node-id xxxxxxxx-xxxx-
xxxx-xxxx-xxxxxxxxxxxx --target-reserved-node-offering-id yyyyyyyy-yyyy-yyyy-
yyyy-yyyyyyyyyyyy
{
    "ExchangedReservedNode": {
```

```
        "UsagePrice": 0.0,
        "OfferingType": "No Upfront",
        "State": "exchanging",
        "FixedPrice": 0.0,
        "CurrencyCode": "USD",
        "ReservedNodeId": "zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzz",
        "NodeType": "dc2.large",
        "NodeCount": 1,
        "RecurringCharges": [
            {
                "RecurringChargeFrequency": "Hourly",
                "RecurringChargeAmount": 0.2
            }
        ],
        "ReservedNodeOfferingType": "Regular",
        "StartTime": "2018-06-27T18:02:58Z",
        "ReservedNodeOfferingId": "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyyy",
        "Duration": 31536000
    }
}
```

Vous pouvez vérifier que l'échange est terminé en appelant describe-reserved-nodes et en vérifiant la valeur de `Node type`.

Sécurité dans Amazon Redshift

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

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. L'efficacité de notre sécurité est régulièrement testée et vérifiée par des auditeurs tiers dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Redshift, veuillez consulter Services AWS concernés par le programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre organisation, et la législation et la réglementation applicables.

L'accès aux ressources Amazon Redshift est contrôlé à quatre niveaux :

- Gestion des clusters : la capacité à créer, configurer et supprimer des clusters est contrôlée par les autorisations accordées à l'utilisateur ou au compte associé à vos informations d'identification AWS de sécurité. Les utilisateurs disposant des autorisations appropriées peuvent utiliser l' Console de gestion AWS interface de programmation AWS Command Line Interface (CLI) ou l'interface de programmation d'applications (API) Amazon Redshift pour gérer leurs clusters. Cet accès est géré à l'aide de politiques IAM.

> **Important**
>
> Amazon Redshift dispose d'un ensemble de bonnes pratiques pour la gestion des autorisations, des identités et des accès sécurisés. Nous vous recommandons de vous familiariser avec ces dernières lorsque vous commencerez à utiliser Amazon Redshift. Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Redshift.

- Connectivité au cluster : les groupes de sécurité Amazon Redshift spécifient les AWS instances autorisées à se connecter à un cluster Amazon Redshift au format Inter-Domain Classless Routing (CIDR). Pour plus d'informations sur la création de groupes de sécurité Amazon Redshift, Amazon EC2 et Amazon VPC, ainsi que leur association à des clusters, consultez la section Groupes de sécurité Amazon Redshift.
- Accès à la base de données : la possibilité d'accéder aux objets de base de données, tels que les tables et les vues, est contrôlée par les comptes d'utilisateur dans la base de données Amazon Redshift. Les utilisateurs peuvent uniquement accéder aux ressources de la base de données auxquelles leurs comptes d'utilisateur ont l'autorisation d'accéder. Vous créez ces comptes d'utilisateur Amazon Redshift et gérez les autorisations à l'aide des instructions SQL CREATE USER, CREATE GROUP, GRANT et REVOKE. Pour plus d'informations, consultez Gestion de la sécurité de la base de données dans le Guide du développeur de base de données Amazon Redshift.
- Informations d'identification temporaires de base de données et authentification unique : en plus de créer et de gérer les utilisateurs de base de données à l'aide des commandes SQL, telles que CREATE USER et ALTER USER, vous pouvez configurer votre client SQL avec des pilotes JDBC ou ODBC Amazon Redshift personnalisés. Ces pilotes gèrent la création d'utilisateurs de base de données et de mots de passe temporaires dans le cadre du processus de connexion à une base de données.

  Les pilotes authentifient les utilisateurs de base de données sur la base de l'authentification d' Gestion des identités et des accès AWS (IAM). Si vous gérez déjà les identités des utilisateurs en dehors de AWS, vous pouvez utiliser un fournisseur d'identité (IdP) compatible SAML 2.0 pour gérer l'accès aux ressources Amazon Redshift. Vous utilisez un rôle IAM pour configurer votre IdP AWS et pour permettre à vos utilisateurs fédérés de générer des informations d'identification de base de données temporaires et de se connecter aux bases de données Amazon Redshift. Pour de plus amples informations, veuillez consulter Utilisation de l'authentification IAM pour générer des informations d'identification de l'utilisateur de base de données.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Amazon Redshift. Les rubriques suivantes vous montrent comment configurer Amazon Redshift pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Amazon Redshift.

Rubriques

- Protection des données dans Amazon Redshift
- Identity and Access Management dans Amazon Redshift
- Gestion des mots de passe d'administration Amazon Redshift à l'aide de AWS Secrets Manager
- Journalisation et surveillance dans Amazon Redshift
- Validation de la conformité pour Amazon Redshift
- Résilience d'Amazon Redshift
- Sécurité de l'infrastructure dans Amazon Redshift
- Configuration et analyse des vulnérabilités dans Amazon Redshift

Protection des données dans Amazon Redshift

Le modèle de responsabilité AWS partagée (modèle de) s'applique à la protection des données dans Amazon Redshift. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la FAQ sur la confidentialité des données et les . Pour plus d’informations sur la protection des données en Europe, consultez le Centre du règlement général sur la protection des données (RGPD).

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 Amazon Redshift ou une autre entreprise à Services AWS l'aide de la console, de l'API ou AWS des AWS CLI SDK. 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

La protection des données consiste à protéger les données en transit (lorsqu'elles se déplacent vers et depuis Amazon Redshift) et au repos (lorsqu'elles sont stockées sur des disques dans les centres de données Amazon Redshift). Vous pouvez protéger les données en transit en utilisant SSL ou un chiffrement côté client. Vous disposez des options suivantes pour protéger les données au repos dans Amazon Redshift.

- Utilisation du chiffrement côté serveur – Vous demandez à Amazon Redshift de chiffrer vos données avant de les enregistrer sur les disques dans ses centres de données et de les déchiffrer lorsque vous téléchargez les objets.
- Utilisation du chiffrement côté client – Vous pouvez chiffrer les données côté client et charger ces dernières sur Amazon Redshift. Dans ce cas, vous gérez le processus de chiffrement, les clés de chiffrement et les outils associés.

Chiffrement au repos

Server-side le chiffrement concerne le chiffrement des données au repos, c'est-à-dire qu'Amazon Redshift chiffre éventuellement vos données au fur et à mesure qu'il les écrit dans ses centres de données et les déchiffre pour vous lorsque vous y accédez. Tant que vous authentifiez votre

demande et que vous avez des autorisations d'accès, il n'y a aucune différence dans la manière dont vous accédez aux données chiffrées ou déchiffrées.

Amazon Redshift protège les données au repos grâce au chiffrement. Vous pouvez éventuellement protéger toutes les données stockées sur les disques d'un cluster et toutes les sauvegardes dans Amazon S3 avec Advanced Encryption Standard AES-256.

Pour gérer les clés utilisées pour chiffrer et déchiffrer vos ressources Amazon Redshift, vous utilisez ().AWS Key Management ServiceAWS KMS AWS KMS combine du matériel et des logiciels sécurisés et hautement disponibles pour fournir un système de gestion des clés adapté au cloud. À l'aide de AWS KMS, vous pouvez créer des clés de chiffrement et définir les politiques qui contrôlent la manière dont ces clés peuvent être utilisées. AWS KMS prend en charge AWS CloudTrail, afin que vous puissiez auditer l'utilisation des clés pour vérifier que les clés sont utilisées de manière appropriée. Vous pouvez utiliser vos AWS KMS clés en combinaison avec Amazon Redshift et les services pris en charge AWS . Pour obtenir la liste des services compatibles AWS KMS, consultez la section Comment les AWS services sont utilisés AWS KMS dans le guide du AWS Key Management Service développeur.

Si vous choisissez de gérer le mot de passe administrateur de votre cluster provisionné ou de votre espace de noms sans serveur en utilisant, Amazon AWS Secrets Manager Redshift accepte également une clé AWS KMS supplémentaire qui AWS Secrets Manager permet de chiffrer vos informations d'identification. Cette clé supplémentaire peut être une clé générée automatiquement ou une clé personnalisée que vous fournissez. AWS Secrets Manager

L'éditeur de requête Amazon Redshift v2 stocke en toute sécurité les informations saisies dans l'éditeur de requête comme suit :

- L'Amazon Resource Name (ARN) de la clé KMS à utiliser pour chiffrer les données de l'éditeur de requête v2.
- Informations de connexion à la base de données.
- Les noms et le contenu des fichiers et des dossiers.

L'éditeur de requête Amazon Redshift v2 chiffre les informations à l'aide d'un chiffrement de niveau bloc avec votre clé KMS ou la clé KMS du compte de service. Le chiffrement de vos données Amazon Redshift est contrôlé par les propriétés de votre cluster Amazon Redshift.

Rubriques

- Chiffrement de base de données Amazon Redshift

Chiffrement de base de données Amazon Redshift

Dans Amazon Redshift, votre base de données est chiffrée par défaut pour protéger vos données au repos. Le chiffrement de base de données s'applique au cluster et à ses instantanés.

Vous pouvez modifier un cluster non chiffré pour utiliser le chiffrement AWS Key Management Service (AWS KMS). Pour ce faire, vous pouvez utiliser une clé AWS détenue ou une clé gérée par le client. Lorsque vous modifiez votre cluster pour activer le AWS KMS chiffrement, Amazon Redshift migre automatiquement vos données vers un nouveau cluster chiffré. Les instantanés créés à partir du cluster chiffré sont également chiffrés. Vous pouvez également migrer un cluster chiffré vers un cluster non chiffré en modifiant le cluster et en changeant l'option Chiffrer la base de données. Pour plus d'informations, consultez Modification du chiffrement d'un cluster.

Bien que vous puissiez toujours transformer le cluster chiffré par défaut en cluster non chiffré après l'avoir créé, nous vous recommandons de conserver le chiffrement d'un cluster contenant des données sensibles. En outre, vous pouvez être contraint d'utiliser le chiffrement en fonction des directives ou règlements régissant vos données. Par exemple, la norme de sécurité des données du secteur des cartes de paiement (PCI DSS), la Sarbanes-Oxley loi (SOX), la Health Insurance Portability and Accountability Act (HIPAA) et d'autres réglementations similaires fournissent des directives pour le traitement de types spécifiques de données.

Amazon Redshift utilise une hiérarchie de clés de chiffrement pour chiffrer la base de données. Vous pouvez utiliser AWS Key Management Service (AWS KMS) ou un module de sécurité matérielle (HSM) pour gérer les clés de chiffrement de niveau supérieur dans cette hiérarchie. Le processus qu'utilise Amazon Redshift pour le chiffrement diffère en fonction de la façon dont vous gérez les clés. Amazon Redshift s'intègre automatiquement à un HSM AWS KMS , mais pas à celui-ci. Lorsque vous utilisez un HSM, vous devez utiliser des certificats client et de serveur pour configurer une connexion approuvée entre Amazon Redshift et votre HSM.

> **Important**
>
> Amazon Redshift peut perdre l'accès à la clé KMS pour un cluster alloué ou un espace de noms sans serveur lorsque vous désactivez la clé KMS gérée par le client. Dans ces cas, Amazon Redshift effectue une sauvegarde de l'entrepôt de données Amazon Redshift et la met dans l'état `inaccessible-kms-key` pendant 14 jours. Si vous restaurez la clé KMS pendant cette période, Amazon Redshift rétablira l'accès et l'entrepôt fonctionnera normalement. Si la période de 14 jours prend fin sans que la clé KMS soit restaurée, Amazon Redshift supprimera l'entrepôt de données. Lorsqu'un entrepôt est en état `inaccessible-kms-key`, il présente les caractéristiques suivantes :

- Vous ne pouvez exécuter aucune requête sur l'entrepôt de données.
- Si l'entrepôt de données est l'entrepôt producteur d'une unité de partage des données, vous ne pouvez pas exécuter de requêtes de partage de données à partir d'entrepôts de consommateurs.
- Vous ne pouvez pas créer d'instantanés entre régions.

Pour plus d'informations sur la restauration d'une clé KMS désactivée, consultez la section Activer et désactiver les clés dans le Guide du développeur AWS Key Management Service . Si la clé KMS de l'entrepôt a été supprimée, vous pouvez utiliser la sauvegarde pour créer un nouvel entrepôt de données avant que l'entrepôt en état `inaccessible-kms-key` ne soit supprimé.

Améliorations du processus de chiffrement pour améliorer les performances et la disponibilité

Chiffrement avec des nœuds RG et RA3

Les mises à jour apportées au processus de chiffrement pour les nœuds RG et RA3 ont considérablement amélioré l'expérience. Les requêtes de lecture et d'écriture peuvent être exécutées au cours du processus avec un impact moindre sur les performances du chiffrement. De plus, le chiffrement se termine beaucoup plus rapidement. Les étapes du processus mises à jour incluent une opération de restauration et la migration des métadonnées du cluster vers un cluster cible. L'expérience améliorée s'applique aux types de chiffrement tels que AWS KMS, par exemple. Lorsque vous disposez de volumes de données de l'ordre du pétaoctet, l'opération a été réduite de plusieurs semaines à quelques jours.

Avant de chiffrer votre cluster, si vous prévoyez de continuer à exécuter des charges de travail de base de données, vous pouvez améliorer les performances et accélérer le processus en ajoutant des nœuds avec un redimensionnement élastique. Vous ne pouvez pas utiliser le redimensionnement élastique lorsque le chiffrement est en cours, alors faites-le avant de chiffrer. Notez que l'ajout de nœuds entraîne généralement des coûts plus élevés.

Chiffrement avec d'autres types de nœuds

Lorsque vous chiffrez un cluster avec des nœuds DC2, vous n'êtes pas en mesure d'exécuter des requêtes d'écriture, comme avec les nœuds RG ou RA3. Seules les requêtes de lecture peuvent être exécutées.

Notes d'utilisation pour le chiffrement avec les nœuds RG et RA3

Les informations et ressources suivantes vous aident à vous préparer au chiffrement et à surveiller le processus.

- Exécution de requêtes après le démarrage du chiffrement : une fois le chiffrement démarré, les lectures et les écritures sont disponibles en quinze minutes environ. La durée du processus de chiffrement complet dépend de la quantité de données sur le cluster et des niveaux de charge de travail.
- Combien de temps dure le chiffrement ? – Le temps nécessaire pour chiffrer vos données dépend de plusieurs facteurs, notamment du nombre de charges de travail en cours d'exécution, des ressources de calcul utilisées, du nombre de nœuds et du type de nœuds. Nous vous recommandons d'effectuer d'abord le chiffrement dans un environnement de test. En règle générale, si vous travaillez avec des volumes de données en pétaoctets, le chiffrement peut prendre entre 1 et 3 jours.
- Comment savoir si le chiffrement est terminé ? — Une fois le chiffrement activé, la fin du premier instantané confirme que le chiffrement est terminé.
- Annulation du chiffrement : si vous devez annuler l'opération de chiffrement, la meilleure méthode consiste à effectuer une restauration à partir de la sauvegarde la plus récente effectuée avant le lancement du chiffrement. Vous devrez réappliquer toutes les nouvelles mises à jour (updates/deletes/inserts) après la dernière sauvegarde.
- Exécution d'une restauration de table : notez que vous ne pouvez pas restaurer une table d'un cluster non chiffré vers un cluster chiffré.
- Chiffrement d'un cluster à nœud unique : le chiffrement d'un cluster à nœud unique présente des limites de performances. Cela prend plus de temps que le chiffrement pour un cluster multi-nœuds.
- Création d'une sauvegarde après chiffrement : lorsque vous chiffrez les données de votre cluster, aucune sauvegarde n'est créée tant que le cluster n'est pas entièrement chiffré. Le temps que cela prend peut varier. La durée de la sauvegarde peut aller de quelques heures à plusieurs jours, selon la taille du cluster. Une fois le chiffrement terminé, il peut s'écouler un certain temps avant que vous puissiez créer une sauvegarde.

  Notez que, puisqu'une opération de sauvegarde et de restauration a lieu pendant le processus de chiffrement, les tables ou les vues matérialisées créées avec `BACKUP NO` ne sont pas conservées. Pour plus d'informations, consultez CREATE TABLE ou CREATE MATERIALIZED VIEW.

Rubriques

- Chiffrement en utilisant AWS KMS
- Chiffrement à l’aide de modules de sécurité matérielle
- Rotation des clés de chiffrement
- Modification du chiffrement d’un cluster
- Migration vers un cluster HSM-encrypted
- Rotation des clés de chiffrement

Chiffrement en utilisant AWS KMS

Lorsque vous optez AWS KMS pour la gestion des clés avec Amazon Redshift, il existe une hiérarchie à quatre niveaux de clés de chiffrement. Ces clés, par ordre hiérarchique, sont la clé racine, une clé de chiffrement du cluster (CEK), une clé de chiffrement de base de données (DEK) et les clés de chiffrement des données.

Lorsque vous lancez votre cluster, Amazon Redshift renvoie une liste de ceux AWS KMS keys qu'Amazon Redshift ou AWS votre compte a créés ou dans lesquels Amazon Redshift est autorisé à utiliser. AWS KMS Vous sélectionnez une clé KMS en guise de clé racine dans la hiérarchie de chiffrement.

Par défaut, Amazon Redshift sélectionne une clé propre générée automatiquement comme AWS clé racine pour votre AWS compte à utiliser dans Amazon Redshift.

Si vous ne souhaitez pas utiliser la clé par défaut, vous devez disposer (ou créer) une clé KMS gérée par le client séparément AWS KMS avant de lancer votre cluster dans Amazon Redshift. Les clés gérées par le client vous donnent davantage de flexibilité, en vous permettant notamment de créer, d'effectuer la rotation, de désactiver et de définir le contrôle d'accès, ainsi que de contrôler les clés de chiffrement utilisées pour protéger vos données. Pour plus d'informations sur la création d'une clé KMS, veuillez consulter Création de clés dans le Guide du développeur AWS Key Management Service .

Si vous souhaitez utiliser une AWS KMS clé d'un autre AWS compte, vous devez être autorisé à utiliser la clé et spécifier son Amazon Resource Name (ARN) dans Amazon Redshift. Pour plus d'informations sur l'accès aux clés AWS KMS, consultez la section Contrôle de l'accès à vos clés dans le guide du AWS Key Management Service développeur.

Une fois que vous avez choisi une clé racine, Amazon Redshift vous demande de AWS KMS générer une clé de données et de la chiffrer à l'aide de la clé racine sélectionnée. Cette clé de données

est utilisée comme clé CEK dans Amazon Redshift. AWS KMS exporte la clé CEK chiffrée vers Amazon Redshift, où elle est stockée en interne sur un disque sur un réseau distinct du cluster avec l'affectation de la clé KMS et le contexte de chiffrement de la clé CEK. Seule la clé CEK chiffrée est exportée vers Amazon Redshift ; la clé KMS reste dans AWS KMS. Amazon Redshift transmet également au cluster la clé CEK chiffrée sur un canal sécurisé et la charge dans la mémoire. Amazon Redshift appelle ensuite AWS KMS pour déchiffrer le CEK et charge le CEK déchiffré en mémoire. Pour plus d'informations sur les subventions, le contexte de chiffrement et d'autres concepts AWS KMS connexes, consultez la section Concepts du guide du AWS Key Management Service développeur.

Ensuite, Amazon Redshift génère une clé de manière aléatoire à utiliser en tant que clé DEK et la charge en mémoire dans le cluster. La clé CEK déchiffrée est utilisée pour chiffrer la clé DEK, qui est ensuite transmise via un canal sécurisé depuis le cluster pour être stockée en interne par Amazon Redshift sur le disque dans un autre réseau que celui du cluster. A l'instar de la clé CEK, les versions chiffrées et déchiffrées de la clé DEK sont chargées en mémoire dans le cluster. La version déchiffrée de la clé DEK est ensuite utilisée pour chiffrer les clés de chiffrement individuelles qui sont générées de façon aléatoire pour chaque bloc de données de la base de données.

Lorsque le cluster redémarre, Amazon Redshift démarre avec les versions cryptées stockées en interne du CEK et du DEK, les recharge en mémoire, puis AWS KMS appelle pour déchiffrer à nouveau le CEK avec la clé KMS afin qu'il puisse être chargé en mémoire. La clé CEK déchiffrée est ensuite utilisée pour déchiffrer la clé DEK à nouveau, et la clé DEK déchiffré est chargée dans la mémoire et utilisée pour chiffrer et déchiffrer les clés de bloc de données en fonction des besoins.

Pour plus d’informations sur la création de clusters Amazon Redshift chiffrés avec des clés AWS KMS , consultez Création d’un cluster.

Copier AWS KMS—instantanés chiffrés vers un autre Région AWS

AWS KMS les clés sont spécifiques à un Région AWS. Si vous souhaitez activer la copie d'instantanés Amazon Redshift d'un cluster source chiffré vers un autre Région AWS, mais que vous souhaitez utiliser votre propre AWS KMS clé pour les instantanés de destination, vous devez configurer une autorisation permettant à Amazon Redshift d'utiliser une clé racine dans votre compte de destination. Région AWS Cette autorisation permet à Amazon Redshift de chiffrer les instantanés dans la Région AWS de destination. Si vous souhaitez que les instantanés de destination soient chiffrés à l'aide d'une clé Région AWS détenue, vous n'avez pas besoin de configurer d'autorisations dans la destination. Région AWS Pour de plus amples informations sur la copie d'instantanés entre régions, veuillez consulter Copier un instantané vers un autre AWS Région.

> **Note**
>
> Si vous activez la copie d'instantanés à partir d'un cluster chiffré et que vous l'utilisez AWS KMS comme clé racine, vous ne pouvez pas renommer votre cluster car le nom du cluster fait partie du contexte de chiffrement. Si vous devez renommer votre cluster, vous pouvez désactiver la copie des instantanés dans la AWS région source, renommer le cluster, puis configurer et réactiver la copie des instantanés.

Le processus permettant de configurer l'autorisation de copier des instantanés est le suivant.

1. Dans la AWS région de destination, créez une autorisation de copie instantanée en procédant comme suit :
   - Si vous n'avez pas encore de AWS KMS clé à utiliser, créez-en une. Pour plus d'informations sur la création de AWS KMS clés, consultez la section Création de clés dans le guide du AWS Key Management Service développeur.
   - Spécifiez un nom pour l'autorisation de copie d'instantanés. Ce nom doit être unique dans cette AWS région pour votre AWS compte.
   - Spécifiez l'ID AWS KMS clé pour lequel vous créez la subvention. Si vous ne spécifiez pas d'ID de clé, l'autorisation s'applique à votre clé par défaut.
2. Dans la AWS région source, activez la copie des instantanés et spécifiez le nom de la licence de copie d'instantanés que vous avez créée dans la AWS région de destination.

Ce processus précédent n'est nécessaire que si vous activez la copie des instantanés à l' AWS CLI aide de l'API Amazon Redshift ou des SDK. Si vous utilisez la console, Amazon Redshift fournit le flux de travail approprié pour configurer l'autorisation lorsque vous activez la copie d'instantanés entre régions. Pour de plus amples informations sur la configuration de copie d'instantanés entre régions pour les clusters chiffrés par AWS KMSà l'aide de la console, veuillez consulter Configuration d'une copie instantanée entre régions pour un AWS KMS—cluster chiffré.

Avant que l'instantané ne soit copié dans la AWS région de destination, Amazon Redshift le déchiffre à l'aide de la clé racine dans la AWS région source et le chiffre à nouveau temporairement à l'aide d'une clé RSA générée aléatoirement qu'Amazon Redshift gère en interne. Amazon Redshift copie ensuite l'instantané via un canal sécurisé vers la AWS région de destination, le déchiffre à l'aide de la clé RSA gérée en interne, puis le chiffre à nouveau à l'aide de la clé racine dans la région de destination. AWS

Chiffrement à l’aide de modules de sécurité matérielle

Si vous ne l'utilisez pas AWS KMS pour la gestion des clés, vous pouvez utiliser un module de sécurité matérielle (HSM) pour la gestion des clés avec Amazon Redshift.

> **Important**
>
> Le chiffrement HSM n'est pas pris en charge pour les types de nœuds DC2, RG et RA3.

Les HSM sont des dispositifs qui permettent de contrôler directement la génération et la gestion des clés. Ils offrent une plus grande sécurité en séparant la gestion des clés des couches application et base de données. Amazon Redshift prend en charge la AWS CloudHSM version classique pour la gestion des clés. Le processus de chiffrement est différent lorsque vous utilisez HSM pour gérer vos clés de chiffrement au lieu de AWS KMS.

> **Important**
>
> Amazon Redshift prend uniquement AWS CloudHSM en charge la version classique. Nous ne prenons pas en charge le nouveau AWS CloudHSM service.
> AWS CloudHSM Classic est fermé aux nouveaux clients. Pour plus d'informations, consultez la section Tarification de CloudHSM Classic. AWS CloudHSM La version classique n'est pas disponible dans toutes les AWS régions. Pour plus d'informations sur AWS les régions disponibles, consultez le tableau des AWS régions.

Lorsque vous configurez votre cluster pour utiliser un HSM, Amazon Redshift envoie une requête au HSM pour générer et stocker une clé à utiliser comme CEK. Cependant, contrairement à cela AWS KMS, le HSM n'exporte pas le CEK vers Amazon Redshift. Au lieu de cela, Amazon Redshift génère de manière aléatoire la clé DEK dans le cluster et la transmet au HSM pour qu'elle soit chiffrée par la clé CEK. Le HSM renvoie la clé DEK chiffrée à Amazon Redshift, où elle est encore chiffrée à l'aide d'une clé racine interne générée de manière aléatoire et stockée en interne sur un disque sur un autre réseau que celui du cluster. Amazon Redshift charge également la version déchiffrée du DEK en mémoire dans le cluster afin que le DEK puisse être utilisé pour chiffrer et déchiffrer les clés individuelles des blocs de données.

Si le cluster est redémarré, Amazon Redshift déchiffre le DEK enregistré en interne et chiffré deux fois à l'aide de la clé racine interne pour rétablir l'état du DEK stocké en interne. CEK-encrypted Le CEK-encrypted DEK est ensuite transmis au HSM pour être déchiffré et renvoyé à Amazon Redshift,

où il peut être à nouveau chargé en mémoire pour être utilisé avec les clés de bloc de données individuelles.

Configuration d'une connexion approuvée entre Amazon Redshift et un HSM

Lorsque vous optez pour utiliser un HSM pour la gestion de votre clé de cluster, vous devez configurer un lien réseau de confiance entre Amazon Redshift et votre HSM. Cela nécessite une configuration de certificats de client et de serveur. La connexion approuvée est utilisée pour transmettre les clés de chiffrement entre le HSM et Amazon Redshift pendant les opérations de chiffrement et de déchiffrement.

Amazon Redshift crée un certificat client public à partir d'une paire de clés privée et publique générée de manière aléatoire. Celles-ci sont chiffrées et stockées en interne. Vous téléchargez et enregistrez le certificat de client public dans votre HSM et l'affectez à la partition HSM applicable.

Vous fournissez à Amazon Redshift l'adresse IP du HSM, le nom de la partition HSM, le mot de passe de la partition HSM et un certificat public du serveur HSM, qui est chiffré à l'aide d'une clé racine interne. Amazon Redshift termine le processus de configuration et vérifie qu'il peut se connecter au HSM. S'il ne peut pas, le cluster est passé à l'État INCOMPATIBLE_HSM et le cluster n'est pas créé. Dans ce cas, vous devez supprimer le cluster incomplet, puis réessayer.

> **Important**
>
> Lorsque vous modifiez votre cluster pour utiliser une partition HSM différente, Amazon Redshift vérifie qu'il peut se connecter à la nouvelle partition, mais il ne vérifie pas qu'une clé de chiffrement valide existe. Avant d'utiliser la nouvelle partition, vous devez répliquer vos clés sur la nouvelle partition. Si le cluster est redémarré et qu'Amazon Redshift ne trouve pas de clé valide, le redémarrage échoue. Pour plus d'informations, consultez Réplication de clés entre HSM.

Après la configuration initiale, si Amazon Redshift ne parvient pas à se connecter au HSM, un événement est enregistré. Pour plus d'informations sur ces événements, veuillez consulter Notifications d'événements Amazon Redshift.

Rotation des clés de chiffrement

Dans Amazon Redshift, vous pouvez effectuer une rotation des clés de chiffrement pour les clusters chiffrés. Lorsque vous démarrez le processus de rotation des clés, Amazon Redshift effectue une rotation de la clé CEK pour le cluster spécifié et pour les instantanés automatiques ou manuels du

cluster. Amazon Redshift effectue également une rotation de la clé DEK pour le cluster spécifié, mais ne peut pas effectuer une rotation de la clé DEK pour les instantanés pendant qu'ils sont stockés en interne dans Amazon Simple Storage Service (Amazon S3) et chiffrés à l'aide de la clé DEK existante.

Pendant que la rotation est en cours, le cluster est mis dans l'état ROTATING_KEYS jusqu'à ce qu'il soit terminé, auquel cas le cluster retourne à l'état AVAILABLE. Amazon Redshift gère le déchiffrement et le rechiffrement pendant le processus de rotation des clés.

> **Note**
>
> Vous ne pouvez pas effectuer une rotation des clés pour des instantanés sans cluster source. Avant de supprimer un cluster, demandez-vous si ses instantanés reposent sur la rotation des clés.

Etant donné que le cluster est temporairement indisponible pendant le processus de rotation des clés, vous devez effectuer la rotation des clés uniquement dès que les données le nécessitent ou lorsque vous pensez que les clés ont été volées. La bonne pratique consiste à examiner le type de données que vous stockez et à prévoir à quelle fréquence effectuer la rotation des clés de chiffrement des données. La fréquence à laquelle effectuer la rotation des clés varie en fonction de vos stratégies d'entreprise concernant la sécurité des données et des normes du secteur relatives aux données sensibles et à la conformité réglementaire. Assurez-vous que votre plan tient compte des besoins en matière de sécurité autant que des considérations concernant la disponibilité de votre cluster.

Pour plus d’informations sur la rotation des clés, consultez Rotation des clés de chiffrement.

Modification du chiffrement d’un cluster

Vous pouvez modifier un cluster non chiffré pour utiliser le chiffrement AWS Key Management Service (AWS KMS) à l'aide d'une clé AWS détenue ou d'une clé gérée par le client. Lorsque vous modifiez votre cluster pour activer le chiffrement AWS KMS , Amazon Redshift migre automatiquement vos données vers un nouveau cluster chiffré. Vous pouvez également migrer un cluster chiffré vers un cluster non chiffré en modifiant le cluster avec le AWS CLI, mais pas avec le Console de gestion AWS.

Pendant l'opération de migration, votre cluster est disponible en mode lecture seule et son statut est redimensionnement en cours.

Si votre cluster est configuré pour activer la copie instantanée AWS entre régions, vous devez la désactiver avant de modifier le chiffrement. Pour plus d'informations, consultez Copier un instantané vers un autre AWS Région et Configuration d'une copie instantanée entre régions pour un AWS KMS—cluster chiffré. Vous ne pouvez pas activer le chiffrement HSM (module de sécurité matérielle) en modifiant le cluster. Créez plutôt un nouveau HSM-encrypted cluster et migrez vos données vers le nouveau cluster. Pour de plus amples informations, veuillez consulter Migration vers un cluster HSM-encrypted.

Amazon Redshift console

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters, puis sélectionnez le cluster pour lequel vous souhaitez modifier les clés de chiffrement.
3. Choisissez Propriétés.
4. Dans Configurations de base de données, choisissez Modifier, puis Modification du chiffrement.
5. Choisissez l'une des options de chiffrement et Enregistrez les modifications.

AWS CLI

Pour modifier le cluster non chiffré à utiliser AWS KMS, exécutez la commande `modify-cluster` CLI et spécifiez`--encrypted`, comme indiqué ci-dessous. Par défaut, votre clé KMS par défaut est utilisée. Pour spécifier une clé gérée par le client, incluez l'option `--kms-key-id`.

```
aws redshift modify-cluster --cluster-identifier <value> --encrypted --kms-key-id
 <value>
```

Pour supprimer le chiffrement de votre cluster, exécutez la commande suivante de l'interface de ligne de commande.

```
aws redshift modify-cluster --cluster-identifier <value> --no-encrypted
```

Migration vers un cluster HSM-encrypted

Pour migrer un cluster non chiffré vers un cluster chiffré en utilisant un module de sécurité matérielle (HSM), vous créez un nouveau cluster chiffré et déplacez vos données vers le nouveau cluster. Vous ne pouvez pas migrer vers un HSM-encrypted cluster en modifiant le cluster.

Pour migrer d'un cluster non chiffré vers un HSM-encrypted cluster, vous devez d'abord décharger vos données du cluster source existant. Vous devez ensuite les recharger dans un nouveau cluster cible avec le paramètre de chiffrement choisi. Pour plus d'informations sur le lancement d'un cluster chiffré, consultez Chiffrement de base de données Amazon Redshift.

Jusqu'à la dernière étape du processus de migration, votre cluster source reste disponible pour les requêtes en lecture seule. La dernière étape consiste à renommer les clusters source et cible afin de permuter les points de terminaison de manière à ce que la totalité du trafic soit redirigée vers le nouveau cluster cible. Le cluster cible est indisponible tant que vous ne l'avez pas redémarré après l'avoir renommé. Suspendez tous les chargements de données et autres opérations en écriture sur le cluster source pendant le transfert des données.

Pour préparer la migration

1. Identifiez tous les systèmes dépendants qui interagissent avec Amazon Redshift, par exemple les outils de Business Intelligence (BI) et les systèmes Extract-transform-load (ETL).
2. Identifiez les requêtes de validation permettant de tester la migration.

   Par exemple, vous pouvez utiliser la requête suivante pour trouver le nombre de tables définies par l'utilisateur.

   ```
   select count(*)
   from pg_table_def
   where schemaname != 'pg_catalog';
   ```

   La requête suivante renvoie la liste de toutes les tables définies par l'utilisateur et le nombre de lignes de chacune d'entre elles.

   ```
   select "table", tbl_rows
   from svv_table_info;
   ```
3. Choisissez le moment opportun pour réaliser la migration. Pour savoir quand l'utilisation du cluster est à son plus bas, surveillez les mesures relatives au cluster, notamment l'utilisation de

la CPU et le nombre de connexions à la base de données. Pour plus d'informations, consultez Affichage des données de performances de cluster.

4. Ignorez les tables inutilisées.

   Pour obtenir la liste des tables et la fréquence d'interrogation de chacune, exécutez la requête suivante.

```
select database,
schema,
table_id,
"table",
round(size::float/(1024*1024)::float,2) as size,
sortkey1,
nvl(s.num_qs,0) num_qs
from svv_table_info t
left join (select tbl,
perm_table_name,
count(distinct query) num_qs
from stl_scan s
where s.userid > 1
and   s.perm_table_name not in ('Internal worktable','S3')
group by tbl,
perm_table_name) s on s.tbl = t.table_id
where t."schema" not in ('pg_internal');
```

5. Lancez un nouveau cluster chiffré.

   Indiquez le même numéro de port pour le cluster cible que celui qu'utilisait le cluster source. Pour plus d'informations sur le lancement d'un cluster chiffré, consultez Chiffrement de base de données Amazon Redshift.

6. Configurez les processus de déchargement et chargement des données.

   Vous pouvez utiliser l' Unload/Copy utilitaire Amazon Redshift pour vous aider à migrer des données entre des clusters. L'utilitaire exporte les données depuis le cluster source vers un emplacement sur Amazon S3. Les données sont cryptées avec AWS KMS. L'utilitaire importe ensuite automatiquement les données sur le cluster cible. En option, vous pouvez utiliser l'utilitaire pour nettoyer Amazon S3 une fois la migration terminée.

7. Effectuez un test afin de vérifier que le processus fonctionne et d'estimer la durée pendant laquelle les opérations en écriture doivent être suspendues.

Lors des opérations de déchargement et chargement des données, vous devez préserver la cohérence des données en suspendant tous les chargements habituels et autres opérations en écriture. Utilisez l'une de vos plus grandes tables pour exécuter le test de déchargement/chargement et estimer les délais requis.

8. Créez des objets de base de données, tels que des schémas, vues ou tables. Pour vous aider à générer les instructions DDL (Data Definition Language) nécessaires, vous pouvez utiliser AdminViewsles scripts du AWS GitHub référentiel.

Pour migrer votre cluster

1. Arrêtez tous les processus ETL sur le cluster source.

   Pour vérifier qu'il n'y a aucune opération d'écriture en cours, utilisez la console de gestion Amazon Redshift afin de surveiller les IOPS d'écriture. Pour plus d’informations, consultez Affichage des données de performances de cluster.

2. Exécutez les requêtes de validation que vous avez identifiées précédemment afin de collecter des informations sur le cluster source chiffré avant de procéder à la migration.
3. (Facultatif) Créez une file d'attente de gestion de la charge de travail (WLM) pour exploiter le maximum de ressources disponibles à la fois dans le cluster source et le cible. Par exemple, créez une file d'attente nommée `data_migrate` et configurez-la avec 95 % de mémoire et un niveau de simultanéité de 4. Pour de plus amples informations, veuillez consulter la rubrique Acheminement des requêtes vers les files d'attente dans le Guide du développeur de bases de données Amazon Redshift.
4. À l'aide de la `data_migrate` file d'attente, exécutez le UnloadCopyUtility.

   Surveillez la progression des opérations UNLOAD et COPY à l'aide de la console Amazon Redshift.

5. Exécutez à nouveau les requêtes de validation et vérifiez que leurs résultats correspondent à ceux du cluster source.
6. Renommez vos clusters source et cible pour permuter les points de terminaison. Pour éviter une interruption de l'activité, effectuez cette opération en dehors des heures de travail,
7. Vérifiez que vous pouvez vous connecter au cluster cible à partir de tous vos clients SQL, notamment via les outils ETL et de génération de rapports.
8. Fermez le cluster source non chiffré.

Rotation des clés de chiffrement

Vous pouvez utiliser la procédure suivante pour effectuer une rotation des clés de chiffrement avec Amazon Redshift.

Pour effectuer une rotation des clés de chiffrement pour un cluster.

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters, puis le cluster pour lequel vous souhaitez mettre à jour les clés de chiffrement.
3. Pour Actions, choisissez Rotate encryption (Effectuer une rotation du chiffrement) pour afficher la page Rotate encryption keys (Effectuer une rotation des clés de chiffrement).
4. Sur la page Rotate encryption keys (Effectuer une rotation des clés de chiffrement), choisissez Rotate encryption keys (Effectuer une rotation des clés de chiffrement).

Chiffrement en transit

Vous pouvez configurer votre environnement pour protéger la confidentialité et l’intégrité des données en transit.

Les informations suivantes s'appliquent au chiffrement des données en transit entre un cluster Amazon Redshift et des clients SQL via : JDBC/ODBC

- Vous pouvez vous connecter aux clusters Amazon Redshift depuis les outils clients SQL via des connexions Java Database Connectivity (JDBC) et Open Database Connectivity (ODBC).
- Amazon Redshift prend en charge les connexions SSL (Secure Sockets Layer) pour chiffrer les données et les certificats de serveur pour valider le certificat du serveur auquel le client se connecte. Le client se connecte au nœud principal d’un cluster Amazon Redshift. Pour plus d’informations, consultez Configuration des options de sécurité des connexions.
- Pour prendre en charge les connexions SSL, Amazon Redshift crée et installe AWS Certificate Manager (ACM) des certificats émis sur chaque cluster. Pour plus d’informations, consultez Transition vers les certificats ACM pour les connexions SSL.
- Pour protéger vos données en transit dans le AWS cloud, Amazon Redshift utilise le protocole SSL à accélération matérielle pour communiquer avec Amazon S3 ou Amazon DynamoDB pour les opérations de copie, de déchargement, de sauvegarde et de restauration.

Les détails suivants s’appliquent au chiffrement de données en transit entre un cluster Amazon Redshift et Amazon S3 ou DynamoDB :

- Amazon Redshift utilise l’accélération matérielle SSL afin de communiquer avec Amazon S3 ou DynamoDB pour les opérations de copie (COPY), de déchargement (UNLOAD), de sauvegarde et de restauration.
- Redshift Spectrum prend en charge le chiffrement côté serveur (SSE) Amazon S3 à l'aide de la clé par défaut de votre compte gérée par le AWS Key Management Service (KMS).
- Vous pouvez chiffrer les charges Amazon Redshift avec Amazon S3 et. AWS KMS Pour plus d'informations, consultez Chiffrer vos charges Amazon Redshift avec Amazon S3 et. AWS KMS

Les informations suivantes s'appliquent au chiffrement et à la signature des données en transit entre les AWS CLI clients du SDK ou de l'API et les points de terminaison Amazon Redshift :

- Amazon Redshift fournit des points de terminaison HTTPS pour le chiffrement des données en transit.
- Pour protéger l’intégrité des requêtes d’API adressées à Amazon Redshift, les appels d’API doivent être signés par l’appelant. Les appels sont signés par un X.509 certificat ou par la clé d'accès AWS secrète du client conformément au processus de signature Signature version 4 (Sigv4). Pour plus d’informations, consultez Processus de signature Signature Version 4 dans le Références générales AWS.
- Utilisez le AWS CLI ou l'un des AWS SDK pour envoyer des demandes à AWS. Ces outils signent automatiquement les demandes avec la clé d’accès que vous spécifiez lors de leur configuration.

Les détails suivants s’appliquent au chiffrement de données en transit entre les clusters Amazon Redshift et Amazon Redshift Query Editor V2 :

- Les données sont transmises entre l'éditeur de requêtes v2 et les clusters Amazon Redshift via un TLS-encrypted canal.

Contrôles de chiffrement VPC avec Amazon Redshift

Amazon Redshift prend en charge les contrôles de chiffrement VPC, une fonctionnalité de sécurité qui vous aide à appliquer le chiffrement en transit pour tout le trafic au sein et entre les VPC d'une région. Ce document explique comment utiliser les contrôles de chiffrement VPC avec les clusters Amazon Redshift et les groupes de travail sans serveur.

Les contrôles de chiffrement VPC fournissent un contrôle centralisé pour surveiller et appliquer le chiffrement en transit au sein de vos VPC. Lorsqu'il est activé en mode Enforce, il garantit que tout le trafic réseau est chiffré soit au niveau de la couche matérielle (à l'aide de AWS Nitro System), soit au niveau de la couche application (à l'aide de TLS/SSL).

Amazon Redshift s'intègre aux contrôles de chiffrement VPC pour vous aider à répondre aux exigences de conformité dans des secteurs tels que la santé (HIPAA), le gouvernement (FedRAMP) et les finances (PCI DSS).

Comment fonctionnent les contrôles de chiffrement VPC avec Amazon Redshift

Les contrôles de chiffrement VPC fonctionnent selon deux modes :

- Mode surveillance : fournit une visibilité sur l'état de chiffrement des flux de trafic et aide à identifier les ressources qui autorisent le trafic non chiffré.
- Mode d'application : empêche la création ou l'utilisation de ressources qui autorisent le trafic non chiffré au sein du VPC. Tout le trafic doit être chiffré au niveau de la couche matérielle (Nitro-based instances) ou de la couche application (TLS/SSL).

Exigences relatives à l'utilisation des contrôles de chiffrement VPC

Exigences relatives au type d'instance

Amazon Redshift a besoin d' Nitro-based instances pour prendre en charge les contrôles de chiffrement VPC. Tous les types d'instances Redshift modernes prennent en charge les fonctionnalités de chiffrement nécessaires.

SSL/TLS exigences

Lorsque les contrôles de chiffrement VPC sont activés en mode d'application, le paramètre require_ssl doit être défini sur true et ne peut pas être désactivé. Cela garantit que toutes les connexions client utilisent des connexions TLS cryptées.

Migration vers les contrôles de chiffrement VPC

Pour les clusters et groupes de travail existants

Vous ne pouvez pas activer les contrôles de chiffrement VPC en mode renforcé sur un VPC qui contient des clusters Redshift ou des groupes de travail sans serveur existants. Consultez les étapes suivantes pour utiliser les contrôles de chiffrement si vous disposez déjà d'un cluster ou d'un groupe de travail :

1. Créez un instantané de votre cluster ou de votre espace de noms existant
2. Créez un nouveau VPC avec les contrôles de chiffrement VPC activés en mode d'application
3. Effectuez une restauration depuis le snapshot vers le nouveau VPC à l'aide de l'une des opérations suivantes :

   - Pour les clusters provisionnés : utilisez l'opération `restore-from-cluster-snapshot`
   - Pour le mode sans serveur : utilisez l'`restore-from-snapshot`opération sur votre groupe de travail

Lorsque vous créez de nouveaux clusters ou groupes de travail dans un VPC avec les contrôles de chiffrement activés, le paramètre require_ssl doit être défini sur true.

Amazon Redshift a besoin d' Nitro-based instances pour prendre en charge les contrôles de chiffrement VPC. Tous les types d'instances Redshift modernes prennent en charge les fonctionnalités de chiffrement nécessaires.

SSL/TLS exigences

Lorsque les contrôles de chiffrement VPC sont activés en mode d'application, le paramètre require_ssl doit être défini sur true et ne peut pas être désactivé. Cela garantit que toutes les connexions client utilisent des connexions TLS cryptées.

Considérations et restrictions

Lorsque vous utilisez les contrôles de chiffrement VPC dans Amazon Redshift, tenez compte des points suivants :

Restrictions relatives à l'état du VPC

- La création de clusters et de groupes de travail est bloquée lorsque les contrôles de chiffrement VPC sont activés `enforce-in-progress`
- Vous devez attendre que le VPC passe en `enforce` mode mode avant de créer de nouvelles ressources

Configuration du protocole SSL

- Paramètre require_ssl : doit toujours être `true` destiné aux clusters et aux groupes de travail créés dans des VPC soumis au chiffrement

- Une fois qu'un cluster ou un groupe de travail est créé dans un VPC à chiffrement renforcé`require_ssl`, il ne peut pas être désactivé pendant toute sa durée de vie

Disponibilité dans les Régions

Cette fonctionnalité n'est pas disponible en mode d'application avec Amazon Redshift Serverless dans les régions suivantes :

- Amérique du Sud (São Paulo)
- Europe (Zurich)

Gestion des clés

Vous pouvez configurer votre environnement pour protéger des données avec des clés.

- Amazon Redshift s'intègre automatiquement à AWS Key Management Service (AWS KMS) pour la gestion des clés. AWS KMS utilise le chiffrement des enveloppes. Pour plus d'informations, consultez Chiffrement d'enveloppe.
- Lorsque les clés de chiffrement sont gérées dans AWS KMS, Amazon Redshift utilise une architecture à quatre niveaux basée sur des clés pour le chiffrement. L'architecture se compose de clés de chiffrement de AES-256 données générées aléatoirement, d'une clé de base de données, d'une clé de cluster et d'une clé racine. Pour plus d'informations, consultez Comment Amazon Redshift l'utilise. AWS KMS
- Vous pouvez créer votre propre clé gérée par le client dans AWS KMS. Pour plus d'informations, consultez les sections Créer une clé KMS etAutoriser l'utilisation d'un AWS KMS clé gérée par le client avec Amazon Redshift (Provisioned) et Amazon Redshift Serverless.
- Vous pouvez également importer votre propre matériel clé pour le neuf AWS KMS keys. Pour plus d'informations, voir Importation de matériel clé dans AWS Key Management Service (AWS KMS).
- Amazon Redshift prend en charge la gestion des clés de chiffrement dans des modules HSM (Hardware Security Modules) externes. Il peut s'agir d'un module HSM sur site ou d' AWS CloudHSM. Lorsque vous utilisez un HSM, vous devez utiliser des certificats client et de serveur pour configurer une connexion approuvée entre Amazon Redshift et votre HSM. Amazon Redshift prend uniquement en charge la AWS CloudHSM version classique pour la gestion des clés. Pour plus d'informations, consultez Chiffrement à l'aide de modules de sécurité matérielle. Pour plus d'informations AWS CloudHSM, voir Qu'est-ce que c'est AWS CloudHSM ?

- Vous pouvez effectuer une rotation des clés de chiffrement pour les clusters chiffrés. Pour plus d'informations, consultez Rotation des clés de chiffrement.

Autoriser l'utilisation d'un AWS KMS clé gérée par le client avec Amazon Redshift (Provisioned) et Amazon Redshift Serverless

Amazon Redshift s'intègre à AWS Key Management Service (AWS KMS) pour chiffrer vos données au repos. Lorsque vous utilisez une clé gérée par le client, vous contrôlez totalement la politique en matière de clés, la rotation des clés et l'activation ou la désactivation de la clé. Pour plus d'informations sur les clés gérées par le client, consultez Clés gérées par le client dans le Guide du développeur AWS Key Management Service .

Lorsqu'Amazon Redshift utilise une clé gérée par le client dans le cadre d'opérations cryptographiques, il agit pour le compte de l'utilisateur qui crée ou modifie le cluster provisionné Amazon Redshift ou la ressource Amazon Redshift Serverless.

Autorisations requises

Pour créer et utiliser un cluster provisionné Amazon Redshift ou une ressource Amazon Redshift Serverless chiffrée à l'aide d'une clé gérée par le client, un utilisateur doit être autorisé à effectuer les opérations suivantes sur la clé gérée par le client :

- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:Encrypt`
- `kms:Decrypt`
- `kms:DescribeKey`

Le propriétaire ou l'administrateur de la clé gérée par le client peut ajouter ces autorisations pour des utilisateurs spécifiques dans la politique clé de la clé gérée par le client, ou dans une politique IAM si la politique clé le permet.

Amazon Redshift accède à la clé gérée par le client par le biais de subventions. AWS KMS Assurez-vous que votre politique en matière de clés n'empêche pas Amazon Redshift de créer ou d'utiliser des subventions sur la clé. Par exemple, des instructions Deny explicites ou des conditions restrictives sur les instructions Allow peuvent bloquer la création de subventions et entraîner l'échec des opérations.

Pour des raisons de sécurité, nous vous recommandons de ne fournir que les autorisations requises pour votre cas d'utilisation. Par exemple, vous pouvez limiter l'`kms:CreateGrant`autorisation en utilisant une clé de condition telle que`kms:GrantIsForAWSResource`.

Pour plus d'informations sur le contrôle de l'accès aux AWS KMS clés, consultez les sections Politiques relatives aux clés AWS KMS et Autorisation des utilisateurs d'autres comptes à utiliser une clé KMS dans le Guide du AWS Key Management Service développeur.

Création de jetons de données

La tokenisation est le processus de remplacement des valeurs réelles par des valeurs opaques à des fins de sécurité des données. Security-sensitive les applications utilisent la tokenisation pour remplacer les données sensibles telles que les informations personnelles identifiables (PII) ou les informations de santé protégées (PHI) par des jetons afin de réduire les risques de sécurité. La suppression de jetons (detokenization) inverse les jetons avec des valeurs réelles pour les utilisateurs autorisés avec des stratégies de sécurité appropriées.

Pour l'intégration avec des services de création de jetons tiers, vous pouvez utiliser les fonctions définies par l'utilisateur Amazon Redshift (UDF) que vous créez à l'aide de AWS Lambda. Pour plus d'informations, consultez Fonctions Lambda définies par l'utilisateur dans le Guide du développeur de bases de données Amazon Redshift. Pour obtenir des exemples, consultez Protegrity.

Amazon Redshift envoie des demandes de création de jetons à un serveur de création de jetons accessible via une API REST ou un point de terminaison prédéfini. Deux fonctions Lambda complémentaires ou plus traitent les demandes de création et de suppression de jetons. Pour ce traitement, vous pouvez utiliser les fonctions Lambda fournies par un fournisseur de création de jetons tiers. Vous pouvez également utiliser les fonctions Lambda que vous enregistrez en tant que UDF Lambda dans Amazon Redshift.

Par exemple, supposons qu'une requête soit soumise qui appelle une FDU de création ou de suppression de jetons sur une colonne. Le cluster Amazon Redshift spoule les rangées d'arguments applicables et envoie ces rangées par lots à la fonction Lambda en parallèle. Les données sont transférées entre les nœuds de calcul Amazon Redshift et Lambda dans une connexion réseau séparée et isolée qui n'est pas accessible aux clients. La fonction Lambda transmet les données au point de terminaison du serveur de création de jetons. Le serveur de création de jetons crée ou supprime les jetons de données si nécessaire et les renvoie. Les fonctions Lambda transmettent ensuite les résultats au cluster Amazon Redshift pour traitement ultérieur, si nécessaire, puis renvoient les résultats de la requête.

Routage du trafic inter-réseaux dans Amazon Redshift

Vous pouvez acheminer le trafic via des routes de réseau privé et connu dans Amazon Redshift. Cette page explique comment acheminer le trafic sur un réseau d'entreprise et entre les ressources de la même Région AWS.

Pour acheminer le trafic entre Amazon Redshift, les clients et applications sur un réseau d'entreprise :

- Configurez une connexion privée entre votre cloud privé virtuel (VPC) et votre réseau d'entreprise. Configurez une connexion VPN IPSec sur Internet ou une connexion physique privée à l'aide d'une Direct Connect connexion. Direct Connect vous permet d'établir une interface virtuelle privée depuis votre réseau local directement vers votre Amazon VPC, vous fournissant ainsi une connexion réseau privée à haut débit entre votre réseau et votre VPC. Avec des interfaces virtuelles multiples, vous pouvez même établir une connectivité privée vers des VPC multiples, tout en maintenant l'isolation réseau. Pour plus d'informations, consultez Qu'est-ce qu' AWS Site-to-Site un VPN ? et qu'est-ce que c'est Direct Connect ?

Pour acheminer le trafic entre un cluster Amazon Redshift dans un VPC et des compartiments Amazon S3 dans la même région : AWS

- Configurez un point de terminaison de VPC privé Amazon S3 pour accéder de manière privée aux données Amazon S3 à partir d'un chargement ou d'un déchargement ETL. Pour plus d'informations, consultez Points de terminaison pour Amazon S3.
- Activez le « Routage VPC amélioré » pour un cluster Amazon Redshift, en spécifiant un point de terminaison de VPC Amazon S3 cible. Le trafic généré par les commandes Amazon Redshift COPY, UNLOAD ou CREATE LIBRARY est ensuite acheminé par le point de terminaison privé. Pour plus d'informations, consultez Activation du routage VPC amélioré.

Identity and Access Management dans Amazon Redshift

L'accès à Amazon Redshift nécessite des informations d'identification qui AWS peuvent être utilisées pour authentifier vos demandes. Ces informations d'identification doivent disposer des autorisations nécessaires pour accéder à AWS des ressources, telles qu'un cluster Amazon Redshift. Les sections suivantes fournissent des détails sur la façon dont vous pouvez utiliser Gestion des identités et des accès AWS (IAM) et Amazon Redshift pour contribuer à sécuriser vos ressources en contrôlant qui peut y accéder :

- Authentification par des identités
- Contrôle d’accès

> **Important**
>
> Cette rubrique contient un ensemble de bonnes pratiques pour la gestion des autorisations, des identités et des accès sécurisés. Nous vous recommandons de vous familiariser avec les bonnes pratiques d’utilisation de l’IAM avec Amazon Redshift. Il s’agit notamment d’utiliser les rôles IAM pour l’application des autorisations. Une bonne compréhension de ces sections vous aidera à maintenir un entrepôt des données Amazon Redshift plus sûr.

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identité. 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), de l'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 interface de ligne de commande 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 avec 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.

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 utilisateur à un rôle IAM (console) ou en appelant une opération AWS CLI ou AWS 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 intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

> **Note**
>
> Les transferts de sessions d'accès (FAS) de Redshift sont valides pendant 12 heures uniquement. Après cette période, toute session de connexion utilisant le transfert de sessions d'accès pour intégrer d'autres services doit être rétablie.

Cross-service prévention adjointe confuse

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. En AWS, l'usurpation d'identité interservices peut entraîner la confusion du problème des adjoints. Cross-service l'usurpation d'identité peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé à accéder

autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte. Pour plus d'informations, consultez la section Prévention de la Cross-service confusion chez les adjoints dans le Guide de l'utilisateur IAM.

Nous vous recommandons d'utiliser `aws:SourceArn` les clés contextuelles de condition `aws:SourceAccount` globale dans les politiques basées sur les ressources afin de limiter les autorisations qu'Amazon Redshift accorde à un autre service pour la ressource. Si la valeur `aws:SourceArn` ne contient pas l'ID de compte, tel qu'un ARN de compartiment Amazon S3, vous devez utiliser les deux clés de contexte de condition globale pour limiter les autorisations. Si vous utilisez les deux clés de contexte de condition globale et que la valeur de `aws:SourceArn` contient l'ID de compte, la valeur de `aws:SourceAccount` et le compte indiqué dans la valeur de `aws:SourceArn` doivent utiliser le même ID de compte lorsqu'il est utilisé dans la même déclaration de politique.

L'exemple suivant montre une politique que vous pouvez appliquer pour limiter le problème de confusion chez les adjoints pour Amazon Redshift.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionForRedshift",
    "Effect": "Allow",
    "Principal": {
      "Service": "redshift.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:redshift:us-east-1:123456789012:cluster:my-cluster"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

L'exemple suivant illustre une politique pour Amazon Redshift Serverless.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionForRedshiftServerless",
    "Effect": "Allow",
    "Principal": {
      "Service": "redshift-serverless.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:redshift-serverless:us-east-1:123456789012:workgroup/
my-workgroup"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Contrôle d’accès

Vous pouvez disposer d’informations d’identification valides pour authentifier vos demandes, mais à moins d’avoir des autorisations, vous ne pouvez pas créer ou accéder aux ressources Amazon Redshift. Par exemple, vous devez disposer des autorisations nécessaires pour créer un cluster Amazon Redshift, créer un instantané, ajouter un abonnement à un événement, etc.

Les sections suivantes décrivent comment gérer les autorisations pour Amazon Redshift. Nous vous recommandons de lire d’abord la présentation.

- Présentation de la gestion des autorisations d’accès à vos ressources Amazon Redshift
- Utilisation des politiques basées sur l’identité (politiques IAM) pour Amazon Redshift

Présentation de la gestion des autorisations d’accès à vos ressources Amazon Redshift

Chaque AWS ressource appartient à un AWS compte, et les autorisations de création ou d'accès aux ressources sont régies par des politiques d'autorisations. Un administrateur de compte peut associer des politiques d'autorisations aux identités IAM (c'est-à-dire aux utilisateurs, aux groupes et aux

rôles), et certains services (tels que AWS Lambda) permettent également d'associer des politiques d'autorisations aux ressources.

> **Note**
>
> Un administrateur de compte (ou utilisateur administrateur) est un utilisateur doté des privilèges d'administrateur. Pour plus d'informations, consultez Bonnes pratiques IAM dans le Guide de l'utilisateur IAM.

Lorsque vous accordez des autorisations, vous décidez qui doit les obtenir, à quelles ressources ces autorisations s'appliquent et les actions spécifiques que vous souhaitez autoriser sur ces ressources.

Ressources et opérations Amazon Redshift

Amazon Redshift fournit les ressources, actions et clés de contexte de condition spécifiques au service en vue de leur utilisation dans les politiques d'autorisation IAM.

Autorisations d'accès Amazon Redshift, Amazon Redshift sans serveur, API de données Amazon Redshift et Éditeur de requêtes Amazon Redshift v2

Lorsque vous configurez Contrôle d'accès, vous écrivez des politiques d'autorisation que vous pouvez attacher à une identité IAM (politiques basées sur l'identité). Pour des informations de référence détaillées, consultez les rubriques suivantes dans la Référence de l'autorisation de service :

- Pour Amazon Redshift, consultez Actions, ressources et clés de condition pour Amazon Redshift qui utilisent le préfixe `redshift:`.
- Pour Amazon Redshift sans serveur, consultez Actions, ressources et clés de condition pour Amazon Redshift sans serveur qui utilisent le préfixe `redshift-serverless:`.
- Pour l'API de données Amazon Redshift, consultez Actions, ressources et clés de condition l'API de données Amazon Redshift qui utilisent le préfixe `redshift-data:`.
- Pour l'éditeur de requêtes Amazon Redshift v2, voir Actions, ressources et clés de condition pour AWS SQL Workbench (éditeur de requêtes Amazon Redshift v2) qui utilisent le préfixe. `sqlworkbench:`

  L'éditeur de requête v2 inclut des actions avec autorisations uniquement qui ne correspondent pas directement à une opération d'API. Ces actions sont indiquées dans la référence d'autorisation de service avec `[permission only]`.

Cette référence contient des informations sur les opérations d'API qui peuvent être utilisées dans une politique IAM. Il inclut également la AWS ressource pour laquelle vous pouvez accorder les autorisations et les clés de condition que vous pouvez inclure pour un contrôle d'accès précis. Pour plus d'informations sur les conditions, consultez Utilisation de conditions de politique IAM pour un contrôle d'accès précis.

Vous spécifiez les actions dans le champ `Action` de la politique, la valeur de ressource dans le champ `Resource` de la politique, et les conditions dans le champ `Condition` de la politique. Pour spécifier une action pour Amazon Redshift, utilisez le préfixe `redshift:` suivi du nom de l'opération d'API (par exemple, `redshift:CreateCluster`).

Présentation de la propriété des ressources

Le propriétaire d'une ressource est le AWS compte qui a créé une ressource. En d'autres termes, le propriétaire de la ressource est le AWS compte de l'entité principale (le compte root, un utilisateur IAM ou un rôle IAM) qui authentifie la demande qui crée la ressource. Les exemples suivants illustrent comment cela fonctionne :

- Si vous utilisez les informations d'identification du compte root de votre AWS compte pour créer un cluster de bases de données, votre AWS compte est le propriétaire de la ressource Amazon Redshift.
- Si vous créez un rôle IAM dans votre AWS compte avec l'autorisation de créer des ressources Amazon Redshift, toute personne pouvant assumer ce rôle peut créer des ressources Amazon Redshift. Votre compte AWS , auquel le rôle appartient, reste le propriétaire des ressources Amazon Redshift.
- Si vous créez un utilisateur IAM dans votre AWS compte et que vous lui accordez l'autorisation de créer des ressources Amazon Redshift, celui-ci peut créer des ressources Amazon Redshift. Toutefois, votre compte AWS , auquel appartient l'utilisateur, détient ces ressources Amazon Redshift. Dans la plupart des cas, cette méthode n'est pas recommandée. Nous vous recommandons de créer un rôle IAM et d'y associer des autorisations, puis de l'attribuer à un utilisateur.

Gestion de l'accès aux ressources

Une politique d'autorisation décrit qui a accès à quoi. La section suivante explique les options disponibles pour créer des politiques d'autorisations.

> **Note**
>
> Cette section traite de l'utilisation d'IAM dans le contexte d'Amazon Redshift. Elle ne fournit pas d'informations détaillées sur le service IAM. Pour une documentation complète sur IAM, consultez la rubrique Qu'est-ce que IAM ? dans le Guide de l'utilisateur IAM. Pour plus d'informations sur la syntaxe et les descriptions des politiques IAM, consultez la Référence des politiques AWS IAM dans le Guide de l'utilisateur IAM.

Les politiques attachées à une identité IAM sont appelées politiques basées sur une entité (politiques IAM) et les politiques attachées à une ressource sont appelées politiques basées sur une ressource. Amazon Redshift prend en charge uniquement les politiques basées sur l'identité (politiques IAM).

Identity-based politiques (politiques IAM)

Vous pouvez attribuer des autorisations en associant des politiques à un rôle IAM, puis en attribuant ce rôle à un utilisateur ou à un groupe. Voici un exemple de politique qui contient des autorisations pour créer, supprimer, modifier et redémarrer les clusters Amazon Redshift pour votre compte AWS .

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid":"AllowManageClusters",
      "Effect":"Allow",
      "Action": [
        "redshift:CreateCluster",
        "redshift:DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource":"*"
    }
  ]
}
```

Pour plus d'informations sur l'utilisation des politiques basées sur l'identité avec Amazon Redshift, consultez Utilisation des politiques basées sur l'identité (politiques IAM) pour Amazon Redshift. Pour plus d'informations sur les utilisateurs, les groupes, les rôles et les autorisations, consultez Identités (utilisateurs, groupes et rôles) dans le Guide de l'utilisateur IAM.

Resource-based politiques

D'autres services, tels qu'Amazon S3, prennent également en charge les politiques d'autorisation basées sur une ressource. Par exemple, vous pouvez attacher une politique à un compartiment S3 pour gérer les autorisations d'accès à ce compartiment. Amazon Redshift ne prend pas en charge les politiques basées sur une ressource.

Spécification des éléments d'une politique : actions, effets, ressources et principaux

Pour chaque ressource Amazon Redshift (voirRessources et opérations Amazon Redshift), le service définit un ensemble d'opérations d'API (voir Actions). Pour accorder des autorisations pour ces opérations d'API, Amazon Redshift définit un ensemble d'actions que vous pouvez spécifier dans une politique. Une opération d'API peut exiger des autorisations pour plusieurs actions.

Voici les éléments de base d'une politique :

- Ressource : dans une politique, vous utilisez un Amazon Resource Name (ARN) pour identifier la ressource à laquelle la politique s'applique. Pour plus d'informations, consultez Ressources et opérations Amazon Redshift.
- Action : vous utilisez des mots clés d'action pour identifier les opérations de ressource que vous voulez accorder ou refuser. Par exemple, l'autorisation `redshift:DescribeClusters` permet à l'utilisateur d'effectuer l'opération Amazon Redshift `DescribeClusters`.
- Effet – Vous spécifiez l'effet produit lorsque l'utilisateur demande l'action spécifique, qui peut être une autorisation ou un refus. Si vous n'accordez pas explicitement l'accès pour (autoriser) une ressource, l'accès est implicitement refusé. Vous pouvez aussi explicitement refuser l'accès à une ressource, ce que vous pouvez faire afin de vous assurer qu'un utilisateur n'y a pas accès, même si une politique différente accorde l'accès.
- Principal – dans les politiques basées sur une identité (politiques IAM), l'utilisateur auquel la politique est attachée est le principal implicite. Pour les politiques basées sur une ressource, vous spécifiez l'utilisateur, le compte, le service ou une autre entité qui doit recevoir les autorisations (s'applique uniquement aux politiques basées sur une ressource). Amazon Redshift ne prend pas en charge les politiques basées sur une ressource.

Pour en savoir plus sur la syntaxe et les descriptions des politiques IAM, consultez la Référence des politiques AWS IAM dans le Guide de l'utilisateur IAM.

Pour un tableau présentant toutes les actions de l'API Amazon Redshift et les ressources auxquelles elles s'appliquent, consultez Autorisations d'accès Amazon Redshift, Amazon Redshift sans serveur, API de données Amazon Redshift et Éditeur de requêtes Amazon Redshift v2.

Spécification de conditions dans une politique

Lorsque vous accordez des autorisations, vous pouvez utiliser le langage de la politique d'accès pour spécifier les conditions définissant quand une politique doit prendre effet. Par exemple, il est possible d'appliquer une politique après seulement une date spécifique. Pour plus d'informations sur la spécification des conditions dans un langage de politique d'accès, consultez Éléments de politique IAM JSON : Condition dans le Guide de l'utilisateur IAM.

Pour identifier les conditions dans lesquelles une politique d'autorisations s'applique, incluez un élément `Condition` à votre politique d'autorisations IAM. Par exemple, vous pouvez créer une politique qui autorise un utilisateur à créer un cluster à l'aide de l'action `redshift:CreateCluster` et vous pouvez ajouter un élément `Condition` pour limiter cet utilisateur à la création du cluster dans une région spécifique uniquement. Pour plus de détails, consultez Utilisation de conditions de politique IAM pour un contrôle d'accès précis. Pour obtenir une liste de toutes les valeurs clés conditionnelles et des actions et ressources Amazon Redshift auxquelles elles s'appliquent, consultez Autorisations d'accès Amazon Redshift, Amazon Redshift sans serveur, API de données Amazon Redshift et Éditeur de requêtes Amazon Redshift v2.

Utilisation de conditions de politique IAM pour un contrôle d'accès précis

Dans Amazon Redshift, vous pouvez utiliser des clés de condition pour restreindre l'accès aux ressources en fonction des balises de ces ressources. Vous trouverez ci-dessous des clés de condition Amazon Redshift courantes.

Clé de condition	Description
`aws:RequestTag`	Nécessite que les utilisateurs incluent une clé de balise (nom) et une valeur chaque fois qu'ils créent une ressource. Pour plus d'informations, consultez aws : RequestTag dans le guide de l'utilisateur IAM.

Clé de condition	Description
`aws:ResourceTag`	Limite l'accès utilisateur aux ressources basées sur des clés et des valeurs de balise spécifiques. Pour plus d'informations, consultez aws : ResourceTag dans le guide de l'utilisateur IAM.
`aws:TagKeys`	Utilisez cette clé pour comparer les clés de balise d'une demande avec celles spécifiées dans la politique. Pour plus d'informations, consultez aws : TagKeys dans le guide de l'utilisateur IAM.

Pour plus d'informations sur les balises, consultez Étiqueter les ressources dans Amazon Redshift..

Pour obtenir une liste des actions d'API qui prennent en charge les clés de condition `redshift:RequestTag` et `redshift:ResourceTag`, consultez Autorisations d'accès Amazon Redshift, Amazon Redshift sans serveur, API de données Amazon Redshift et Éditeur de requêtes Amazon Redshift v2.

Les clés de condition suivantes peuvent être utilisées avec l' GetClusterCredentialsaction Amazon Redshift.

Clé de condition	Description
`redshift:DurationSeconds`	Limite le nombre de secondes qui peut être spécifié pour la durée.
`redshift:DbName`	Limite les noms de base de données qui peuvent être spécifiés.
`redshift:DbUser`	Limite les noms d'utilisateur de base de données qui peuvent être spécifiés.

Exemple 1 : Restreindre l'accès à l'aide de la clé de ResourceTag condition aws :

Utilisez la politique IAM suivante pour permettre à un utilisateur de modifier un cluster Amazon Redshift uniquement pour un AWS compte spécifique de la `us-west-2` région avec une balise nommée `environment` avec une valeur de balise de. `test`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Sid":"AllowModifyTestCluster",
        "Effect": "Allow",
        "Action": "redshift:ModifyCluster",
        "Resource": "arn:aws:redshift:us-west-2:123456789012:cluster:*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/environment": "test"
            }
        }
    }
}
```

Exemple 2 : Restreindre l'accès à l'aide de la clé de RequestTag condition aws :

Utilisez la politique IAM suivante pour permettre à un utilisateur de créer un cluster Amazon Redshift uniquement si la commande de création du cluster comprend une balise nommée `usage` et une valeur de balise `production`. La condition avec `aws:TagKeys` et le modificateur `ForAllValues` spécifie que seules les clés `costcenter` et `usage` peuvent être spécifiées dans la demande.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Sid":"AllowCreateProductionCluster",
        "Effect": "Allow",
        "Action": [
            "redshift:CreateCluster",
            "redshift:CreateTags"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/usage": "production"
            },
```

```
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "costcenter",
                    "usage"
                ]
            }
        }
    }
}
```

Utilisation des politiques basées sur l'identité (politiques IAM) pour Amazon Redshift

Cette rubrique fournit des exemples de politiques basées sur une identité dans lesquelles un administrateur de compte peut attacher des politiques d'autorisation aux identités IAM (c'est-à-dire aux utilisateurs, groupes et rôles).

> **Important**
>
> Nous vous recommandons de consulter d'abord les rubriques d'introduction qui expliquent les concepts de base et les options dont vous disposez pour gérer l'accès à vos ressources Amazon Redshift. Pour plus d'informations, consultez Présentation de la gestion des autorisations d'accès à vos ressources Amazon Redshift.

Un exemple de politique d'autorisation est exposé ci-dessous. La politique permet à un utilisateur de créer, de supprimer, de modifier et de redémarrer tous les clusters, puis refuse l'autorisation de supprimer ou de modifier les clusters dont l'identifiant de cluster commence par `production` in Région AWS `us-west-2` et Compte AWS `123456789012`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid":"AllowClusterManagement",
      "Action": [
```

```
        "redshift:CreateCluster",
        "redshift:DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid":"DenyDeleteModifyProtected",
      "Action": [
        "redshift:DeleteCluster",
        "redshift:ModifyCluster"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:cluster:production*"
      ],
      "Effect": "Deny"
    }
  ]
}
```

La politique possède deux énoncés:

- Le premier énoncé accorde des autorisations à un utilisateur pour créer, supprimer, modifier et redémarrer des clusters. L'instruction spécifie un caractère générique (*) comme `Resource` valeur afin que la politique s'applique à toutes les ressources Amazon Redshift détenues par le compte root AWS .
- Le second énoncé refuse l’autorisation de supprimer ou de modifier un cluster. L’énoncé spécifie un cluster Amazon Resource Name (ARN) pour la valeur `Resource` qui inclut un caractère générique (*). Par conséquent, cette déclaration s'applique à tous les clusters Amazon Redshift détenus par le AWS compte root par lequel l'identifiant du cluster commence`production`.

AWS politiques gérées pour Amazon Redshift

AWS répond à de nombreux cas d'utilisation courants en fournissant des politiques IAM autonomes créées et administrées par AWS. Les politiques gérées octroient les autorisations requises dans les

cas d'utilisation courants et vous évitent d'avoir à réfléchir aux autorisations qui sont requises. Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Vous pouvez également créer vos propres politiques IAM personnalisées pour autoriser les autorisations pour les opérations et les ressources de l'API Amazon Redshift. Vous pouvez attacher ces politiques personnalisées aux rôles ou groupes IAM qui nécessitent ces autorisations.

Les sections suivantes décrivent les politiques AWS gérées, que vous pouvez associer aux utilisateurs de votre compte, et sont spécifiques à Amazon Redshift.

Amazon Redshift met à jour AWS stratégies gérées

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon Redshift depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques sur les modifications apportées à cette page, abonnez-vous au flux RSS sur la page de l'historique des documents Amazon Redshift.

Modifier	Description	Date
AmazonRedshiftFederatedAuthorization : nouvelle politique	Amazon Redshift a ajouté une nouvelle politique de facilité d'utilisation pour exécuter des requêtes avec Amazon Redshift Federated Authorization.	21 novembre 2025
AmazonRedshiftServiceLinkedRolePolicy : mise à jour d'une politique existante	L'autorisation pour l'action `lakeformation:GetDataAccess` est ajoutée à la politique gérée. Son ajout permet d'obtenir les informations du catalogue fédéré auprès de AWS Lake Formation. Les conditions supplémentaires pour les actions	13 mars 2025

Modifier	Description	Date
	`glue:GetCatalog` et `glue:GetCatalogs` sont ajoutées à la politique gérée.	
AmazonRedshiftServiceLinkedRolePolicy : mise à jour d'une politique existante	Les autorisations pour les actions `glue:GetCatalog` et `glue:GetCatalogs` sont ajoutées à la politique gérée. Leur ajout donne l'autorisation d'obtenir des informations de catalogue à partir de AWS Glue.	3 décembre 2024
AmazonRedshiftServiceLinkedRolePolicy : mise à jour d'une politique existante	L'autorisation pour l'action `servicequotas:GetServiceQuota` est ajoutée à la politique gérée. Cela donne l'autorisation d'accéder aux quotas ou aux limites.	8 mars 2024
AmazonRedshiftQueryEditorV2FullAccess : mise à jour d'une politique existante	Les autorisations pour les actions `redshift-serverless:ListNamespaces` et `redshift-serverless:ListWorkgroups` sont ajoutées à la politique gérée. Leur ajout donne l'autorisation de répertorier les espaces de noms et les groupes de travail sans serveur dans l'entrepôt de données Amazon Redshift.	21 février 2024

Modifier	Description	Date
AmazonRedshiftQueryEditorV2NoSharing : mise à jour d'une politique existante	Les autorisations pour les actions `redshift-serverless:ListNamespaces` et `redshift-serverless:ListWorkgroups` sont ajoutées à la politique gérée. Leur ajout donne l'autorisation de répertorier les espaces de noms et les groupes de travail sans serveur dans l'entrepôt de données Amazon Redshift.	21 février 2024
AmazonRedshiftQueryEditorV2ReadSharing : mise à jour d'une politique existante	Les autorisations pour les actions `redshift-serverless:ListNamespaces` et `redshift-serverless:ListWorkgroups` sont ajoutées à la politique gérée. Leur ajout donne l'autorisation de répertorier les espaces de noms et les groupes de travail sans serveur dans l'entrepôt de données Amazon Redshift.	21 février 2024

Modifier	Description	Date
AmazonRedshiftQueryEditorV2ReadWriteSharing : mise à jour d'une politique existante	Les autorisations pour les actions `redshift-serverless:ListNamespaces` et `redshift-serverless:ListWorkgroups` sont ajoutées à la politique gérée. Leur ajout donne l'autorisation de répertorier les espaces de noms et les groupes de travail sans serveur dans l'entrepôt de données Amazon Redshift.	21 février 2024
AmazonRedshiftReadOnlyAccess : mise à jour d'une politique existante	L'autorisation pour l'action `redshift:ListRecommendations` est ajoutée à la politique gérée. Cela donne l'autorisation de répertorier les recommandations d'Amazon Redshift Advisor.	7 février 2024
AmazonRedshiftServiceLinkedRolePolicy : mise à jour d'une politique existante	Les autorisations pour les actions `ec2:AssignIpv6Addresses` et `ec2:UnassignIpv6Addresses` sont ajoutées à la politique gérée. Leur ajout donne l'autorisation d'attribuer des adresses IP ou d'annuler leur attribution.	31 octobre 2023

Modifier	Description	Date
AmazonRedshiftQueryEditorV2NoSharing : mise à jour d'une politique existante	Les autorisations pour les actions `sqlworkbench:GetAutocompletionMetadata` et `sqlworkbench:GetAutocompletionResource` sont ajoutées à la politique gérée. Leur ajout permet de générer et de récupérer des informations de base de données pour la saisie automatique du code SQL lors de la modification des requêtes.	16 août 2023
AmazonRedshiftQueryEditorV2ReadSharing : mise à jour d'une politique existante	Les autorisations pour les actions `sqlworkbench:GetAutocompletionMetadata` et `sqlworkbench:GetAutocompletionResource` sont ajoutées à la politique gérée. Leur ajout permet de générer et de récupérer des informations de base de données pour la saisie automatique du code SQL lors de la modification des requêtes.	16 août 2023

Modifier	Description	Date
AmazonRedshiftQueryEditorV2ReadWriteSharing : mise à jour d'une politique existante	Les autorisations pour les actions `sqlworkbench:GetAutocompletionMetadata` et `sqlworkbench:GetAutocompletionResource` sont ajoutées à la politique gérée. Leur ajout permet de générer et de récupérer des informations de base de données pour la saisie automatique du code SQL lors de la modification des requêtes.	16 août 2023

Modifier	Description	Date
AmazonRedshiftServiceLinkedRolePolicy : mise à jour d'une politique existante	Les autorisations pour les actions visant AWS Secrets Manager à créer et à gérer des secrets sont ajoutées à la politique gérée. Les autorisations ajoutées sont les suivantes : • `secretsmanager:GetRandomPassword` • `secretsmanager:DescribeSecret` • `secretsmanager:PutSecretValue` • `secretsmanager:UpdateSecret` • `secretsmanager:UpdateSecretVersionStage` • `secretsmanager:RotateSecret` • `secretsmanager:DeleteSecret`	14 août 2023

Modifier	Description	Date
AmazonRedshiftServiceLinkedRolePolicy : mise à jour d'une politique existante	Les autorisations pour les actions de création et de gestion de groupes de sécurité et de règles de routage dans Amazon EC2 sont supprimées de la politique gérée. Ces autorisations portaient sur la création de sous-réseaux et de VPC. Les autorisations supprimées sont les suivantes : • `ec2:AuthorizeSecurityGroupEgress` • `ec2:AuthorizeSecurityGroupIngress` • `ec2:UpdateSecurityGroupRuleDescriptionsEgress` • `ec2:ReplaceRouteTableAssociation` • `ec2:CreateRouteTable` • `ec2:AttachInternetGateway` • `ec2:UpdateSecurityGroupRuleDescriptionsIngress` • `ec2:AssociateRouteTable` • `ec2:RevokeSecurityGroupIngress` • `ec2:CreateRoute`	8 mai 2023

Modifier	Description	Date
	• `ec2:CreateSecurityGroup` • `ec2:RevokeSecurityGroupEgress` • `ec2:ModifyVpcAttribute` • `ec2:CreateSubnet` • `ec2:CreateInternetGateway` • `ec2:CreateVpc` Ils étaient associés à la balise Purpose:RedshiftMigrateToVpc de ressource. L'identification limitait la portée des autorisations à des tâches de migration d'Amazon EC2 Classic vers Amazon EC2 VPC. Pour plus d'informations sur les balises de ressources, consultez la section Contrôle de l'accès aux AWS ressources à l'aide de balises.	

Modifier	Description	Date
AmazonRedshiftDataFullAccess : mise à jour d'une politique existante	L'autorisation pour l'action `redshift:GetClusterCredentialsWithIAM` est ajoutée à la politique gérée. En l'ajoutant, on accorde l'autorisation d'obtenir des informations d'identification temporaires améliorées pour accéder à une base de données Amazon Redshift par l'utilisateur spécifié Compte AWS.	7 avril 2023
AmazonRedshiftServiceLinkedRolePolicy : mise à jour d'une politique existante	Les autorisations relatives aux actions sur Amazon EC2 pour la création et la gestion des règles de groupe de sécurité sont ajoutées à la politique gérée. Ces groupes et règles de sécurité sont spécifiquement associés à la balise de ressource Amazon Redshift `aws:RequestTag/Redshift` . Cela permet de limiter l'étendue des autorisations à des ressources Amazon Redshift spécifiques.	6 avril 2023

Modifier	Description	Date
AmazonRedshiftQueryEditorV2NoSharing : mise à jour d'une politique existante	L'autorisation pour l'action `sqlworkbench:GetSchemaInference` est ajoutée à la politique gérée. En l'ajoutant, vous obtenez l'autorisation d'obtenir les colonnes et les types de données déduits d'un fichier.	21 mars 2023
AmazonRedshiftQueryEditorV2ReadSharing : mise à jour d'une politique existante	L'autorisation pour l'action `sqlworkbench:GetSchemaInference` est ajoutée à la politique gérée. En l'ajoutant, vous obtenez l'autorisation d'obtenir les colonnes et les types de données déduits d'un fichier.	21 mars 2023
AmazonRedshiftQueryEditorV2ReadWriteSharing : mise à jour d'une politique existante	L'autorisation pour l'action `sqlworkbench:GetSchemaInference` est ajoutée à la politique gérée. En l'ajoutant, vous obtenez l'autorisation d'obtenir les colonnes et les types de données déduits d'un fichier.	21 mars 2023

Modifier	Description	Date
AmazonRedshiftQueryEditorV2NoSharing : mise à jour d'une politique existante	L'autorisation pour l'action `sqlworkbench:AssociateNotebookWithTab` est ajoutée à la politique gérée. Son ajout a pour effet d'accorder l'autorisation de créer et de mettre à jour des onglets liés au propre bloc-notes d'un utilisateur.	2 février 2023
AmazonRedshiftQueryEditorV2ReadSharing : mise à jour d'une politique existante	L'autorisation pour l'action `sqlworkbench:AssociateNotebookWithTab` est ajoutée à la politique gérée. Son ajout a pour effet d'accorder l'autorisation de créer et de mettre à jour des onglets liés au propre bloc-notes d'un utilisateur ou au bloc-notes partagé avec ce dernier.	2 février 2023
AmazonRedshiftQueryEditorV2ReadWriteSharing : mise à jour d'une politique existante	L'autorisation pour l'action `sqlworkbench:AssociateNotebookWithTab` est ajoutée à la politique gérée. Son ajout a pour effet d'accorder l'autorisation de créer et de mettre à jour des onglets liés au propre bloc-notes d'un utilisateur ou au bloc-notes partagé avec ce dernier.	2 février 2023

Modifier	Description	Date
AmazonRedshiftQueryEditorV2NoSharing : mise à jour d'une politique existante	Pour autoriser l'utilisation de blocs-notes, Amazon Redshift a ajouté l'autorisation pour les actions suivantes : • `sqlworkbench:ListNotebooks` • `sqlworkbench:CreateNotebook` • `sqlworkbench:DuplicateNotebook` • `sqlworkbench:CreateNotebookFromVersion` • `sqlworkbench:ImportNotebook` • `sqlworkbench:GetNotebook` • `sqlworkbench:UpdateNotebook` • `sqlworkbench:DeleteNotebook` • `sqlworkbench:CreateNotebookCell` • `sqlworkbench:DeleteNotebookCell` • `sqlworkbench:UpdateNotebookCellContent` • `sqlworkbench:UpdateNotebookCellLayout`	17 octobre 2022

Modifier	Description	Date
	• sqlworkbench:BatchGetNotebookCell • sqlworkbench:ListNotebookVersions • sqlworkbench:CreateNotebookVersion • sqlworkbench:GetNotebookVersion • sqlworkbench:DeleteNotebookVersion • sqlworkbench:RestoreNotebookVersion • sqlworkbench:ExportNotebook	

Modifier	Description	Date
AmazonRedshiftQueryEditorV2ReadSharing : mise à jour d'une politique existante	Pour autoriser l'utilisation de blocs-notes, Amazon Redshift a ajouté l'autorisation pour les actions suivantes : • `sqlworkbench:ListNotebooks` • `sqlworkbench:CreateNotebook` • `sqlworkbench:DuplicateNotebook` • `sqlworkbench:CreateNotebookFromVersion` • `sqlworkbench:ImportNotebook` • `sqlworkbench:GetNotebook` • `sqlworkbench:UpdateNotebook` • `sqlworkbench:DeleteNotebook` • `sqlworkbench:CreateNotebookCell` • `sqlworkbench:DeleteNotebookCell` • `sqlworkbench:UpdateNotebookCellContent` • `sqlworkbench:UpdateNotebookCellLayout`	17 octobre 2022

Modifier	Description	Date
	• sqlworkbench:BatchGetNotebookCell • sqlworkbench:ListNotebookVersions • sqlworkbench:CreateNotebookVersion • sqlworkbench:GetNotebookVersion • sqlworkbench:DeleteNotebookVersion • sqlworkbench:RestoreNotebookVersion • sqlworkbench:ExportNotebook	

Modifier	Description	Date
AmazonRedshiftQueryEditorV2ReadWriteSharing : mise à jour d'une politique existante	Pour autoriser l'utilisation de blocs-notes, Amazon Redshift a ajouté l'autorisation pour les actions suivantes : • `sqlworkbench:ListNotebooks` • `sqlworkbench:CreateNotebook` • `sqlworkbench:DuplicateNotebook` • `sqlworkbench:CreateNotebookFromVersion` • `sqlworkbench:ImportNotebook` • `sqlworkbench:GetNotebook` • `sqlworkbench:UpdateNotebook` • `sqlworkbench:DeleteNotebook` • `sqlworkbench:CreateNotebookCell` • `sqlworkbench:DeleteNotebookCell` • `sqlworkbench:UpdateNotebookCellContent` • `sqlworkbench:UpdateNotebookCellLayout`	17 octobre 2022

Modifier	Description	Date
	• `sqlworkbench:BatchGetNotebookCell` • `sqlworkbench:ListNotebookVersions` • `sqlworkbench:CreateNotebookVersion` • `sqlworkbench:GetNotebookVersion` • `sqlworkbench:DeleteNotebookVersion` • `sqlworkbench:RestoreNotebookVersion` • `sqlworkbench:ExportNotebook`	
AmazonRedshiftServiceLinkedRolePolicy : mise à jour d'une politique existante	Amazon Redshift a ajouté l'espace de noms `AWS/Redshift` pour permettre la publication de métriques vers. CloudWatch	29 septembre 2022
AmazonRedshiftQueryEditorV2NoSharing : mise à jour d'une politique existante	Amazon Redshift a ajouté l'autorisation aux actions `sqlworkbench:ListQueryExecutionHistory` et `sqlworkbench:GetQueryExecutionHistory` . Cela permet de consulter l'historique des requêtes.	30 août 2022

Modifier	Description	Date
AmazonRedshiftQueryEditorV2ReadSharing : mise à jour d'une politique existante	Amazon Redshift a ajouté l'autorisation aux actions `sqlworkbench:ListQueryExecutionHistory` et `sqlworkbench:GetQueryExecutionHistory`. Cela permet de consulter l'historique des requêtes.	30 août 2022
AmazonRedshiftQueryEditorV2ReadWriteSharing : mise à jour d'une politique existante	Amazon Redshift a ajouté l'autorisation aux actions `sqlworkbench:ListQueryExecutionHistory` et `sqlworkbench:GetQueryExecutionHistory`. Cela permet de consulter l'historique des requêtes.	30 août 2022
AmazonRedshiftFullAccess : mise à jour d'une politique existante	Les autorisations pour Amazon Redshift Serverless sont ajoutées à la politique AmazonRedshiftFullAccess gérée existante.	22 juillet 2022

Modifier	Description	Date
AmazonRedshiftDataFullAccess : mise à jour d'une politique existante	Amazon Redshift a mis à jour la condition de portée par défaut `redshift-serverless:GetCredentials` de l'autorisation de la balise `aws:ResourceTag/RedshiftDataFullAccess` passant de `StringEquals` à `StringLike` pour accorder l'accès aux ressources marquées avec une clé de balise `RedshiftDataFullAccess` et n'importe quelle valeur de balise.	11 juillet 2022
AmazonRedshiftDataFullAccess : mise à jour d'une politique existante	Amazon Redshift a ajouté de nouvelles autorisations pour permettre à `redshift-serverless:GetCredentials` d'obtenir des informations d'identification temporaires pour Amazon Redshift sans serveur.	8 juillet 2022
AmazonRedshiftQueryEditorV2NoSharing : mise à jour d'une politique existante	Amazon Redshift a ajouté l'autorisation à l'action `sqlworkbench:GetAccountSettings` . Ceci accorde l'autorisation d'obtenir les paramètres de compte.	15 juin 2022

Modifier	Description	Date
AmazonRedshiftQueryEditorV2ReadSharing : mise à jour d'une politique existante	Amazon Redshift a ajouté l'autorisation à l'action `sqlworkbench:GetAccountSettings` . Ceci accorde l'autorisation d'obtenir les paramètres de compte.	15 juin 2022
AmazonRedshiftQueryEditorV2ReadWriteSharing : mise à jour d'une politique existante	Amazon Redshift a ajouté l'autorisation à l'action `sqlworkbench:GetAccountSettings` . Ceci accorde l'autorisation d'obtenir les paramètres de compte.	15 juin 2022
AmazonRedshiftServiceLinkedRolePolicy : mise à jour d'une politique existante	Pour permettre un accès public aux nouveaux points de terminaison Amazon Redshift sans serveur, Amazon Redshift attribue et associe des adresses IP élastiques à l'interface réseau élastique du point de terminaison de VPC dans le compte client. Il le fait par le biais des autorisations fournies par le rôle lié au service. Pour permettre ce cas d'utilisation, les actions d'allocation et de libération d'une adresse IP élastique sont ajoutées au rôle lié au service Amazon Redshift sans serveur.	26 mai 2022

Modifier	Description	Date
AmazonRedshiftQueryEditorV2FullAccess : mise à jour d'une politique existante	Autorisations pour l'action `sqlworkbench:ListTaggedResources` . Elles s'appliquent spécifiquement aux ressources de l'éditeur de requête v2 Amazon Redshift. Cette mise à jour de la politique donne le droit d'appeler `tag:GetResources` uniquement via l'éditeur de requête v2.	22 février 2022
AmazonRedshiftQueryEditorV2NoSharing : mise à jour d'une politique existante	Autorisations pour l'action `sqlworkbench:ListTaggedResources` . Elles s'appliquent spécifiquement aux ressources de l'éditeur de requête v2 Amazon Redshift. Cette mise à jour de la politique donne le droit d'appeler `tag:GetResources` uniquement via l'éditeur de requête v2.	22 février 2022
AmazonRedshiftQueryEditorV2ReadSharing : mise à jour d'une politique existante	Autorisations pour l'action `sqlworkbench:ListTaggedResources` . Elles s'appliquent spécifiquement aux ressources de l'éditeur de requête v2 Amazon Redshift. Cette mise à jour de la politique donne le droit d'appeler `tag:GetResources` uniquement via l'éditeur de requête v2.	22 février 2022

Modifier	Description	Date
AmazonRedshiftQueryEditorV2ReadWriteSharing : mise à jour d'une politique existante	Autorisations pour l'action `sqlworkbench:ListTaggedResources` . Elles s'appliquent spécifiquement aux ressources de l'éditeur de requête v2 Amazon Redshift. Cette mise à jour de la politique donne le droit d'appeler `tag:GetResources` uniquement via l'éditeur de requête v2.	22 février 2022
AmazonRedshiftQueryEditorV2ReadSharing : mise à jour d'une politique existante	L'autorisation pour l'action `sqlworkbench:AssociateQueryWithTab` est ajoutée à la politique gérée. L'ajout permet aux clients de créer des onglets d'éditeur liés à une requête partagée avec eux.	22 février 2022
AmazonRedshiftServiceLinkedRolePolicy : mise à jour d'une politique existante	Amazon Redshift a ajouté des autorisations pour de nouvelles actions afin de permettre la gestion du réseau Amazon Redshift et des ressources VPC.	22 novembre 2021

Modifier	Description	Date
AmazonRedshiftAllCommandsFullAccess – Nouvelle politique	Amazon Redshift a ajouté une nouvelle v permettant d'utiliser le rôle IAM créé à partir de la console Amazon Redshift et de le définir comme valeur par défaut pour que le cluster exécute les commandes COPY depuis Amazon S3, UNLOAD, CREATE EXTERNAL SCHEMA, CREATE EXTERNAL FUNCTION, CREATE MODEL ou CREATE LIBRARY.	18 novembre 2021
AmazonRedshiftServiceLinkedRolePolicy : mise à jour d'une politique existante	Amazon Redshift a ajouté des autorisations pour de nouvelles actions afin de permettre la gestion des groupes de journaux et des flux de CloudWatch journaux Amazon Redshift, y compris l'exportation des journaux d'audit.	15 novembre 2021
AmazonRedshiftFullAccess : mise à jour d'une politique existante	Amazon Redshift a ajouté de nouvelles autorisations pour permettre l'explicabilité du modèle, DynamoDB, Redshift Spectrum et la fédération Amazon RDS.	7 octobre 2021

Modifier	Description	Date
AmazonRedshiftQueryEditorV2FullAccess – Nouvelle politique	Amazon Redshift a ajouté une nouvelle politique permettant un accès complet à l'éditeur de requête Amazon Redshift v2.	24 septembre 2021
AmazonRedshiftQueryEditorV2NoSharing – Nouvelle politique	Amazon Redshift a ajouté une nouvelle politique permettant d'utiliser l'éditeur de requête Amazon Redshift v2 sans partager de ressources.	24 septembre 2021
AmazonRedshiftQueryEditorV2ReadSharing – Nouvelle politique	Amazon Redshift a ajouté une nouvelle politique pour autoriser le partage de lecture dans l'éditeur de requête Amazon Redshift v2.	24 septembre 2021
AmazonRedshiftQueryEditorV2ReadWriteSharing – Nouvelle politique	Amazon Redshift a ajouté une nouvelle politique permettant le partage de lecture et de mise à jour dans l'éditeur de requête Amazon Redshift v2.	24 septembre 2021
AmazonRedshiftFullAccess : mise à jour d'une politique existante	Amazon Redshift a ajouté de nouvelles autorisations pour autoriser `sagemaker:*Job*` .	18 août 2021
AmazonRedshiftDataFullAccess : mise à jour d'une politique existante	Amazon Redshift a ajouté de nouvelles autorisations pour autoriser `AuthorizeDataShare` .	12 août 2021

Modifier	Description	Date
AmazonRedshiftDataFullAccess : mise à jour d'une politique existante	Amazon Redshift a ajouté de nouvelles autorisations pour autoriser `BatchExecuteStatement` .	27 Juillet 2021
Amazon Redshift a activé le suivi des modifications	Amazon Redshift a commencé à suivre les modifications apportées à ses politiques AWS gérées.	27 Juillet 2021

AmazonRedshiftReadOnlyAccess

Permet d'accéder en lecture seule à toutes les ressources Amazon Redshift d'un compte. AWS

Vous trouverez la AmazonRedshiftReadOnlyAccess politique sur la console IAM et AmazonRedshiftReadOnlyAccess dans le AWS Managed Policy Reference Guide.

AmazonRedshiftFullAccess

Donne un accès complet à toutes les ressources Amazon Redshift associées à un AWS compte. De plus, cette politique accorde un accès complet à toutes les ressources Amazon Redshift sans serveur.

Vous trouverez la AmazonRedshiftFullAccess politique sur la console IAM et AmazonRedshiftFullAccess dans le AWS Managed Policy Reference Guide.

AmazonRedshiftQueryEditor

AmazonRedshiftQueryEditor – Accorde un accès complet à l'éditeur de requête dans la console Amazon Redshift.

Vous trouverez la AmazonRedshiftQueryEditor politique sur la console IAM et AmazonRedshiftQueryEditor dans le AWS Managed Policy Reference Guide.

AmazonRedshiftDataFullAccess

Accorde un accès complet aux opérations et aux ressources de l'API Amazon Redshift Data pour un AWS compte.

Vous trouverez la AmazonRedshiftDataFullAccess politique sur la console IAM et AmazonRedshiftDataFullAccess dans le AWS Managed Policy Reference Guide.

AmazonRedshiftQueryEditorV2FullAccess

Accorde un accès complet aux opérations et ressources de l'éditeur de requête Amazon Redshift v2. Cette politique permet également d'accéder à d'autres services requis.

Vous trouverez la AmazonRedshiftQueryEditorV2FullAccess politique sur la console IAM et AmazonRedshiftQueryEditorV2FullAccess dans le AWS Managed Policy Reference Guide.

AmazonRedshiftQueryEditorV2NoSharing

Permet de travailler avec l'éditeur de requête Amazon Redshift v2 sans partager de ressources. Cette politique permet également d'accéder à d'autres services requis. Le principal utilisant cette politique ne peut pas étiqueter ses ressources (telles que des requêtes) pour les partager avec d'autres principaux dans le même Compte AWS.

Vous trouverez la AmazonRedshiftQueryEditorV2NoSharing politique sur la console IAM et AmazonRedshiftQueryEditorV2NoSharing dans le AWS Managed Policy Reference Guide.

AmazonRedshiftQueryEditorV2ReadSharing

Permet de travailler avec l'éditeur de requête Amazon Redshift v2 avec un partage limité des ressources. Cette politique permet également d'accéder à d'autres services requis. Le principal utilisant cette politique peut étiqueter ses ressources (telles que des requêtes) pour les partager avec d'autres principaux dans le même Compte AWS. Le principal autorisé peut lire les ressources partagées avec son équipe, mais ne peut pas les mettre à jour.

Vous trouverez la AmazonRedshiftQueryEditorV2ReadSharing politique sur la console IAM et AmazonRedshiftQueryEditorV2ReadSharing dans le AWS Managed Policy Reference Guide.

AmazonRedshiftQueryEditorV2ReadWriteSharing

Permet de travailler avec l'éditeur de requête Amazon Redshift v2 avec le partage de ressources. Cette politique permet également d'accéder à d'autres services requis. Le principal utilisant cette politique peut étiqueter ses ressources (telles que des requêtes) pour les partager avec d'autres principaux dans le même Compte AWS. Le principal autorisé peut lire et mettre à jour les ressources partagées avec son équipe.

Vous trouverez la AmazonRedshiftQueryEditorV2ReadWriteSharing politique sur la console IAM et AmazonRedshiftQueryEditorV2ReadWriteSharing dans le AWS Managed Policy Reference Guide.

AmazonRedshiftServiceLinkedRolePolicy

Vous ne pouvez pas vous connecter AmazonRedshiftServiceLinkedRolePolicy à vos entités IAM. Cette politique est associée à un rôle lié au service qui permet à Amazon Redshift d'accéder aux ressources du compte. Pour plus d'informations, consultez Utilisation des rôles liés à un service pour Amazon Redshift.

Vous trouverez la AmazonRedshiftServiceLinkedRolePolicy politique sur la console IAM et AmazonRedshiftServiceLinkedRolePolicy dans le AWS Managed Policy Reference Guide.

AmazonRedshiftAllCommandsFullAccess

Permet d'utiliser le rôle IAM créé à partir de la console Amazon Redshift et de le définir comme valeur par défaut pour que le cluster exécute les commandes COPY à partir d'Amazon S3, UNLOAD, CREATE EXTERNAL SCHEMA, CREATE EXTERNAL FUNCTION et CREATE MODEL. La politique accorde également l'autorisation d'exécuter des instructions SELECT pour des services connexes, tels qu'Amazon S3, CloudWatch Logs, Amazon SageMaker AI ou AWS Glue.

Vous trouverez la AmazonRedshiftAllCommandsFullAccess politique sur la console IAM et AmazonRedshiftAllCommandsFullAccess dans le AWS Managed Policy Reference Guide.

AmazonRedshiftFederatedAuthorization

La politique consolide les actions IAM nécessaires pour exécuter une requête dans une base de données Glue Data Catalog avec les autorisations fédérées Amazon Redshift. Cette requête passe par AWS Glue et nécessite donc des actions Obtenir sur les objets du catalogue pour découvrir les objets, et des actions Créer, mettre à jour, renommer et supprimer pour modifier les objets. Notez que les ressources sont gérées par Amazon Redshift. Par conséquent, le principal aura également besoin des autorisations Redshift pour terminer la requête. `glue:FederateAuthorization`L'action permet à AWS Glue de déléguer les décisions d'autorisation concernant les objets du catalogue à Amazon Redshift.

Cette politique permet au principal d'exécuter des requêtes sur le catalogue avec les autorisations fédérées Amazon Redshift, mais n'autorise pas l'enregistrement et la désinscription de l'espace de noms Amazon Redshift auprès de Glue. AWS Consultez la documentation sur les exigences en matière de politique IAM pour la configuration des autorisations fédérées Amazon Redshift.

Vous trouverez la AmazonRedshiftFederatedAuthorization politique sur la console IAM et AmazonRedshiftFederatedAuthorization dans le AWS Managed Policy Reference Guide.

Vous pouvez également créer vos propres politiques IAM personnalisées pour autoriser les autorisations pour les opérations et les ressources de l'API Amazon Redshift. Vous pouvez attacher ces politiques personnalisées aux rôles ou groupes IAM qui nécessitent ces autorisations.

Autorisations requises pour utiliser Redshift Spectrum

Amazon Redshift Spectrum nécessite des autorisations pour d'autres AWS services pour accéder aux ressources. Pour plus de détails sur les autorisations dans les politiques IAM pour Redshift Spectrum, consultez Politiques IAM pour Amazon Redshift Spectrum dans le Guide du développeur de bases de données Amazon Redshift.

Autorisations requises pour utiliser la console Amazon Redshift

Pour qu'un utilisateur puisse utiliser la console Amazon Redshift, il doit disposer d'un ensemble minimum d'autorisations lui permettant de décrire les ressources Amazon Redshift de son AWS compte. Ces autorisations doivent également permettre à l'utilisateur de décrire d'autres informations connexes, notamment la sécurité Amazon EC2, Amazon CloudWatch, Amazon SNS et les informations réseau.

Si vous créez une politique IAM plus restrictive que les autorisations minimales requises, la console ne fonctionne pas comme prévu pour les utilisateurs dotés de cette politique IAM. Pour que ces utilisateurs puissent toujours utiliser la console Amazon Redshift, attachez également la politique gérée `AmazonRedshiftReadOnlyAccess` à l'utilisateur. La procédure à suivre est décrite dans la section AWS politiques gérées pour Amazon Redshift.

Pour plus d'informations sur l'accès d'un utilisateur à l'éditeur de requêtes sur la console Amazon Redshift, consultez Autorisations requises pour utiliser l'éditeur de requêtes de la console Amazon Redshift.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API Amazon Redshift AWS CLI ou l'API Amazon Redshift.

Autorisations requises pour utiliser l’éditeur de requêtes de la console Amazon Redshift

Pour qu’un utilisateur puisse travailler avec l’éditeur de requêtes Amazon Redshift, cet utilisateur doit disposer d’un ensemble minimum d’autorisations pour les opérations d’API de données Amazon Redshift et Amazon Redshift. Pour vous connecter à une base de données à l’aide d’un secret, vous devez également disposer des autorisations Secrets Manager.

Pour permettre à un utilisateur d'accéder à l'éditeur de requêtes sur la console Amazon Redshift, joignez les règles `AmazonRedshiftQueryEditor` et les politiques `AmazonRedshiftReadOnlyAccess` AWS gérées. La politique `AmazonRedshiftQueryEditor` accorde l’autorisation à l’utilisateur de récupérer les résultats de ses propres instructions SQL uniquement. C'est-à-dire des déclarations soumises par le même organisme, `aws:userid` comme indiqué dans cette section de la politique `AmazonRedshiftQueryEditor` AWS gérée.

```
{
    "Sid":"DataAPIIAMStatementPermissionsRestriction",
    "Action": [
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:ListStatements"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "redshift-data:statement-owner-iam-userid": "${aws:userid}"
        }
    }
}
```

Pour permettre à un utilisateur de récupérer les résultats des instructions SQL d’autres personnes dans le même rôle IAM, créez votre propre politique sans la condition de limiter l’accès à l’utilisateur actuel. Limitez également l’accès pour modifier une politique à un administrateur.

Autorisations requises pour utiliser l’éditeur de requête v2

Pour qu'un utilisateur puisse utiliser l'éditeur de requêtes Amazon Redshift v2, il doit disposer d'un ensemble minimum d'autorisations sur Amazon Redshift, les opérations de l'éditeur de requêtes v2 et

d'autres AWS services tels que AWS Key Management Service AWS Secrets Manager, et le service de balisage.

Pour donner à un utilisateur un accès complet à l'éditeur de requêtes v2, joignez la politique `AmazonRedshiftQueryEditorV2FullAccess` AWS gérée. La politique `AmazonRedshiftQueryEditorV2FullAccess` donne à l'utilisateur l'autorisation de partager des ressources de l'éditeur de requête v2, telles que des requêtes, avec d'autres membres de la même équipe. Pour plus d'informations sur la façon dont l'accès aux ressources de l'éditeur de requête v2 est contrôlé, reportez-vous à la définition de la politique gérée spécifique pour l'éditeur de requête v2 dans la console IAM.

Certaines politiques AWS gérées par l'éditeur de requêtes Amazon Redshift v2 utilisent des AWS balises dans le cadre de certaines conditions pour définir l'accès aux ressources. Dans l'éditeur de requête v2, le partage des requêtes est basé sur la clé et la valeur de balise `"aws:ResourceTag/sqlworkbench-team": "${aws:PrincipalTag/sqlworkbench-team}"` dans la politique IAM attachée au principal (le rôle IAM). Les principaux dans le même Compte AWS avec la même valeur de balise (par exemple, `accounting-team`), font partie de la même équipe dans l'éditeur de requête v2. Vous ne pouvez être associé qu'à une seule équipe à la fois. Un utilisateur disposant d'autorisations administratives peut configurer des équipes dans la console IAM en attribuant à tous les membres de l'équipe la même valeur pour la balise `sqlworkbench-team`. Si la valeur de la balise de `sqlworkbench-team` est modifié pour un utilisateur IAM ou un rôle IAM, il peut y avoir un retard jusqu'à ce que la modification soit reflétée dans les ressources partagées. Si la valeur de balise d'une ressource (telle qu'une requête) est modifiée, il peut à nouveau y avoir un retard jusqu'à ce que la modification soit reflétée. Les membres de l'équipe doivent également posséder l'autorisation `tag:GetResources` pour le partage.

Exemple : pour ajouter le **`tag`** accounting-team pour un rôle IAM

1. Connectez-vous au Console de gestion AWS et ouvrez la console IAM à https://console.aws.amazon.com/iam/ l'adresse.
2. Dans le panneau de navigation de la console, choisissez Roles (Rôles), puis choisissez le nom du rôle que vous souhaitez modifier.
3. Choisissez l'onglet Tags (Balises), puis Add tags (Ajouter des balises).
4. Ajoutez la clé de balise sqlworkbench-team et la valeur `accounting-team`.
5. Sélectionnez Enregistrer les modifications.

Maintenant, lorsqu'un principal IAM (auquel ce rôle IAM est attaché) partage une requête avec l'équipe, d'autres principaux ayant la même valeur de balise `accounting-team` peuvent afficher la requête.

Pour plus d'informations sur la procédure d'attachement d'une balise à un principal, y compris les rôles IAM et les utilisateurs IAM, consultez Étiquetage des ressources IAM dans le Guide de l'utilisateur IAM.

Vous pouvez également configurer des équipes au niveau de la session à l'aide d'un fournisseur d'identité (IdP). Cela permet à plusieurs utilisateurs utilisant le même rôle IAM d'avoir une équipe différente. La politique d'approbation de rôle IAM doit permettre l'opération `sts:TagSession`. Pour plus d'informations, consultez Autorisations requises pour ajouter des balises de session dans le Guide de l'utilisateur IAM. Ajoutez l'attribut de balise principal à l'assertion SAML fournie par votre fournisseur d'identité.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:sqlworkbench-
team">
    <AttributeValue>accounting-team</AttributeValue>
</Attribute>
```

Suivez les instructions de votre fournisseur d'identité pour renseigner l'attribut SAML avec le contenu provenant de votre répertoire. Pour plus d'informations sur les fournisseurs d'identité (IdPs) et Amazon Redshift, consultez la section Fournisseurs d'identité Utilisation de l'authentification IAM pour générer des informations d'identification de l'utilisateur de base de données et fédération dans le guide de l'utilisateur IAM.

`sqlworkbench:CreateNotebookVersion` accorde l'autorisation d'obtenir le contenu actuel des cellules du bloc-notes et de créer une version du bloc-notes dans votre compte. Cela signifie qu'au moment de la création de la version, le contenu actuel du bloc-notes est le même que le contenu de la version. Par la suite, le contenu des cellules de la version reste le même lorsque le bloc-notes actuel est mis à jour. `sqlworkbench:GetNotebookVersion` accorde l'autorisation d'obtenir une version du bloc-notes. Un utilisateur qui n'a pas d'autorisation `sqlworkbench:BatchGetNotebookCell` mais qui a des autorisations `sqlworkbench:CreateNotebookVersion` et `sqlworkbench:GetNotebookVersion` sur un bloc-notes a accès aux cellules du bloc-notes de la version. Cet utilisateur sans autorisation `sqlworkbench:BatchGetNotebookCell` peut toujours récupérer le contenu des cellules d'un bloc-notes en créant d'abord une version, puis en obtenant cette version créée.

Autorisations requises pour utiliser le planificateur Amazon Redshift

Lorsque vous utilisez le planificateur Amazon Redshift, vous configurez un rôle IAM avec une relation de confiance avec le planificateur Amazon Redshift (**`scheduler.redshift.amazonaws.com`**) pour permettre à ce dernier d'assumer des autorisations en votre nom. Vous attachez également une politique (autorisations) au rôle pour les opérations de l'API Amazon Redshift que vous souhaitez planifier.

L'exemple suivant montre le document de politique au format JSON pour configurer une relation de confiance avec le planificateur Amazon Redshift et Amazon Redshift.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "scheduler.redshift.amazonaws.com",
                    "redshift.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Pour plus d'informations sur les entités de confiance, consultez la section Création d'un rôle pour déléguer des autorisations à un AWS service dans le Guide de l'utilisateur IAM.

Vous devez également ajouter des autorisations pour les opérations Amazon Redshift que vous souhaitez planifier.

Pour que le planificateur utilise l'opération `ResizeCluster`, ajoutez une autorisation similaire à ce qui suit dans votre politique IAM. Selon votre environnement, vous pouvez rendre la politique plus restrictive.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "redshift:ResizeCluster",
            "Resource": "*"
        }
    ]
}
```

Pour savoir comment créer un rôle pour le planificateur Amazon Redshift, consultez la section Création d'un rôle pour un AWS service (console) dans le guide de l'utilisateur IAM. Effectuez ces choix lorsque vous créez un rôle dans la console IAM :

- Pour Choisir le service qui utilisera ce rôle, choisissez Redshift.
- Pour Sélectionner votre cas d'utilisation, choisissez Redshift - Planificateur.
- Créez ou attachez une politique au rôle qui permet de planifier une opération Amazon Redshift. Choisissez Créer une politique ou modifiez le rôle pour attacher une politique. Entrez la politique JSON pour l'opération à planifier.
- Après avoir créé le rôle, modifiez la Relation de confiance du rôle IAM de façon à inclure le service `redshift.amazonaws.com`.

Le rôle IAM que vous créez a des entités fiables de `scheduler.redshift.amazonaws.com` et `redshift.amazonaws.com`. Il a également une politique jointe qui autorise une action API Amazon Redshift prise en charge, telle que, `"redshift:ResizeCluster"`.

Autorisations requises pour utiliser le EventBridge planificateur Amazon

Lorsque vous utilisez le EventBridge planificateur Amazon, vous configurez un rôle IAM avec une relation de confiance avec le EventBridge planificateur (**`events.amazonaws.com`**) pour permettre au planificateur d'assumer les autorisations en votre nom. Vous associez également une politique (autorisations) au rôle pour les opérations de l'API Amazon Redshift Data que vous souhaitez planifier et une politique pour les EventBridge opérations Amazon.

Vous utilisez le EventBridge planificateur lorsque vous créez des requêtes planifiées à l'aide de l'éditeur de requêtes Amazon Redshift sur la console.

Vous pouvez créer un rôle IAM pour exécuter des requêtes planifiées sur la console IAM. Dans ce rôle IAM, attachez `AmazonEventBridgeFullAccess` et `AmazonRedshiftDataFullAccess`.

L'exemple suivant montre le document de politique au format JSON pour établir une relation de confiance avec le EventBridge planificateur.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "events.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Pour plus d'informations sur les entités de confiance, consultez la section Création d'un rôle pour déléguer des autorisations à un AWS service dans le Guide de l'utilisateur IAM.

Pour savoir comment créer un rôle pour le EventBridge planificateur, consultez la section Création d'un rôle pour un AWS service (console) dans le Guide de l'utilisateur IAM. Effectuez ces choix lorsque vous créez un rôle dans la console IAM :

- Pour Choisissez le service qui utilisera ce rôle : Choisissez CloudWatch les événements.
- Pour Sélectionnez votre cas d'utilisation : Choisissez CloudWatch Events.
- Attachez les politiques de autorisation suivantes : `AmazonEventBridgeFullAccess` et `AmazonRedshiftDataFullAccess`.

Le rôle IAM que vous créez a une entité de confiance de `events.amazonaws.com`. Il possède également une politique jointe qui autorise les actions de l'API de données Amazon Redshift prises en charge, telles que `"redshift-data:*"`.

Autorisations requises pour utiliser le machine learning (ML) Amazon Redshift

Vous trouverez ci-après une description des autorisations requises pour utiliser le machine learning (ML) Amazon Redshift pour différents cas d'utilisation.

Pour que vos utilisateurs puissent utiliser Amazon Redshift ML avec Amazon SageMaker AI, créez un rôle IAM avec une politique plus restrictive que celle par défaut. Vous pouvez utiliser la politique suivante : Vous pouvez également modifier cette politique afin de répondre à vos besoins.

La politique suivante indique les autorisations requises pour exécuter SageMaker AI Autopilot avec une explicabilité du modèle à partir d'Amazon Redshift.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateTrainingJob",
                "sagemaker:CreateAutoMLJob",
                "sagemaker:CreateCompilationJob",
                "sagemaker:CreateEndpoint",
                "sagemaker:DescribeAutoMLJob",
                "sagemaker:DescribeTrainingJob",
                "sagemaker:DescribeCompilationJob",
                "sagemaker:DescribeProcessingJob",
                "sagemaker:DescribeTransformJob",
                "sagemaker:ListCandidatesForAutoMLJob",
                "sagemaker:StopAutoMLJob",
                "sagemaker:StopCompilationJob",
                "sagemaker:StopTrainingJob",
                "sagemaker:DescribeEndpoint",
                "sagemaker:InvokeEndpoint",
                "sagemaker:StopProcessingJob",
                "sagemaker:CreateModel",
                "sagemaker:CreateProcessingJob"
```

```
            ],
            "Resource": [
                "arn:aws:sagemaker:*:*:model/*redshift*",
                "arn:aws:sagemaker:*:*:training-job/*redshift*",
                "arn:aws:sagemaker:*:*:automl-job/*redshift*",
                "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
                "arn:aws:sagemaker:*:*:processing-job/*redshift*",
                "arn:aws:sagemaker:*:*:transform-job/*redshift*",
                "arn:aws:sagemaker:*:*:endpoint/*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/
*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/
*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/
*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "SageMaker",
                        "/aws/sagemaker/Endpoints",
                        "/aws/sagemaker/ProcessingJobs",
                        "/aws/sagemaker/TrainingJobs",
                        "/aws/sagemaker/TransformJobs"
                    ]
```

```
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr:BatchCheckLayerAvailability",
                "ecr:BatchGetImage",
                "ecr:GetAuthorizationToken",
                "ecr:GetDownloadUrlForLayer"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetBucketAcl",
                "s3:GetBucketCors",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:PutBucketCors",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload",
                "s3:CreateBucket"
            ],
            "Resource": [
                "arn:aws:s3:::redshift-downloads",
                "arn:aws:s3:::redshift-downloads/*",
                "arn:aws:s3:::*redshift*",
                "arn:aws:s3:::*redshift*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetBucketAcl",
```

```
                "s3:GetBucketCors",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:PutBucketCors",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload",
                "s3:CreateBucket"
            ],
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "s3:ExistingObjectTag/Redshift": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "redshift.amazonaws.com",
                        "sagemaker.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

La politique suivante indique les autorisations minimales complètes pour autoriser l’accès à Amazon DynamoDB, Redshift Spectrum et à la fédération Amazon RDS.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateTrainingJob",
                "sagemaker:CreateAutoMLJob",
                "sagemaker:CreateCompilationJob",
                "sagemaker:CreateEndpoint",
                "sagemaker:DescribeAutoMLJob",
                "sagemaker:DescribeTrainingJob",
                "sagemaker:DescribeCompilationJob",
                "sagemaker:DescribeProcessingJob",
                "sagemaker:DescribeTransformJob",
                "sagemaker:ListCandidatesForAutoMLJob",
                "sagemaker:StopAutoMLJob",
                "sagemaker:StopCompilationJob",
                "sagemaker:StopTrainingJob",
                "sagemaker:DescribeEndpoint",
                "sagemaker:InvokeEndpoint",
                "sagemaker:StopProcessingJob",
                "sagemaker:CreateModel",
                "sagemaker:CreateProcessingJob"
            ],
            "Resource": [
                "arn:aws:sagemaker:*:*:model/*redshift*",
                "arn:aws:sagemaker:*:*:training-job/*redshift*",
                "arn:aws:sagemaker:*:*:automl-job/*redshift*",
                "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
                "arn:aws:sagemaker:*:*:processing-job/*redshift*",
                "arn:aws:sagemaker:*:*:transform-job/*redshift*",
                "arn:aws:sagemaker:*:*:endpoint/*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
```

```
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/
*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/
*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/
*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "SageMaker",
                        "/aws/sagemaker/Endpoints",
                        "/aws/sagemaker/ProcessingJobs",
                        "/aws/sagemaker/TrainingJobs",
                        "/aws/sagemaker/TransformJobs"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr:BatchCheckLayerAvailability",
                "ecr:BatchGetImage",
                "ecr:GetAuthorizationToken",
                "ecr:GetDownloadUrlForLayer"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
```

```
                "s3:GetBucketAcl",
                "s3:GetBucketCors",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:PutBucketCors",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload",
                "s3:CreateBucket"
            ],
            "Resource": [
                "arn:aws:s3:::redshift-downloads",
                "arn:aws:s3:::redshift-downloads/*",
                "arn:aws:s3:::*redshift*",
                "arn:aws:s3:::*redshift*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetBucketAcl",
                "s3:GetBucketCors",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:PutBucketCors",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload",
                "s3:CreateBucket"
            ],
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {
```

```
                "s3:ExistingObjectTag/Redshift": "true"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "dynamodb:Scan",
            "dynamodb:DescribeTable",
            "dynamodb:Getitem"
        ],
        "Resource": [
            "arn:aws:dynamodb:*:*:table/*redshift*",
            "arn:aws:dynamodb:*:*:table/*redshift*/index/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "elasticmapreduce:ListInstances"
        ],
        "Resource": [
            "arn:aws:elasticmapreduce:*:*:cluster/*redshift*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "elasticmapreduce:ListInstances"
        ],
        "Resource": "*",
        "Condition": {
            "StringEqualsIgnoreCase": {
                "elasticmapreduce:ResourceTag/Redshift": "true"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "lambda:InvokeFunction"
        ],
        "Resource": "arn:aws:lambda:*:*:function:*redshift*"
    },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:DeleteDatabase",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:DeleteTable",
                "glue:BatchDeleteTable",
                "glue:UpdateTable",
                "glue:GetTable",
                "glue:GetTables",
                "glue:BatchCreatePartition",
                "glue:CreatePartition",
                "glue:DeletePartition",
                "glue:BatchDeletePartition",
                "glue:UpdatePartition",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:BatchGetPartition"
            ],
            "Resource": [
                "arn:aws:glue:*:*:table/*redshift*/*",
                "arn:aws:glue:*:*:catalog",
                "arn:aws:glue:*:*:database/*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetResourcePolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret",
                "secretsmanager:ListSecretVersionIds"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "secretsmanager:GetRandomPassword",
                "secretsmanager:ListSecrets"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "secretsmanager:ResourceTag/Redshift": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "redshift.amazonaws.com",
                        "glue.amazonaws.com",
                        "sagemaker.amazonaws.com",
                        "athena.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

Facultativement, pour utiliser une AWS KMS clé de chiffrement, ajoutez les autorisations suivantes à la politique.

```
{
    "Effect": "Allow",
    "Action": [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:Encrypt",
        "kms:GenerateDataKey*"
    ],
```

```
    "Resource": [
        "arn:aws:kms:<your-region>:<your-account-id>:key/<your-kms-key>"
    ]
}
```

Pour permettre à Amazon Redshift et SageMaker AI d'assumer le rôle IAM précédent pour interagir avec d'autres services, ajoutez la politique de confiance suivante au rôle.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift.amazonaws.com",
          "sagemaker.amazonaws.com",
          "forecast.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Dans ce qui précède, le compartiment Amazon S3 `redshift-downloads/redshift-ml/` est l'emplacement où sont stockés les exemples de données utilisés pour les autres étapes et exemples. Vous pouvez supprimer ce compartiment si vous n'avez pas besoin de charger des données à partir d'Amazon S3. Ou alors, remplacez-le par d'autres compartiments Amazon S3 que vous utilisez pour charger des données dans Amazon Redshift.

Les valeurs **`your-account-id`**, **`your-role`** et **`your-s3-bucket`** sont l'ID de compte, le rôle et le compartiment que vous spécifiez dans votre commande CREATE MODEL.

Vous pouvez éventuellement utiliser la section AWS KMS clés de l'exemple de politique si vous spécifiez une AWS KMS clé à utiliser avec Amazon Redshift ML. La valeur **`your-kms-key`** est la clé que vous utilisez dans le cadre de votre instruction CREATE MODEL.

Lorsque vous spécifiez un cloud privé virtuel (VPC) privé pour votre tâche de réglage d'hyperparamètres, ajoutez les autorisations suivantes :

```
{
            "Effect": "Allow",
            "Action": [
            "ec2:CreateNetworkInterface",
            "ec2:CreateNetworkInterfacePermission",
            "ec2:DeleteNetworkInterface",
            "ec2:DeleteNetworkInterfacePermission",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribeVpcs",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeSubnets",
            "ec2:DescribeSecurityGroups"
            ]
}
```

Pour utiliser l'explication du modèle, assurez-vous que vous disposez des autorisations nécessaires pour appeler les opérations de l'API SageMaker AI. Nous vous recommandons d'utiliser la politique gérée `AmazonSageMakerFullAccess`. Si vous souhaitez créer un rôle IAM avec une politique plus restrictive, utilisez celle qui suit.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:InvokeEndpoint",
        "sagemaker:ListTags"
      ],
```

```
      "Resource": "*"
    }
  ]
}
```

Pour plus d'informations sur la politique `AmazonSageMakerFullAccess` gérée, consultez AmazonSageMakerFullAccess le guide du développeur Amazon SageMaker AI.

Si vous souhaitez créer des modèles de prévision, nous vous recommandons d'utiliser la politique gérée par `AmazonForecastFullAccess`. Si vous souhaitez utiliser une politique plus restrictive, ajoutez la politique suivante à votre rôle IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "forecast:CreateAutoPredictor",
                "forecast:CreateDataset",
                "forecast:CreateDatasetGroup",
                "forecast:CreateDatasetImportJob",
                "forecast:CreateForecast",
                "forecast:CreateForecastExportJob",
                "forecast:DeleteResourceTree",
                "forecast:DescribeAutoPredictor",
                "forecast:DescribeDataset",
                "forecast:DescribeDatasetGroup",
                "forecast:DescribeDatasetImportJob",
                "forecast:DescribeForecast",
                "forecast:DescribeForecastExportJob",
                "forecast:StopResource",
                "forecast:TagResource",
                "forecast:UpdateDatasetGroup"
            ],
            "Resource": "*"
        }
    ]
}
```

Si vous souhaitez créer des modèles Amazon Bedrock, nous vous recommandons d'utiliser la politique gérée par `AmazonBedrockFullAccess`. Si vous souhaitez utiliser une politique plus restrictive, ajoutez la politique suivante à votre rôle IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "bedrock:InvokeModel",
            "Resource": [
                "*",
                "arn:aws:bedrock:us-east-1::foundation-model/*"
            ]
        }
    ]
}
```

Pour plus d'informations sur Amazon Redshift ML, consultez Utilisation du machine learning dans Amazon Redshift, CREATE MODEL ou CREATE EXTERNAL MODEL.

Autorisations pour l'ingestion en streaming

L'ingestion en streaming fonctionne avec deux services. Il s'agit de Kinesis Data Streams et d'Amazon MSK.

Autorisations requises pour utiliser l'ingestion en streaming avec Kinesis Data Streams

Une procédure comportant un exemple de politique gérée est disponible sur la page Mise en route de l'ingestion en streaming à partir d'Amazon Kinesis Data Streams.

Autorisations requises pour utiliser l'ingestion en streaming avec Amazon MSK

Une procédure comportant un exemple de politique gérée est disponible sur la page Mise en route de l'ingestion en streaming à partir d'Amazon Managed Streaming for Apache Kafka.

Autorisations requises pour utiliser les opérations d'API de partage de données

Pour contrôler l'accès aux opérations d'API de partage de données, utilisez des politiques basées sur une action IAM. Pour plus d'informations sur la gestion des politiques IAM, consultez Gestion des politiques IAM dans le Guide de l'utilisateur IAM.

Supposons plus particulièrement qu'un administrateur de cluster producteur ait besoin d'utiliser l'appel `AuthorizeDataShare` pour autoriser la sortie d'une unité de partage des données en dehors d'un Compte AWS. Dans ce cas, vous configurez une politique IAM basée sur l'action pour accorder cette autorisation. Utilisation de l'appel `DeauthorizeDataShare` pour révoquer la sortie.

Lorsque vous utilisez des politiques IAM basées sur des actions, vous pouvez également spécifier une ressource IAM dans la politique, par exemple `DataShareARN`. Ci-dessous, le format et un exemple pour `DataShareARN`.

```
arn:aws:redshift:region:account-id:datashare:namespace-guid/datashare-name
arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-e2e24359e9a8/
SalesShare
```

Vous pouvez restreindre l'accès `AuthorizeDataShare` à une unité de partage des données spécifique en spécifiant le nom de l'unité de partage des données dans la politique IAM.

```
{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/SalesShare"
      ],
      "Effect": "Deny"
    }
  ]
}
```

Vous pouvez également restreindre la politique IAM à toutes les unité de partage des données appartenant à un cluster producteur spécifique. Pour ce faire, remplacez la valeur **`datashare-name`** dans la politique par un caractère générique ou un astérisque. Gardez la valeur `namespace-guid` du cluster.

```
arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-e2e24359e9a8/
*
```

Voici une politique IAM qui empêche une entité d'appeler `AuthorizeDataShare` sur les unités de partage des données appartenant à un cluster producteur spécifique.

```
{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/*"
      ],
      "Effect": "Deny"
    }
  ]
}
```

`DataShareARN` restreint l'accès en fonction du nom de l'unité de partage des données et de l'ID global unique (GUID) de l'espace de noms du cluster propriétaire. Il le fait en spécifiant le nom comme un astérisque.

Politiques relatives aux ressources pour GetClusterCredentials

Pour vous connecter à une base de données de cluster à l'aide d'une connexion JDBC ou ODBC avec des informations d'identification de base de données IAM, ou pour appeler l'`GetClusterCredentials`action par programmation, vous devez être autorisé à lancer l'`redshift:GetClusterCredentials`action avec accès à une ressource. `dbuser`

Si vous utilisez une connexion JDBC ou ODBC, au lieu de `server` et de `port`, vous pouvez spécifier `cluster_id` et `region`, mais pour ce faire, votre politique doit autoriser l'action `redshift:DescribeClusters` avec accès à la ressource `cluster`.

Si vous appelez `GetClusterCredentials` avec les paramètres facultatifs `Autocreate`, `DbGroups` et `DbName`, veillez aussi à autoriser les actions et à permettre l'accès aux ressources répertoriées dans le tableau ci-dessous.

GetCluste rCredentials paramètre	Action	Ressource
`Autocreate`	`redshif CreateC sterUse`	`dbuser`
`DbGroups`	`redshif JoinGrou`	`dbgroup`
`DbName`	NA	`dbname`

Pour plus d'informations sur les ressources, consultez Ressources et opérations Amazon Redshift.

Vous pouvez aussi inclure les conditions suivantes dans votre politique :

- `redshift:DurationSeconds`
- `redshift:DbName`
- `redshift:DbUser`

> **Important**
>
> Pour les intégrations SSO SAML, vous devrez peut-être spécifier une politique IAM à l'aide de la variable. `${redshift:DbUser}` Dans ces cas, nous vous recommandons vivement d'utiliser une instruction de condition qui garantit que l'appelant ne peut pas obtenir les informations d'identification d'un utilisateur qui ne correspondent pas à son AWS nom d'utilisateur. E.g. `"StringEquals": {"aws:userid":"AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}"}`. Consultez Exemple 8 : politique IAM pour l'utilisation GetClusterCredentials. Pour plus d'informations sur les conditions, consultez Spécification de conditions dans une politique

Exemples de politiques gérées par le client

Dans cette section, vous trouverez des exemples de politiques utilisateur qui accordent des autorisations pour diverses actions Amazon Redshift. Ces politiques fonctionnent lorsque vous utilisez l'API Amazon Redshift, les kits de AWS développement logiciel (SDK) ou le. AWS CLI

> **Note**
>
> Tous les exemples utilisent la région USA Ouest (Oregon) (`us-west-2`) et contiennent des ID de compte fictifs.

Exemple 1 : Accorder à l'utilisateur un accès complet à toutes les actions et ressources d'Amazon Redshift

La politique suivante autorise l'accès à toutes les actions Amazon Redshift sur toutes les ressources.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid":"AllowRedshift",
      "Action": [
        "redshift:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

La valeur `redshift:*` dans l'élément `Action` indique toutes les actions dans Amazon Redshift.

Exemple 2 : Refuser à un utilisateur l'accès à un ensemble d'actions Amazon Redshift

Par défaut, toutes les autorisations sont refusées. Cependant, vous devrez parfois refuser explicitement l'accès à une action ou à un ensemble d'actions spécifique. La politique suivante autorise l'accès à toutes les actions Amazon Redshift et refuse explicitement l'accès à toute action

Amazon Redshift dont le nom commence par `Delete`. Cette politique s'applique à toutes les ressources Amazon Redshift dans `us-west-2`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid":"AllowUSWest2Region",
      "Action": [
        "redshift:*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:redshift:us-east-1:111122223333:*"
    },
   {
     "Sid":"DenyDeleteUSWest2Region",
     "Action": [
        "redshift:Delete*"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:redshift:us-east-1:111122223333:*"
   }
  ]
}
```

Exemple 3 : Autoriser un utilisateur à gérer les clusters

La politique suivante permet à un utilisateur de créer, supprimer, modifier et redémarrer tous les clusters, puis refuse l'autorisation de supprimer les clusters si le nom du cluster commence par `protected`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid":"AllowClusterManagement",
```

```
      "Action": [
        "redshift:CreateCluster",
        "redshift:DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid":"DenyDeleteProtected",
      "Action": [
        "redshift:DeleteCluster"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:cluster:protected*"
      ],
      "Effect": "Deny"
    }
  ]
}
```

Exemple 4 : Autoriser un utilisateur à accorder et à révoquer l'accès aux instantanés

La politique suivante autorise un utilisateur, par exemple l'utilisateur A, à effectuer les opérations suivantes :

- Autoriser l'accès à n'importe quel instantané créé à partir d'un cluster nommé `shared`.
- Annuler l'accès aux instantanés pour tous les instantanés créés à partir du cluster `shared` dont le nom d'instantané commence par `revokable`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid":"AllowSharedSnapshots",
```

```
      "Action": [
        "redshift:AuthorizeSnapshotAccess"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:shared/*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid":"AllowRevokableSnapshot",
      "Action": [
        "redshift:RevokeSnapshotAccess"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:*/revokable*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Si l'utilisateur A a autorisé l'utilisateur B à accéder à un instantané, l'utilisateur B doit disposer d'une politique telle que les suivantes pour autoriser l'utilisateur B à restaurer un cluster à partir de l'instantané. La politique suivante permet à l'utilisateur B de décrire et de restaurer à partir d'un instantané et de créer des clusters. Le nom de ces clusters doit commencer par `from-other-account`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid":"AllowDescribeSnapshots",
      "Action": [
        "redshift:DescribeClusterSnapshots"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
```

```
    },
    {
      "Sid":"AllowUserRestoreFromSnapshot",
      "Action": [
        "redshift:RestoreFromClusterSnapshot"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:*/*",
        "arn:aws:redshift:us-west-2:444455556666:cluster:from-other-account*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Exemple 5 : Permettre à un utilisateur de copier un instantané du cluster et de restaurer un cluster à partir d'un instantané

La politique suivante permet à un utilisateur de copier n'importe quel instantané créé à partir du cluster nommé `big-cluster-1` et de restaurer n'importe quel instantané dont le nom commence par `snapshot-for-restore`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid":"AllowCopyClusterSnapshot",
      "Action": [
        "redshift:CopyClusterSnapshot"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:big-cluster-1/*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid":"AllowRestoreFromClusterSnapshot",
      "Action": [
        "redshift:RestoreFromClusterSnapshot"
```

```
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:*/snapshot-for-
restore*",
        "arn:aws:redshift:us-west-2:123456789012:cluster:*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Exemple 6 : Autoriser un utilisateur à accéder à Amazon Redshift, ainsi qu'à des actions et à des ressources courantes pour les AWS services

L'exemple de politique suivant permet d'accéder à toutes les actions et ressources pour Amazon Redshift, Amazon Simple Notification Service (Amazon SNS) et Amazon. CloudWatch Il permet également des actions spécifiques sur toutes les ressources Amazon EC2 liées au compte.

> **Note**
>
> Resource-level les autorisations ne sont pas prises en charge pour les actions Amazon EC2 spécifiées dans cet exemple de politique.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid":"AllowRedshift",
      "Effect": "Allow",
      "Action": [
        "redshift:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
```

```
      "Sid":"AllowSNS",
      "Effect": "Allow",
        "Action": [
          "sns:*"
        ],
        "Resource": [
          "*"
        ]
      },
    {
      "Sid":"AllowCloudWatch",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid":"AllowEC2Actions",
      "Effect": "Allow",
      "Action": [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Exemple 7 : Autoriser un utilisateur à labéliser des ressources avec la console Amazon Redshift

L'exemple de politique suivant permet à un utilisateur de labéliser des ressources avec la console Amazon Redshift à l'aide de Groupes de ressources AWS. Cette politique peut être attachée à un rôle d'utilisateur qui appelle la console Amazon Redshift d'origine ou nouvelle. Pour plus d'informations sur le balisage, consultez Étiqueter les ressources dans Amazon Redshift..

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid":"TaggingPermissions",
            "Effect": "Allow",
            "Action": [
                "redshift:DeleteTags",
                "redshift:CreateTags",
                "redshift:DescribeTags",
                "tag:UntagResources",
                "tag:TagResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple 8 : politique IAM pour l'utilisation GetClusterCredentials

La politique suivante utilise ces exemples de valeurs de paramètre :

- Région: `us-west-2`
- AWS Compte : `123456789012`
- Nom du cluster: `examplecluster`

La politique suivante active les actions `GetCredentials`, `CreateClusterUser` et `JoinGroup`. La politique utilise des clés de condition pour autoriser les `CreateClusterUser` actions `GetClusterCredentials` et uniquement lorsque l'ID AWS utilisateur correspond`"AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"`. L'accès

IAM est demandé pour la base de données "testdb" uniquement. La politique autorise également les utilisateurs à rejoindre un groupe nommé "common_group".

JSON

```
{
"Version":"2012-10-17",
  "Statement": [
    {
     "Sid":"GetClusterCredsStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:GetClusterCredentials"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
${redshift:DbUser}",
        "arn:aws:redshift:us-west-2:123456789012:dbname:examplecluster/testdb",
        "arn:aws:redshift:us-west-2:123456789012:dbgroup:examplecluster/
common_group"
      ],
        "Condition": {
           "StringEquals": {
           "aws:userid":"AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"
           }
        }
    },
    {
      "Sid":"CreateClusterUserStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:CreateClusterUser"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
${redshift:DbUser}"
      ],
      "Condition": {
        "StringEquals": {
          "aws:userid":"AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"
        }
      }
    },
```

```
    {
      "Sid":"RedshiftJoinGroupStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:JoinGroup"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbgroup:examplecluster/
common_group"
      ]
    }
  ]
}
```

L'exemple suivant illustre une politique qui autorise le rôle IAM à appeler l'opération `GetClusterCredentials`. La spécification de la ressource Amazon Redshift `dbuser` accorde au rôle l'accès au nom d'utilisateur de la base de données `temp_creds_user` sur le cluster nommé `examplecluster`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
temp_creds_user"
  }
}
```

Vous pouvez utiliser un caractère générique (*) pour remplacer tout ou partie du nom de cluster, du nom d'utilisateur et des noms de groupes de bases de données. L'exemple suivant autorise tout nom d'utilisateur commençant par `temp_` avec tout cluster dans le compte spécifié.

> **Important**
>
> L'instruction de l'exemple suivant spécifie un caractère générique (*) comme valeur pour la ressource de telle sorte que la politique autorise n'importe quelle ressource commençant par

les caractères spécifiés. L'utilisation d'un caractère générique dans les politiques IAM peut être excessivement permissive. En tant que bonne pratique, il est recommandé d'utiliser la politique la plus restrictive acceptable pour votre application métier.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:*/temp_*"
  }
}
```

L'exemple suivant montre une politique qui autorise le rôle IAM à appeler l'opération `GetClusterCredentials` avec l'option de créer automatiquement un nouvel utilisateur et de spécifier les groupes que l'utilisateur rejoint lors de la connexion. La clause `"Resource": "*"` accorde au rôle l'accès à n'importe quelle ressource, y compris les clusters, utilisateurs de base de données ou groupes d'utilisateurs.

Important

L'instruction de l'exemple suivant spécifie un caractère générique (*) comme ressource pour les actions données, de sorte que la politique autorise l'accès à tous les utilisateurs du cluster et de la base de données et autorise la création de n'importe quel utilisateur. L'utilisation d'un caractère générique dans les politiques IAM peut être excessivement permissive. En tant que bonne pratique, il est recommandé d'utiliser la politique la plus restrictive acceptable pour votre application métier.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": {
```

```
    "Effect": "Allow",
    "Action": [
            "redshift:GetClusterCredentials",
            "redshift:CreateClusterUser",
  "redshift:JoinGroup"
           ],
    "Resource": "*"
  }
}
```

Pour plus d'informations, consultez Syntaxe de l'ARN Amazon Redshift.

Fédération de fournisseurs d’identité natifs pour Amazon Redshift

La gestion des identités et des autorisations pour Amazon Redshift est simplifiée grâce à la fédération des fournisseurs d’identités natifs, car elle exploite votre fournisseur d’identité existant pour simplifier l’authentification et la gestion des autorisations. Pour ce faire, elle permet de partager des métadonnées d’identité avec Redshift à partir de votre fournisseur d’identité. Pour la première itération de cette fonction, le fournisseur d’identité pris en charge est Microsoft Azure Active Directory (Azure AD).

Pour configurer Amazon Redshift afin qu’il puisse authentifier les identités du fournisseur d’identité tiers, vous enregistrez le fournisseur d’identité auprès d’Amazon Redshift. Cela permet à Redshift d’authentifier les utilisateurs et les rôles définis par le fournisseur d’identité. Cela vous évite de devoir effectuer une gestion précise des identités tant dans votre fournisseur d’identité tiers que dans Amazon Redshift, car les informations d’identité sont partagées.

Pour obtenir des informations sur l’utilisation de rôles de session transférés depuis des groupes de fournisseurs d’identité (IdP), consultez PG_GET_SESSION_ROLES dans le Guide du développeur de base de données Amazon Redshift.

Fédération de fournisseurs d’identité (IdP) natifs

Pour terminer la configuration préliminaire entre le fournisseur d’identité et Amazon Redshift, vous effectuez quelques étapes : tout d’abord, vous enregistrez Amazon Redshift en tant qu’application tierce auprès de votre fournisseur d’identité, en demandant les autorisations d’API nécessaires. Vous créez ensuite des utilisateurs et des groupes dans le fournisseur d’identité. Enfin, vous enregistrez le fournisseur d’identité auprès d’Amazon Redshift, à l’aide d’instructions SQL, qui définissent des paramètres d’authentification uniques pour le fournisseur d’identité. Dans le cadre de l’enregistrement

du fournisseur d'identité auprès de Redshift, vous attribuez un espace de noms pour vous assurer que les utilisateurs et les rôles sont correctement regroupés.

Une fois le fournisseur d'identité enregistré auprès d'Amazon Redshift, la communication est configurée entre Redshift et le fournisseur d'identité. Un client peut ensuite transmettre des jetons et s'authentifier auprès de Redshift en tant qu'entité de fournisseur d'identité. Amazon Redshift utilise les informations d'appartenance au groupe de fournisseurs d'identités pour mapper les rôles Redshift. Si l'utilisateur n'existe pas auparavant dans Redshift, il est créé. Les rôles sont créés et mappés à des groupes de fournisseurs d'identité, s'ils n'existent pas. L'administrateur Amazon Redshift accorde des autorisations sur les rôles, et les utilisateurs peuvent exécuter des requêtes et effectuer d'autres tâches de base de données.

Les étapes suivantes décrivent le fonctionnement de la fédération de fournisseurs d'identités natifs lorsqu'un utilisateur se connecte :

1. Lorsqu'un utilisateur se connecte à l'aide de l'option de fournisseurs d'identités natifs, à partir du client, le jeton du fournisseur d'identité est envoyé du client au pilote.
2. L'utilisateur est authentifié. Si l'utilisateur n'existe pas déjà dans Amazon Redshift, un nouvel utilisateur est créé. Redshift mappe les groupes de fournisseurs d'identité de l'utilisateur aux rôles Redshift.
3. Les autorisations sont attribuées, en fonction des rôles Redshift de l'utilisateur. Ils sont accordés aux utilisateurs et aux rôles par un administrateur.
4. L'utilisateur peut interroger Redshift.

Outils client de bureau

Pour obtenir des instructions sur l'utilisation de la fédération de fournisseurs d'identités natifs pour se connecter à Amazon Redshift avec Power BI, consultez le billet de blog Integrate Amazon Redshift native IdP federation with Microsoft Azure Active Directory (AD) and Power BI (Intégrer la fédération d'identités natives Amazon Redshift à Microsoft Azure Active Directory (AD) et Power BI). Cet article décrit une implémentation étape par étape de la configuration de fournisseur d'identité natif Amazon Redshift avec Azure AD. Il détaille les étapes de configuration de la connexion client pour Power BI Desktop ou pour le service Power BI. Les étapes comprennent l'enregistrement de l'application, la configuration des autorisations et la configuration des informations d'identification.

Pour savoir comment intégrer la fédération IdP native d'Amazon Redshift à Azure AD, à l'aide de Power BI Desktop et de JDBC Client-SQL Workbench/J, regardez la vidéo suivante :

Pour savoir comment utiliser la fédération native des fournisseurs d'identité pour se connecter à Amazon Redshift via un client SQL, en particulier DBeaver ou SQL Workbench/J, consultez l'article de blog Intégrer la fédération IdP native Amazon Redshift à Microsoft Azure AD à l'aide d'un client SQL.

Limitations

Les limitations suivantes s'appliquent :

- Les pilotes Amazon Redshift prennent en charge `BrowserIdcAuthPlugin` à partir des versions suivantes :
  - Pilote JDBC Amazon Redshift v2.1.0.30
  - Pilote ODBC Amazon Redshift v2.1.3
  - Pilote Python Amazon Redshift v2.1.3
- Les pilotes Amazon Redshift prennent en charge `IdpTokenAuthPlugin` à partir des versions suivantes :
  - Pilote JDBC Amazon Redshift v2.1.0.19
  - Pilote ODBC Amazon Redshift v2.0.0.9
  - Pilote Python Amazon Redshift v2.0.914
- Aucune prise en charge du routage VPC amélioré — Le routage VPC amélioré n'est pas pris en charge lorsque vous utilisez la fédération native des fournisseurs d'identité. Pour plus d'informations sur le routage VPC amélioré, consultez la section Routage VPC amélioré dans Amazon Redshift.
- AWS Mise en cache d'IAM Identity Center : AWS IAM Identity Center met en cache les informations de session. Cela peut entraîner des problèmes d'accès imprévisibles lorsque vous tentez de vous connecter à votre base de données Redshift via l'éditeur de requêtes v2 Redshift. En effet, la session AWS IAM Identity Center associée dans l'éditeur de requêtes v2 reste valide, même si l'utilisateur de la base de données est déconnecté de la AWS console. Le cache expire au bout d'une heure, ce qui résout généralement les problèmes.

Configuration du fournisseur d'identité sur Amazon Redshift

Cette section présente les étapes à suivre pour configurer le fournisseur d'identité et Amazon Redshift afin d'établir une communication pour la fédération des fournisseurs d'identité natifs. Vous avez besoin d'un compte actif auprès de votre fournisseur d'identité. Avant de configurer Amazon

Redshift, vous enregistrez Redshift en tant qu'application auprès de votre fournisseur d'identité, en accordant le consentement de l'administrateur.

Effectuez les étapes suivantes dans Amazon Redshift :

1. Vous exécutez une instruction SQL pour enregistrer le fournisseur d'identité, y compris des descriptions des métadonnées de l'application Azure. Pour créer le fournisseur d'identité dans Amazon Redshift, exécutez la commande suivante après avoir remplacé la valeur des paramètres issuer, client_id, client_secret et audience. Ces paramètres sont spécifiques à Microsoft Azure AD. Remplacez le nom du fournisseur d'identité par le nom de votre choix et remplacez l'espace de noms par un nom unique pour contenir les utilisateurs et les rôles de votre répertoire de fournisseur d'identité.

```
CREATE IDENTITY PROVIDER oauth_standard TYPE azure
NAMESPACE 'aad'
PARAMETERS '{
"issuer":"https://sts.windows.net/2sdfdsf-d475-420d-b5ac-667adad7c702/",
"client_id":"<client_id>",
"client_secret":"BUAH~ewrqewrqwerUUY^%tHe1oNZShoiU7",
"audience":["https://analysis.windows.net/powerbi/connector/AmazonRedshift"]
}'
```

   Le type `azure` indique que le fournisseur facilite spécifiquement la communication avec Microsoft Azure AD. Il s'agit actuellement du seul fournisseur d'identité tiers pris en charge.

   - issuer : identifiant de l'auteur à qui faire confiance lors de la réception d'un jeton. L'identifiant unique du tenant_id (ID de locataire) est joint à l'auteur.
   - client_id : identifiant public unique de l'application enregistrée auprès du fournisseur d'identité. Celui-ci peut être référencé en tant qu'ID d'application.
   - client_secret : identifiant secret, ou mot de passe, connu uniquement du fournisseur d'identité et de l'application enregistrée.
   - audience : ID d'application attribué à l'application dans Azure.

   Au lieu d'utiliser un secret client partagé, vous pouvez définir des paramètres pour spécifier un certificat, une clé privée et un mot de passe de clé privée lorsque vous créez le fournisseur d'identité.

```
CREATE IDENTITY PROVIDER example_idp TYPE azure
NAMESPACE 'example_aad'
PARAMETERS '{"issuer":"https://sts.windows.net/2sdfdsf-d475-420d-
b5ac-667adad7c702/",
"client_id":"<client_id>",
"audience":["https://analysis.windows.net/powerbi/connector/AmazonRedshift"],
"client_x5t":"<certificate thumbprint>",
"client_pk_base64":"<private key in base64 encoding>",
"client_pk_password":"test_password"}';
```

Le mot de passe de la clé privée, client_pk_password, est facultatif.

2. Facultatif : exécutez des commandes SQL dans Amazon Redshift pour créer en amont des utilisateurs et des rôles. Cela facilite l'octroi d'autorisations à l'avance. Le nom du rôle dans Amazon Redshift est le suivant <Namespace>: < GroupName sur Azure AD>. Par exemple, lorsque vous créez un groupe dans Microsoft Azure AD appelé `rsgroup` et un espace de noms appelé `aad`, le nom du rôle est `aad:rsgroup`. Les noms d'utilisateur et de rôle dans Amazon Redshift sont définis à partir de ces noms d'utilisateur et de ces appartenances aux groupes dans l'espace de noms du fournisseur d'identité.

   Le mappage des rôles et des utilisateurs comprend la vérification de leur valeur `external_id`, pour s'assurer qu'elle est à jour. L'ID externe correspond à l'identifiant du groupe ou de l'utilisateur dans le fournisseur d'identité. Par exemple, l'ID externe d'un rôle correspond à l'ID de groupe Azure AD correspondant. De même, l'ID externe de chaque utilisateur correspond à son ID dans le fournisseur d'identité.

   ```
   create role "aad:rsgroup";
   ```

3. Accordez des autorisations pertinentes aux rôles selon vos besoins. Par exemple :

   ```
   GRANT SELECT on all tables in schema public to role "aad:rsgroup";
   ```

4. Vous pouvez également accorder des autorisations à un utilisateur spécifique.

   ```
   GRANT SELECT on table foo to aad:alice@example.com
   ```

   Notez que l'appartenance au rôle d'un utilisateur externe fédéré n'est disponible que dans la session de cet utilisateur. Cela a des conséquences sur la création d'objets de base de données.

Lorsqu'un utilisateur externe fédéré crée une vue ou une procédure stockée, par exemple, il ne peut pas déléguer l'autorisation de ces objets à d'autres utilisateurs et rôles.

Explication des espaces de noms

Un espace de noms mappe un utilisateur ou un rôle à un fournisseur d'identité spécifique. Par exemple, le préfixe pour les utilisateurs créés dans AWS IAM est. `iam:` Ce préfixe empêche les collisions de noms d'utilisateur et permet la prise en charge de plusieurs magasins d'identités. Si un utilisateur alice@example.com de la source d'identité enregistrée auprès de l'espace de noms aad se connecte, l'utilisateur `aad:alice@example.com` est créé dans Redshift s'il n'existe pas déjà. Notez qu'un espace de noms d'utilisateur et de rôle a une fonction différente de celle d'un espace de noms de cluster Amazon Redshift, qui est un identifiant unique associé à un cluster.

Création automatique de rôles Amazon Redshift pour les fournisseurs d'identité

Cette fonctionnalité vous permet de créer automatiquement des rôles dans Redshift en fonction de l'appartenance à un groupe auprès de votre fournisseur d'identité (IdP). Auto-creating roles prend en charge Azure Active Directory avec l'intégration native d'IdP.

La création automatique de rôles présente plusieurs avantages. Lorsque vous créez automatiquement un rôle, Redshift le crée avec l'appartenance à un groupe dans votre IdP, ce qui vous permet d'éviter la création et la maintenance manuelles fastidieuses des rôles. Vous avez également la possibilité de filtrer quels groupes sont mappés aux rôles Redshift.

Comment ça marche

Lorsque vous, en tant qu'utilisateur IdP, vous connectez à Redshift, la séquence d'événements suivante se produit :

1. Redshift récupère les adhésions à vos groupes depuis l'IdP.
2. Redshift crée automatiquement des rôles correspondant à ces groupes, selon le format des rôles *idp_namespace*:*rolename*.
3. Redshift vous accorde des autorisations pour les rôles mappés.

À chaque connexion utilisateur, chaque groupe qui n'est pas présent dans le catalogue mais dont l'utilisateur fait partie est créé automatiquement. Vous pouvez éventuellement définir des filtres d'inclusion et d'exclusion pour contrôler les groupes IdP pour lesquels des rôles Redshift ont été créés.

Configuration de la création automatique des rôles

Utilisez les commandes `CREATE IDENTITY PROVIDER` et `ALTER IDENTITY PROVIDER` pour activer et configurer la création automatique de rôles.

```
-- Create a new IdP with auto role creation enabled
CREATE IDENTITY PROVIDER <idp_name> TYPE azure
  NAMESPACE '<namespace>'
  APPLICATION_ARN 'app_arn'
  IAM_ROLE 'role_arn'
  AUTO_CREATE_ROLES TRUE;

-- Enable on existing IdP
ALTER IDENTITY PROVIDER <idp_name>
  AUTO_CREATE_ROLES TRUE;

-- Disable
ALTER IDENTITY PROVIDER <idp_name>
  AUTO_CREATE_ROLES FALSE;
```

Groupes de filtres

Vous pouvez éventuellement filtrer les groupes IdP mappés aux rôles Redshift à l'aide des modèles `INCLUDE` et `EXCLUDE`. En cas de conflit entre les modèles, `EXCLUDE` a la priorité sur `INCLUDE`.

```
-- Only create roles for groups with 'dev'
CREATE IDENTITY PROVIDER <idp_name> TYPE azure
  ...
  AUTO_CREATE_ROLES TRUE
  INCLUDE GROUPS LIKE '%dev%';

-- Exclude 'test' groups
ALTER IDENTITY PROVIDER <idp_name>
  AUTO_CREATE_ROLES TRUE
  EXCLUDE GROUPS LIKE '%test%';
```

Exemples

L'exemple suivant montre comment activer la création automatique de rôles sans filtrage.

```
CREATE IDENTITY PROVIDER prod_idc TYPE azure ...
  AUTO_CREATE_ROLES TRUE;
```

L’exemple suivant inclut les groupes de développement et exclut les groupes de test.

```
ALTER IDENTITY PROVIDER prod_idc
  AUTO_CREATE_ROLES TRUE
  INCLUDE GROUPS LIKE '%dev%'
  EXCLUDE GROUPS LIKE '%test%';
```

Bonnes pratiques

Tenez compte des bonnes pratiques suivantes lorsque vous activez la création automatique pour les rôles :

- Utilisez les filtres `INCLUDE` et `EXCLUDE` pour contrôler quels groupes obtiennent des rôles.
- Auditez régulièrement les rôles et nettoyez ceux qui ne sont pas utilisés.
- Tirez parti des hiérarchies de rôles Redshift pour simplifier la gestion des autorisations.

Connectez Redshift à AWS IAM Identity Center pour une expérience d'authentification unique

Vous pouvez gérer l’accès des utilisateurs et des groupes aux entrepôts des données Amazon Redshift par le biais de la propagation d’identité approuvée.

La propagation d'identité sécurisée est une AWS IAM Identity Center fonctionnalité que les administrateurs de Connected Services AWS peuvent utiliser pour accorder et auditer l'accès aux données de service. L’accès à ces données est basé sur les attributs utilisateur tels que les associations de groupe. La mise en place d'une propagation d'identité sécurisée nécessite une collaboration entre les administrateurs de Connected Services AWS et les administrateurs d'IAM Identity Center. Pour plus d’informations, consultez Prérequis et considérations.

Pour illustrer un cas de bout en bout, vous pouvez utiliser un Amazon Quick tableau de bord ou l'éditeur de requêtes Amazon Redshift v2 pour accéder à Redshift. Dans ce cas, l'accès est basé sur les groupes AWS IAM Identity Center. Redshift peut déterminer qui est un utilisateur et son appartenance à un groupe. AWS IAM Identity Center permet également de connecter et de gérer les identités via un fournisseur d'identité tiers (IdP) tel qu'Okta ou. PingOne

Une fois que votre administrateur a configuré la connexion entre Redshift et AWS IAM Identity Center, il peut configurer un accès précis en fonction des groupes de fournisseurs d'identité afin d'autoriser l'accès des utilisateurs aux données.

> **Important**
>
> Lorsque vous supprimez un utilisateur d'un AWS IAM Identity Center ou d'un répertoire de fournisseurs d'identité connectés (IdP), il n'est pas automatiquement supprimé du catalogue Amazon Redshift. Pour supprimer manuellement l'utilisateur du catalogue Amazon Redshift, exécutez la `DROP USER` commande pour supprimer complètement l'utilisateur qui a été supprimé d'un AWS IAM Identity Center ou d'un IdP. Pour plus d'informations sur la procédure à suivre pour supprimer un utilisateur, consultez DROP USER dans le Guide du développeur de base de données Amazon Redshift.

Avantages de l'intégration de Redshift avec AWS IAM Identity Center

L'utilisation d' AWS IAM Identity Center avec Redshift peut bénéficier à votre organisation des manières suivantes :

- Les auteurs de tableaux de bord Amazon Quick peuvent se connecter aux sources de données Redshift sans avoir à saisir de nouveau les mots de passe ou à demander à un administrateur de configurer des rôles IAM avec des autorisations complexes.
- AWS IAM Identity Center fournit un emplacement central pour les utilisateurs de votre personnel. AWS Vous pouvez créer des utilisateurs et des groupes directement dans AWS IAM Identity Center ou connecter des utilisateurs et des groupes existants que vous gérez via un fournisseur d'identité basé sur des normes comme Okta ou Microsoft Entra ID (Azure AD). PingOne AWS IAM Identity Center dirige l'authentification vers la source de vérité que vous avez choisie pour les utilisateurs et les groupes, et gère un répertoire des utilisateurs et des groupes auxquels Redshift peut accéder. Pour plus d'informations, consultez Gestion de votre source d'identité et Fournisseurs d'identité pris en charge dans le Guide de l'utilisateur AWS IAM Identity Center.
- Vous pouvez partager une instance AWS IAM Identity Center avec plusieurs clusters et groupes de travail Redshift grâce à une simple fonctionnalité de découverte automatique et de connexion. Cela permet d'ajouter rapidement des clusters sans avoir à configurer la connexion AWS IAM Identity Center pour chacun d'entre eux, et garantit que tous les clusters et groupes de travail disposent d'une vue cohérente des utilisateurs, de leurs attributs et de leurs groupes. Notez que l'instance AWS IAM Identity Center de votre organisation doit se trouver dans la même région que tous les partages de données Redshift auxquels vous vous connectez.
- Comme les identités des utilisateurs sont connues et journalisées en même temps que l'accès aux données, il vous est plus facile de respecter les règles de conformité en auditant l'accès des utilisateurs dans AWS CloudTrail.

Personas d’administrateur pour la connexion des applications

Les personas suivants sont essentiels pour connecter les applications analytiques à l’application gérée par AWS IAM Identity Center pour Redshift :

- Administrateur de l’application : crée une application et configure les services avec lesquels elle permettra des échanges de jetons d’identité. Cet administrateur spécifie également les utilisateurs et les groupes qui ont accès à l’application.
- Administrateur de données : configure un accès précis aux données. Les utilisateurs et les groupes d' AWS IAM Identity Center peuvent correspondre à des autorisations spécifiques.

Connexion à Amazon Redshift avec AWS IAM Identity Center via Amazon Quick

Voici comment utiliser Quick pour s'authentifier auprès de Redshift lorsqu'il est connecté à AWS IAM Identity Center et que l'accès est géré via celui-ci : Autorisation des connexions depuis Quick vers des clusters Amazon Redshift. Ces étapes s’appliquent également à Amazon Redshift sans serveur.

Connexion à Amazon Redshift avec AWS IAM Identity Center via l'éditeur de requêtes Amazon Redshift v2

Après avoir terminé les étapes de configuration d'une connexion AWS IAM Identity Center avec Redshift, l'utilisateur peut accéder à la base de données et aux objets appropriés de la base de données via son identité AWS IAM Identity Center-based, identité préfixée par un espace de noms. Pour plus d’informations sur la connexion aux bases de données Redshift avec la connexion à l’éditeur de requêtes v2, consultez Interrogation d’une base de données à l’aide de l’éditeur de requête v2.

Utilisation AWS IAM Identity Center sur plusieurs Régions AWS

Amazon Redshift prend en charge AWS IAM Identity Center dans de nombreux domaines. Régions AWS Vous pouvez étendre AWS IAM Identity Center de votre région principale Région AWS à d'autres régions pour améliorer les performances grâce à la proximité avec les utilisateurs et à la fiabilité. Lorsqu'une nouvelle région est ajoutée dans AWS IAM Identity Center, vous pouvez créer des applications Redshift IAM Identity Center dans la nouvelle région sans répliquer les identités de la région principale. Vous pouvez configurer des autorisations fédérées Amazon Redshift à l'aide d' AWS IAM Identity Center dans la nouvelle région, où vous pouvez activer les contrôles au niveau des lignes, des colonnes et des contrôles de masquage. Pour en savoir plus sur la prise en main d' AWS IAM Identity Center dans plusieurs régions, consultez la section Gérer AWS IAM Identity Center dans plusieurs régions dans le Guide de l' Régions AWSutilisateur d'AWS IAM Identity Center.

Configuration AWS Intégration d'IAM Identity Center à Amazon Redshift

Votre administrateur de cluster Amazon Redshift ou votre administrateur Amazon Redshift Serverless doit effectuer plusieurs étapes pour configurer Redshift en tant qu'application compatible avec AWS IAM Identity Center. Redshift peut ainsi découvrir et se connecter automatiquement à AWS IAM Identity Center pour recevoir les services de connexion et d'annuaire des utilisateurs. Ensuite, lorsque votre administrateur Redshift crée un cluster ou un groupe de travail, il peut autoriser le nouvel entrepôt de données à utiliser AWS IAM Identity Center pour gérer l'accès à la base de données.

L'objectif de l'activation de Redshift en tant qu'application gérée par AWS IAM Identity Center est de vous permettre de contrôler les autorisations des utilisateurs et des groupes depuis AWS IAM Identity Center ou depuis un fournisseur d'identité tiers qui y est intégré. Lorsque les utilisateurs de votre base de données se connectent à une base de données Redshift, par exemple un analyste ou un data scientist, celui-ci vérifie leurs groupes dans AWS IAM Identity Center et ceux-ci correspondent aux noms de rôle dans Redshift. De cette manière, un groupe qui définit le nom d'un rôle de base de données Redshift peut accéder à un ensemble de tables pour l'analyse des ventes, par exemple. Les sections suivantes décrivent comment configurer cela.

Conditions préalables

Les conditions préalables à l'intégration d' AWS IAM Identity Center à Amazon Redshift sont les suivantes :

- Configuration du compte : vous devez configurer AWS IAM Identity Center dans le compte de gestion de votre AWS organisation si vous prévoyez d'utiliser plusieurs comptes ou si vous utilisez des clusters Redshift dans différents comptes avec la même instance AWS IAM Identity Center. Cela inclut la configuration de votre source d'identité. Pour plus d'informations, consultez Prise en main, Identités de personnel et Fournisseurs d'identité pris en charge dans le guide de l'utilisateur AWS IAM Identity Center. Vous devez vous assurer que vous avez créé des utilisateurs ou des groupes dans AWS IAM Identity Center, ou que vous avez synchronisé des utilisateurs et des groupes à partir de votre source d'identité avant de pouvoir les affecter à des données dans Redshift.

  > **Note**
  >
  > Vous pouvez utiliser une instance de compte d' AWS IAM Identity Center, à condition que Redshift et AWS IAM Identity Center soient associés au même compte. Vous pouvez créer

cette instance à l'aide d'un widget lorsque vous créez et configurez un cluster ou un groupe de travail Redshift.

- Configuration d'un émetteur de jetons approuvé : dans certains cas, vous devrez peut-être utiliser un émetteur de jetons approuvé, qui est une entité capable d'émettre et de vérifier des jetons de confiance. Avant de pouvoir le faire, des étapes préliminaires sont nécessaires avant que l'administrateur Redshift qui configure l'intégration d' AWS IAM Identity Center puisse sélectionner l'émetteur du jeton de confiance et ajouter les attributs nécessaires pour terminer la configuration. Cela peut inclure la configuration d'un fournisseur d'identité externe pour qu'il fasse office d'émetteur de jetons de confiance et l'ajout de ses attributs dans la console AWS IAM Identity Center. Pour effectuer ces étapes, consultez Utilisation d'applications avec un émetteur de jetons approuvés.

  > **Note**
  >
  > La configuration d'un émetteur de jetons approuvé n'est pas requise pour toutes les connexions externes. La connexion à votre base de données Redshift à l'aide de l'éditeur de requêtes Amazon Redshift v2 ne nécessite pas la configuration d'un émetteur de jetons approuvé. Toutefois, cela peut s'appliquer à des applications tierces telles que des tableaux de bord ou des applications personnalisées qui s'authentifient auprès de votre fournisseur d'identité.

- Configuration d'un ou de plusieurs rôles IAM : les sections suivantes mentionnent les autorisations qui doivent être configurées. Vous devrez ajouter des autorisations conformément aux bonnes pratiques IAM. Les autorisations spécifiques sont détaillées dans les procédures qui suivent.
- Configuration réseau pour un routage VPC amélioré — Si le routage VPC amélioré est activé, votre VPC doit être en mesure d'accéder aux services AWS IAM Identity Center. Les points de terminaison Interface VPC constituent la méthode recommandée pour fournir cette connectivité.

  > **Note**
  >
  > Configurez cette connectivité avant que les utilisateurs ne se connectent. Pour plus d'informations sur l'utilisation du routage VPC amélioré avec AWS IAM Identity Center, consultez. Utilisation AWS Authentification IAM Identity Center avec routage VPC amélioré

Pour plus d'informations, consultez Bien démarrer avec AWS IAM Identity Center.

Configuration de votre fournisseur d'identité pour qu'il fonctionne avec AWS IAM Identity Center

La première étape du contrôle de la gestion des identités des utilisateurs et des groupes consiste à vous connecter à AWS IAM Identity Center et à configurer votre fournisseur d'identité. Vous pouvez utiliser AWS IAM Identity Center lui-même comme fournisseur d'identité, ou vous pouvez connecter une boutique d'identités tierce, telle qu'Okta, par exemple. Pour plus d'informations sur la configuration de la connexion et de votre fournisseur d'identité, consultez Connexion à un fournisseur d'identité externe dans le Guide de l'utilisateur AWS IAM Identity Center. À la fin de ce processus, assurez-vous qu'un petit groupe d'utilisateurs et de groupes a été ajouté à AWS IAM Identity Center, à des fins de test.

Autorisations administratives

Autorisations requises pour Redshift/AWS Gestion du cycle de vie des applications IAM Identity Center

Vous devez créer une identité IAM, qu'un administrateur Redshift utilise pour configurer Redshift afin de l'utiliser avec AWS IAM Identity Center. Le plus souvent, vous créez un rôle IAM avec des autorisations et vous l'attribuez à d'autres identités selon les besoins. Il doit disposer des autorisations répertoriées pour effectuer les actions suivantes.

Création de l'application Redshift/AWS IAM Identity Center

- `sso:PutApplicationAssignmentConfiguration` : pour la sécurité.
- `sso:CreateApplication`— Utilisé pour créer une application AWS IAM Identity Center.
- `sso:PutApplicationAuthenticationMethod` : accorde l'accès à l'authentification Redshift.
- `sso:PutApplicationGrant` : sert à modifier les informations relatives à l'émetteur de jetons approuvé.
- `sso:PutApplicationAccessScope`— Pour la configuration de l'application Redshift AWS IAM Identity Center. Cela inclut pour AWS Lake Formation et pour les subventions d'accès Amazon S3.
- `redshift:CreateRedshiftIdcApplication`— Utilisé pour créer l'application Redshift AWS IAM Identity Center.

Décrire l'application Redshift/AWS IAM Identity Center

- `sso:GetApplicationGrant` : sert à répertorier les informations relatives à l'émetteur de jetons approuvé.

- `sso:ListApplicationAccessScopes` : pour configurer l'application Redshift AWS IAM Identity Center afin de répertorier les intégrations en aval, telles que pour AWS Lake Formation et les autorisations d'accès S3.
- `redshift:DescribeRedshiftIdcApplications`— Utilisé pour décrire les applications AWS IAM Identity Center existantes.

Modification de l'application Redshift/AWS IAM Identity Center

- `redshift:ModifyRedshiftIdcApplication` : sert à modifier une application Redshift existante.
- `sso:UpdateApplication`— Utilisé pour mettre à jour une application AWS IAM Identity Center.
- `sso:GetApplicationGrant` : récupère les informations relatives à l'émetteur de jetons approuvé.
- `sso:ListApplicationAccessScopes` : pour la configuration de l'application Redshift AWS IAM Identity Center.
- `sso:DeleteApplicationGrant` : supprime les informations relatives à l'émetteur de jetons approuvé.
- `sso:PutApplicationGrant` : sert à modifier les informations relatives à l'émetteur de jetons approuvé.
- `sso:PutApplicationAccessScope`— Pour la configuration de l'application Redshift AWS IAM Identity Center. Cela inclut pour AWS Lake Formation et pour les subventions d'accès Amazon S3.
- `sso:DeleteApplicationAccessScope` : pour supprimer l'application Redshift AWS IAM Identity Center. Cela inclut pour AWS Lake Formation et pour les subventions d'accès Amazon S3.

Suppression de l'application Redshift/AWS IAM Identity Center

- `sso:DeleteApplication`— Utilisé pour supprimer une application AWS IAM Identity Center.
- `redshift:DeleteRedshiftIdcApplication`— Permet de supprimer une application Redshift AWS IAM Identity Center existante.

Autorisations requises pour la gestion du cycle de vie des applications de l' Redshift/query éditeur v2

Vous devez créer une identité IAM, qu'un administrateur Redshift utilise pour configurer Redshift afin de l'utiliser avec AWS IAM Identity Center. Le plus souvent, vous créez un rôle IAM avec

des autorisations et vous l'attribuez à d'autres identités selon les besoins. Il doit disposer des autorisations répertoriées pour effectuer les actions suivantes.

Création de l'application de l'éditeur de requête v2

- `redshift:CreateQev2IdcApplication` :utilisé pour créer l'application de l'éditeur de requête v2.
- `sso:CreateApplication` : permet de créer une application AWS IAM Identity Center.
- `sso:PutApplicationAuthenticationMethod` : accorde l'accès à l'authentification Redshift.
- `sso:PutApplicationGrant` : sert à modifier les informations relatives à l'émetteur de jetons approuvé.
- `sso:PutApplicationAccessScope`— Pour la configuration de l'application Redshift AWS IAM Identity Center. Cela inclut l'éditeur de requêtes v2.
- `sso:PutApplicationAssignmentConfiguration` : pour la sécurité.

Décrire l'application de l'éditeur de requête v2

- `redshift:DescribeQev2IdcApplications`— Utilisé pour décrire l'application AWS IAM Identity Center QEV2.

Modifier l'application de l'éditeur de requête v2

- `redshift:ModifyQev2IdcApplication` : utilisé pour modifier l'application de l'éditeur de requête v2 AWS IAM Identity Center.
- `sso:UpdateApplication`— Utilisé pour modifier l'application AWS IAM Identity Center QEV2.

Supprimer l'application de l'éditeur de requête v2

- `redshift:DeleteQev2IdcApplication` : utilisé pour supprimer l'application de l'éditeur de requête v2.
- `sso:DeleteApplication` : utilisé pour supprimer l'application de l'éditeur de requête v2.

> **Note**
>
> Dans le SDK Amazon Redshift, les API suivantes ne sont pas disponibles :

- CreateQev2IdcApplication
- DescribeQev2IdcApplications
- ModifyQev2IdcApplication
- DeleteQev2IdcApplication

Ces actions sont spécifiques à l'intégration d' AWS IAM Identity Center avec Redshift QEV2 dans la console. AWS Pour de plus amples informations, consultez Actions définies par Amazon Redshift.

Autorisations requises pour que l’administrateur de base de données puisse se connecter à de nouvelles ressources dans la console

Ces autorisations sont requises pour connecter de nouveaux clusters provisionnés ou des groupes de travail Amazon Redshift sans serveur au cours du processus de création. Si vous disposez de ces autorisations, une sélection apparaît dans la console pour que vous choisissiez de vous connecter à l’application gérée par AWS IAM Identity Center pour Redshift.

- `redshift:DescribeRedshiftIdcApplications`
- `sso:ListApplicationAccessScopes`
- `sso:GetApplicationAccessScope`
- `sso:GetApplicationGrant`

Il est recommandé d’associer des politiques d’autorisation à un rôle IAM, puis de l’attribuer à des utilisateurs et à des groupes, le cas échéant. Pour plus d’informations, consultez Identity and Access Management dans Amazon Redshift.

Configuration de Redshift en tant que AWS application gérée avec AWS IAM Identity Center

Avant qu' AWS IAM Identity Center puisse gérer les identités d'un cluster provisionné par Amazon Redshift ou d'un groupe de travail Amazon Redshift Serverless, l'administrateur Redshift doit suivre les étapes nécessaires pour faire de Redshift une application gérée par IAM Identity Center : AWS

1. Sélectionnez l'intégration d'AWS IAM Identity Center dans le menu de la console Amazon Redshift ou Amazon Redshift Serverless, puis sélectionnez Se connecter à AWS IAM Identity

Center. À partir de là, vous devez effectuer une série de sélections pour renseigner les propriétés nécessaires à l'intégration d' AWS IAM Identity Center.

2. Choisissez un nom d'affichage et un nom unique pour l'application AWS IAM Identity Center-managed de Redshift.
3. Spécifiez l'espace de noms de votre organisation. Il s'agit généralement d'une version abrégée du nom de votre organisation. Il est ajouté en tant que préfixe pour vos Center-managed utilisateurs et rôles AWS IAM Identity dans la base de données Redshift.
4. Sélectionnez un rôle IAM à utiliser. Ce rôle IAM doit être distinct des autres rôles utilisés pour Redshift et nous vous recommandons de ne pas l'utiliser à d'autres fins. Les autorisations de politique spécifiques requises sont les suivantes :

   - `sso:DescribeApplication` : requise pour créer une entrée de fournisseur d'identité (IdP) dans le catalogue.
   - `sso:DescribeInstance` : sert à créer manuellement des rôles ou des utilisateurs fédérés par le fournisseur d'identité.
5. Configurez les connexions client et les émetteurs de jetons approuvés. La configuration d'émetteurs de jetons approuvés facilite la propagation d'identités approuvées en établissant une relation avec un fournisseur d'identité externe. La propagation de l'identité permet à un utilisateur, par exemple, de se connecter à une application et d'accéder à des données spécifiques dans une autre application. Cela permet aux utilisateurs de collecter des données à partir d'emplacements distincts de manière plus fluide. À ce stade, dans la console, vous définissez les attributs de chaque émetteur de jetons approuvé. Ces attributs incluent le nom et la réclamation d'audience (ou aud claim), que vous devrez peut-être obtenir à partir des attributs de configuration de l'outil ou du service. Vous devrez peut-être également fournir le nom de l'application à partir du jeton Web JSON (JWT) de l'outil tiers.

   > **Note**
   >
   > L'élément `aud claim` requis à partir de chaque outil ou service tiers peut varier en fonction du type de jeton, qui peut être un jeton d'accès émis par un fournisseur d'identité, ou d'un autre type, tel qu'un jeton d'identification. Chaque fournisseur peut être différent. Lorsque vous implémentez la propagation d'identité approuvée et intégrez Redshift, il est nécessaire de fournir la valeur aud correcte pour le type de jeton que l'outil tiers envoie à AWS. Consultez les recommandations de votre fournisseur d'outils ou de services.

Pour obtenir des informations détaillées sur la propagation d'identité approuvée, consultez Présentation de la propagation d'identité approuvée dans le Guide de l'utilisateur AWS IAM Identity Center .

Une fois que l'administrateur Redshift a terminé les étapes et enregistré la configuration, les propriétés d' AWS IAM Identity Center apparaissent dans la console Redshift. Vous pouvez également interroger la vue système SVV_IDENTITY_PROVIDERS pour vérifier les propriétés de l'application. Celles-ci incluent le nom de l'application et l'espace de noms. Vous utilisez l'espace de noms comme préfixe pour les objets de base de données Redshift associés à l'application. L'exécution de ces tâches fait de Redshift une application compatible avec AWS IAM Identity Center. Les propriétés de la console incluent l'état de l'intégration. Il indique Activé lorsque l'intégration est terminée. À l'issue de ce processus, l'intégration d' AWS IAM Identity Center peut être activée sur chaque nouveau cluster.

Après la configuration, vous pouvez inclure des utilisateurs et des groupes d' AWS IAM Identity Center dans Redshift en choisissant l'onglet Utilisateurs ou Groupes, puis en choisissant Attribuer.

Activation AWS Intégration d'IAM Identity Center pour un nouveau cluster Amazon Redshift ou un nouveau groupe de travail Amazon Redshift Serverless

Votre administrateur de base de données configure les nouvelles ressources Redshift pour qu'elles fonctionnent en harmonie avec AWS IAM Identity Center afin de faciliter la connexion et l'accès aux données. Cela s'effectue dans le cadre des étapes de création d'un cluster provisionné ou d'un groupe de travail sans serveur. Toute personne autorisée à créer des ressources Redshift peut effectuer ces tâches d'intégration à AWS IAM Identity Center. Lorsque vous créez un cluster provisionné, vous commencez par sélectionner Créer un cluster dans la console Amazon Redshift. Les étapes suivantes montrent comment activer la gestion d' AWS IAM Identity Center pour une base de données. (Elle n'inclut pas toutes les étapes de création d'un cluster.)

1. Choisissez Activer pour <nom du cluster> dans la section relative à l'intégration d'IAM Identity Center dans les étapes de création de cluster.
2. Le processus comporte une étape où vous activez l'intégration. Pour ce faire, choisissez Activer l'intégration d'IAM Identity Center dans la console.
3. Pour le nouveau cluster ou groupe de travail, créez des rôles de base de données dans Redshift à l'aide de commandes SQL. Voici la commande :

```
CREATE ROLE <idcnamespace:rolename>;
```

L’espace de noms et le nom du rôle sont les suivants :

- Préfixe de l'espace de noms IAM Identity Center : il s'agit de l'espace de noms que vous avez défini lorsque vous avez configuré la connexion entre AWS IAM Identity Center et Redshift.
- Nom du rôle : ce rôle de base de données Redshift doit correspondre au nom du groupe dans AWS IAM Identity Center.

Redshift se connecte à AWS IAM Identity Center et extrait les informations nécessaires pour créer et mapper le rôle de base de données au groupe AWS IAM Identity Center.

Notez que lorsqu’un nouvel entrepôt des données est créé, le rôle IAM spécifié pour l’intégration AWS IAM Identity Center est automatiquement associé au cluster alloué ou au groupe de travail Amazon Redshift sans serveur. Après avoir saisi les métadonnées de cluster requises et créé la ressource, vous pouvez vérifier l'état de l'intégration d' AWS IAM Identity Center dans les propriétés. Si les noms de vos groupes dans AWS IAM Identity Center comportent des espaces, vous devez utiliser des guillemets dans SQL lorsque vous créez le rôle correspondant.

Après avoir activé la base de données Redshift et créé des rôles, vous êtes prêt à vous connecter à la base de données avec l’éditeur de requêtes Amazon Redshift v2 ou Amazon Quick. Les détails sont expliqués dans les sections suivantes.

Configuration de l’élément par défaut **`RedshiftIdcApplication`** à l’aide de l’API

La configuration est effectuée par votre administrateur d’identité. À l'aide de l'API, vous créez et remplissez un`RedshiftIdcApplication`, qui représente l'application Redshift dans AWS IAM Identity Center.

1. Pour commencer, vous pouvez créer des utilisateurs et les ajouter à des groupes dans AWS IAM Identity Center. Vous pouvez effectuer cette opération dans la AWS console d' AWS IAM Identity Center.
2. Appelez `create-redshift-idc-application` pour créer une application AWS IAM Identity Center et la rendre compatible avec l'utilisation de Redshift. Vous créez l’application en renseignant les valeurs requises. Le nom d’affichage est le nom qui s’affichera sur le tableau de

bord AWS IAM Identity Center. L'ARN du rôle IAM est un ARN doté d'autorisations pour accéder à AWS IAM Identity Center, qui est également endossable par Redshift.

```
aws redshift create-redshift-idc-application
--idc-instance-arn 'arn:aws:sso:::instance/ssoins-1234a01a1b12345d'
--identity-namespace 'MYCO'
--idc-display-name 'TEST-NEW-APPLICATION'
--iam-role-arn 'arn:aws:redshift:us-east-1:012345678901:role/TestRedshiftRole'
--redshift-idc-application-name 'myredshiftidcapplication'
```

L'exemple suivant montre un exemple de réponse `RedshiftIdcApplication` renvoyé à partir de l'appel à `create-redshift-idc-application`.

```
"RedshiftIdcApplication": {
                "IdcInstanceArn": "arn:aws:sso:::instance/ssoins-1234a01a1b12345d",
                "RedshiftIdcApplicationName": "test-application-1",
                "RedshiftIdcApplicationArn": "arn:aws:redshift:us-
east-1:012345678901:redshiftidcapplication:12aaa111-3ab2-3ab1-8e90-b2d72aea588b",
                "IdentityNamespace": "MYCO",
                "IdcDisplayName": "Redshift-Idc-Application",
                "IamRoleArn": "arn:aws:redshift:us-east-1:012345678901:role/
TestRedshiftRole",
                "IdcManagedApplicationArn": "arn:aws:sso::012345678901:application/
ssoins-1234a01a1b12345d/apl-12345678910",
                "IdcOnboardStatus": "arn:aws:redshift:us-
east-1:123461817589:redshiftidcapplication",
                "RedshiftIdcApplicationArn": "Completed",
                "AuthorizedTokenIssuerList": [
                       "TrustedTokenIssuerArn": ...,
                       "AuthorizedAudiencesList": [...]...
                ]}
```

3. Vous pouvez l'utiliser `create-application-assignment` pour affecter des groupes particuliers ou des utilisateurs individuels à l'application gérée dans AWS IAM Identity Center. Vous pouvez ainsi spécifier les groupes à gérer via AWS IAM Identity Center. Si l'administrateur de base de données crée des rôles de base de données dans Redshift, les noms de groupe dans AWS IAM Identity Center correspondent aux noms de rôles dans Redshift. Les rôles contrôlent les autorisations dans la base de données. Pour plus d'informations, voir Attribuer l'accès des utilisateurs aux applications dans la console AWS IAM Identity Center.

4. Après avoir activé l'application, appelez `create-cluster` et incluez l'ARN de l'application gérée Redshift depuis AWS IAM Identity Center. Cela permet d'associer le cluster à l'application gérée dans AWS IAM Identity Center.

Associer un AWS Application IAM Identity Center avec un cluster ou un groupe de travail existant

Si vous avez un cluster ou un groupe de travail existant que vous souhaitez activer pour l'intégration d' AWS IAM Identity Center, vous pouvez le faire en exécutant des commandes SQL. Vous pouvez également exécuter des commandes SQL pour modifier les paramètres de l'intégration. Pour plus d'informations, consultez ALTER IDENTITY PROVIDER.

Il est également possible de supprimer un fournisseur d'identité existant. L'exemple suivant montre comment CASCADE supprime les utilisateurs et les rôles attachés au fournisseur d'identité.

```
DROP IDENTITY PROVIDER
<provider_name> [ CASCADE ]
```

Configuration des autorisations utilisateur

Un administrateur configure les autorisations pour différentes ressources, en fonction des attributs d'identité des utilisateurs et de leur appartenance à des groupes, au sein de leur fournisseur d'identité ou directement dans AWS IAM Identity Center. Par exemple, l'administrateur du fournisseur d'identité peut ajouter un ingénieur de base de données à un groupe correspondant à son rôle. Ce nom de groupe correspond à un nom de rôle de base de données Redshift. Le rôle fournit ou restreint l'accès à des tables ou à des vues spécifiques dans Redshift.

Utilisation AWS Authentification IAM Identity Center avec routage VPC amélioré

Lorsque le routage VPC amélioré est activé, Redshift achemine le trafic via votre cloud privé virtuel (VPC) plutôt que via Internet. Cela inclut les appels effectués par Redshift pour authentifier un utilisateur d' AWS IAM Identity Center. Cela s'applique que l'utilisateur se connecte de manière interactive ou qu'il se connecte à l'aide d'un jeton AWS IAM Identity Center obtenu par le biais d'une propagation d'identité sécurisée. Pour que ces connexions aboutissent, Redshift doit être en mesure d'accéder à AWS IAM Identity Center depuis votre VPC. Les points de terminaison Interface VPC constituent la méthode recommandée pour fournir cette connectivité. Ils permettent à votre cluster provisionné ou à votre groupe de travail Amazon Redshift Serverless d'accéder à AWS IAM Identity Center via le réseau. AWS

> **Important**
>
> Ces exigences s'appliquent à toute connexion authentifiée via AWS IAM Identity Center. Les utilisateurs IAM et les utilisateurs de bases de données locales s'authentifient via différents mécanismes et ne sont pas affectés. Si le routage VPC amélioré est désactivé, ces points de terminaison ne sont pas nécessaires.

> **Note**
>
> La modification du routage VPC amélioré redémarre un cluster provisionné. Pour plus d'informations sur l'activation du routage VPC amélioré, consultez Activation du routage VPC amélioré.

Points de terminaison de VPC d'Interface

Créez les points de terminaison VPC d'interface suivants (AWS PrivateLink) dans le VPC où réside votre cluster ou votre groupe de travail. Les deux points de terminaison sont obligatoires. Si l'un des terminaux est manquant ou inaccessible, la connexion à AWS IAM Identity Center échoue.

`com.amazonaws.region.sso-oauth`

Valide le jeton d'accès AWS IAM Identity Center que l'utilisateur présente lors de la connexion et l'échange contre un jeton limité à votre session Redshift.

`com.amazonaws.region.identitystore`

Résout l'appartenance de l'utilisateur et de son groupe AWS IAM Identity Center à partir de la banque d'identités AWS IAM Identity Center.

Pour plus d'informations sur la création d'un point de terminaison VPC d'interface, consultez Créer un point de terminaison VPC dans le guide de l'utilisateur Amazon VPC.

Avant de créer les points de terminaison, vérifiez que les `DNS resolution` attributs `DNS hostnames` et sont activés pour le VPC sur lequel s'exécute votre cluster ou groupe de travail. Les noms DNS privés dépendent des deux attributs. Pour plus d'informations, consultez DNS attributes for your VPC (Attributs DNS pour votre VPC) dans le Guide de l'utilisateur d'Amazon VPC.

Le routage VPC amélioré nécessite que votre cluster provisionné ou votre groupe de travail Redshift Serverless ne soit pas accessible au public.

Lorsque vous créez chaque point de terminaison, procédez comme suit :

- Activez les noms DNS privés : Redshift se connecte à ces services à l'aide de leurs noms DNS standard. Sans noms DNS privés, ces noms continuent à être résolus en adresses publiques et les appels ne sont pas acheminés vers vos terminaux.
- Créez les points de terminaison dans la région AWS IAM Identity Center — AWS IAM Identity Center est un service régional. Créez ces points de terminaison dans la région où s'exécute votre instance AWS IAM Identity Center. Si votre cluster ou groupe de travail s'exécute dans une autre région et que vous n'utilisez pas la réplication multirégionale AWS IAM Identity Center, utilisez l'option de point de terminaison interrégional afin que les points de terminaison atteignent la AWS région IAM Identity Center.
- Choisissez des sous-réseaux dans les mêmes zones de disponibilité : sélectionnez des sous-réseaux dans les zones de disponibilité utilisées par votre cluster ou groupe de travail.
- Autoriser le HTTPS entrant : le groupe de sécurité attaché à chaque point de terminaison doit autoriser le trafic entrant sur le port TCP 443 depuis les sous-réseaux de votre cluster ou de votre groupe de travail.
- Conservez la politique de point de terminaison par défaut : la politique par défaut autorise un accès complet. Si votre organisation a besoin d'une politique restrictive en matière de terminaux, définissez-la par principe plutôt que par une liste d'actions. Vérifiez ensuite que la connexion est toujours réussie.

Utilisation AWS Network Firewall

AWS Le pare-feu réseau est facultatif. Si vous filtrez le trafic sortant à l'aide du pare-feu AWS réseau au lieu d'utiliser des points de terminaison VPC d'interface, la politique de pare-feu doit autoriser les domaines de service AWS IAM Identity Center. Sinon, la connexion échoue lorsque Redshift ne peut pas les joindre. Ajoutez les domaines suivants à la liste des domaines autorisés de votre pare-feu, en les *`region`* remplaçant par votre région AWS IAM Identity Center :

`oidc.`*`region`*`.amazonaws.com`

Valide le jeton d'accès AWS IAM Identity Center et l'échange contre un jeton limité à votre session Redshift.

`.sso.region.amazonaws.com`

Atteint le service AWS IAM Identity Center pour résoudre l'application AWS IAM Identity Center et ses attributions.

`identitystore.region.amazonaws.com`

Résout l'appartenance de l'utilisateur et de son groupe AWS IAM Identity Center.

Si votre pare-feu utilise une politique de refus par défaut, il doit également autoriser les domaines que Redshift utilise à fonctionner de manière générale dans le cadre d'un routage VPC amélioré, comme Amazon S3 et, si vous interrogez un lac de données, Glue. AWS Pour plus d'informations, consultez la section Routage VPC amélioré dans Amazon Redshift.

L'utilisation des points de terminaison VPC de l'interface, comme décrit dansPoints de terminaison de VPC d'Interface, permet de maintenir ce trafic sur le AWS réseau et ne nécessite pas de liste d'autorisation du pare-feu.

Création automatique de rôles Amazon Redshift pour AWS IAM Identity Center

Cette fonctionnalité est une intégration AWS IAM Identity Center qui vous permet de créer automatiquement des rôles dans Redshift en fonction de l'appartenance à un groupe.

La création automatique de rôles présente plusieurs avantages. Lorsque vous créez automatiquement un rôle, Redshift le crée avec l'appartenance à un groupe dans votre IdP, ce qui vous permet d'éviter la création et la maintenance manuelles fastidieuses des rôles. Vous avez également la possibilité de filtrer les groupes mappés aux rôles Redshift avec des modèles d'inclusion et d'exclusion.

Comment ça marche

Lorsque vous, en tant qu'utilisateur IdP, vous connectez à Redshift, la séquence d'événements suivante se produit :

1. Redshift récupère les adhésions à vos groupes depuis l'IdP.
2. Redshift crée automatiquement des rôles correspondant à ces groupes, selon le format des rôles *idp_namespace*:*rolename*.
3. Redshift vous accorde des autorisations pour les rôles mappés.

À chaque connexion utilisateur, chaque groupe qui n'est pas présent dans le catalogue mais dont l'utilisateur fait partie est créé automatiquement. Vous pouvez éventuellement définir des filtres d'inclusion et d'exclusion pour contrôler les groupes IdP pour lesquels des rôles Redshift ont été créés.

Configuration de la création automatique des rôles

Utilisez les commandes `CREATE IDENTITY PROVIDER` et `ALTER IDENTITY PROVIDER` pour activer et configurer la création automatique de rôles.

```
-- Create a new IdP with auto role creation enabled
CREATE IDENTITY PROVIDER <idp_name> TYPE AWSIDC
  NAMESPACE '<namespace>'
  APPLICATION_ARN 'app_arn'
  IAM_ROLE 'role_arn'
  AUTO_CREATE_ROLES TRUE;

-- Enable on existing IdP
ALTER IDENTITY PROVIDER <idp_name>
  AUTO_CREATE_ROLES TRUE;

-- Disable
ALTER IDENTITY PROVIDER <idp_name>
  AUTO_CREATE_ROLES FALSE;
```

Groupes de filtres

Vous pouvez éventuellement filtrer les groupes IdP mappés aux rôles Redshift à l'aide des modèles `INCLUDE` et `EXCLUDE`. En cas de conflit entre les modèles, `EXCLUDE` a la priorité sur `INCLUDE`.

```
-- Only create roles for groups with 'dev'
CREATE IDENTITY PROVIDER <idp_name> TYPE AWSIDC
  ...
  AUTO_CREATE_ROLES TRUE
  INCLUDE GROUPS LIKE '%dev%';

-- Exclude 'test' groups
ALTER IDENTITY PROVIDER <idp_name>
  AUTO_CREATE_ROLES TRUE
  EXCLUDE GROUPS LIKE '%test%';
```

Exemples

L'exemple suivant montre comment activer la création automatique de rôles sans filtrage.

```
CREATE IDENTITY PROVIDER prod_idc TYPE AWSIDC  ...
  AUTO_CREATE_ROLES TRUE;
```

L'exemple suivant inclut les groupes de développement et exclut les groupes de test.

```
ALTER IDENTITY PROVIDER prod_idc
  AUTO_CREATE_ROLES TRUE
  INCLUDE GROUPS LIKE '%dev%'
  EXCLUDE GROUPS LIKE '%test%';
```

Bonnes pratiques

Tenez compte des bonnes pratiques suivantes lorsque vous activez la création automatique pour les rôles :

- Utilisez les filtres `INCLUDE` et `EXCLUDE` pour contrôler quels groupes obtiennent des rôles.
- Auditez régulièrement les rôles et nettoyez ceux qui ne sont pas utilisés.
- Tirez parti des hiérarchies de rôles Redshift pour simplifier la gestion des autorisations.

Intégration d'Amazon Redshift aux autorisations d'accès Amazon S3

Grâce à l'intégration aux autorisations d'accès Amazon S3, vous pouvez propager en toute simplicité vos identités IAM Identity Center afin de contrôler l'accès aux données Amazon S3. Cette intégration vous permet d'autoriser l'accès aux données Amazon S3 en fonction des utilisateurs et des groupes IAM Identity Center.

Pour plus d'informations sur les autorisations d'accès Amazon S3, consultez Gestion de l'accès avec les octrois d'accès S3.

L'utilisation des autorisations d'accès Amazon S3 donne à votre application les avantages suivants :

- Fine-grained contrôle d'accès aux données Amazon S3, basé sur les identités IAM Identity Center.
- Gestion centralisée des identités IAM Identity Center sur Amazon Redshift et Amazon S3.
- Vous pouvez éviter de gérer des autorisations IAM distinctes pour l'accès à Amazon S3.

Comment ça marche

Pour intégrer votre application aux autorisations d’accès Amazon S3, procédez comme suit :

- Tout d'abord, vous devez configurer Amazon Redshift pour l'intégrer à Amazon S3 Access Grants à l'aide du Console de gestion AWS ou AWS CLI.
- Ensuite, un utilisateur disposant de privilèges d'administrateur iDC accorde l'accès au bucket ou au préfixe Amazon S3 à un iDC spécifique users/groups, en utilisant le service Amazon S3 Access Grants. Pour plus d’informations, consultez Utilisation des autorisations d’accès S3.
- Lorsqu’un utilisateur IdC authentifié auprès de Redshift exécute une requête pour accéder à S3 (telle qu’une opération COPY, UNLOAD ou Spectrum), Amazon Redshift récupère les informations d’identification d’accès S3 temporaires associées à cette identité IdC auprès du service d’autorisations d’accès Amazon S3.
- Amazon Redshift utilise ensuite les informations d’identification temporaires récupérées pour accéder aux sites Amazon S3 autorisés pour cette requête.

Configuration de l’intégration à Amazon S3 avec les autorisations d’accès Amazon S3

Pour configurer l’intégration avec les autorisations d’accès Amazon S3 pour Amazon Redshift, procédez comme suit :

Rubriques

- Configuration de l'intégration avec Amazon S3 Access Grants à l'aide du Console de gestion AWS
- Activation de l'intégration avec Amazon S3 Access Grants à l'aide du AWS CLI

Configuration de l'intégration avec Amazon S3 Access Grants à l'aide du Console de gestion AWS

1. Ouvrez la console Amazon Redshift.
2. Choisissez votre cluster dans le volet Clusters.
3. Sur la page de détails de votre cluster, dans la section Intégration du fournisseur d’identité, activez l’intégration avec le service Autorisations d’accès S3.

> **Note**
>
> La section Intégration du fournisseur d’identité ne s’affiche pas si IAM Identity Center n’est pas configuré. Pour plus d'informations, voir Activation AWS IAM Identity Center.

Activation de l'intégration avec Amazon S3 Access Grants à l'aide du AWS CLI

1. Pour créer une nouvelle application Amazon Redshift IdC avec l’intégration S3 activée, procédez comme suit :

```
aws redshift create-redshift-idc-application <other parameters>
  --service-integrations '[ {"S3AccessGrants": [{"ReadWriteAccess":
 {"Authorization": "Enabled"}}]} ]'
```

2. Pour modifier une application existante afin d’activer l’intégration des autorisations d’accès S3, procédez comme suit :

```
aws redshift modify-redshift-idc-application <other parameters>
  --service-integrations '[ {"S3AccessGrants": [{"ReadWriteAccess":
 {"Authorization": "Enabled"}}]} ]'
```

3. Pour modifier une application existante afin de désactiver l’intégration des autorisations d’accès S3, procédez comme suit :

```
aws redshift modify-redshift-idc-application <other parameters>
  --service-integrations '[ {"S3AccessGrants": [{"ReadWriteAccess":
 {"Authorization": "Disabled"}}]} ]'
```

Utilisation des intégrations avec les autorisations d’accès S3

Après avoir configuré l’intégration des autorisations d’accès S3, les requêtes qui accèdent aux données S3 (telles que les requêtes `COPY`, `UNLOAD` ou Spectrum) utilisent l’identité IdC pour l’autorisation. Les utilisateurs qui ne sont pas authentifiés à l’aide d’IdC peuvent également exécuter ces requêtes, mais ces comptes utilisateur ne bénéficient pas de l’administration centralisée fournie par IdC.

L’exemple suivant montre les requêtes exécutées avec l’intégration des autorisations d’accès S3.

```
COPY table FROM 's3://mybucket/data';  // -- Redshift uses IdC identity
UNLOAD ('SELECT * FROM table') TO 's3://mybucket/unloaded/'    // -- Redshift uses IdC
 identity
```

Interroger des données via AWS Lake Formation

L'utilisation AWS Lake Formation facilite la gouvernance et la sécurisation centralisées de votre lac de données, ainsi que la fourniture d'un accès aux données. La configuration de la propagation des identités vers Lake Formation via AWS IAM Identity Center et Redshift permet à un administrateur d'autoriser un accès précis à un lac de données Amazon S3, en fonction des groupes de fournisseurs d'identité (IdP) de l'organisation. Ces groupes sont gérés via AWS IAM Identity Center. Cette section explique comment configurer quelques cas d'utilisation, les requêtes depuis un lac de données et les requêtes depuis un partage de données, qui montrent comment tirer parti d' AWS IAM Identity Center avec Redshift pour se connecter aux ressources du lac. Formation-governed

À l'aide d'un AWS Connexion IAM Identity Center et Redshift pour interroger un lac de données

Ces étapes concernent un cas d'utilisation dans lequel vous utilisez AWS IAM Identity Center connecté à Redshift pour interroger un lac de données régi par Lake Formation.

Prérequis

Cette procédure exige plusieurs étapes préalables :

1. AWS IAM Identity Center doit être configuré pour prendre en charge l'authentification et la gestion des identités avec Redshift. Vous pouvez activer AWS IAM Identity Center depuis la console et sélectionner une source de fournisseur d'identité (IdP). Ensuite, synchronisez un ensemble d'utilisateurs de votre IdP avec AWS IAM Identity Center. Vous devez également configurer une connexion entre AWS IAM Identity Center et Redshift, en suivant les étapes décrites précédemment dans ce document.
2. Créez un nouveau cluster Amazon Redshift et activez la gestion des identités via AWS IAM Identity Center lors des étapes de configuration.
3. Créez une application AWS IAM Identity Center gérée pour Lake Formation et configurez-la. Cela fait suite à la configuration de la connexion entre AWS IAM Identity Center et Redshift. La procédure est la suivante :
   a. Dans le AWS CLI, utilisez la `modify-redshift-idc-application` commande pour activer l'intégration du service Lake Formation à l'application gérée AWS IAM Identity Center pour Redshift. Cet appel inclut le paramètre `service-integrations`, qui est défini sur une valeur de chaîne de configuration qui active l’autorisation pour accéder à Lake Formation.
   b. Configurez Lake Formation à l’aide de la commande `create-lake-formation-identity-center-configuration`. Cela crée une application AWS IAM Identity Center pour Lake Formation, qui est visible sur le portail AWS IAM Identity Center. L'administrateur doit définir l'`--`

`cli-input-json`argument, dont la valeur est le chemin d'accès à un fichier JSON qui utilise le format standard pour tous les appels d'API AWS CLI. Vous devez inclure des valeurs pour :

- `CatalogId` : l'identifiant du catalogue Lake Formation.
- `InstanceArn`— La valeur ARN de l'instance AWS IAM Identity Center.

Une fois que l'administrateur a terminé la configuration prérequise, l'administrateur de base de données peut créer un schéma externe dans le but d'interroger le lac de données.

1. L'administrateur crée le schéma externe : l'administrateur de base de données Redshift se connecte à la base de données et crée un schéma externe à l'aide de l'instruction SQL suivante :

   ```
   CREATE EXTERNAL SCHEMA if not exists my_external_schema from DATA CATALOG database
    'my_lf_integrated_db' catalog_id '12345678901234';
   ```

   Notez qu'il n'est pas nécessaire de spécifier un rôle IAM dans ce cas, car l'accès est géré via AWS IAM Identity Center.

2. L'administrateur accorde des autorisations : l'administrateur accorde l'utilisation à un groupe AWS IAM Identity Center, qui accorde des autorisations sur les ressources Redshift. Cela s'effectue en exécutant une instruction SQL telle que la suivante :

   ```
   GRANT USAGE ON SCHEMA "my_external_schema" to "MYCO:sales";
   ```

   Ensuite, l'administrateur accorde des autorisations à Lake Formation sur les objets, en fonction des exigences de l'organisation, à l'aide de l' AWS interface de ligne de commande :

   ```
   aws lakeformation grant-permissions ...
   ```

3. Les utilisateurs exécutent des requêtes : à ce stade, un utilisateur AWS IAM Identity Center qui fait partie du groupe de vente peut, à des fins d'illustration, se connecter via l'éditeur de requêtes v2 à la base de données Redshift. Il peut ensuite exécuter une requête qui accède à une table dans le schéma externe, comme dans l'exemple suivant :

   ```
   SELECT * from my_external_schema.table1;
   ```

À l'aide d'un AWS Connexion IAM Identity Center et Redshift pour se connecter à un partage de données

Vous pouvez accéder à un partage de données depuis un autre entrepôt de données Redshift lorsque l'accès est géré via AWS IAM Identity Center. Pour ce faire, vous devez exécuter une requête pour configurer une base de données externe. Avant de terminer ces étapes, il est supposé qu'une connexion est configurée entre Redshift et AWS IAM Identity Center et que vous avez créé l' AWS Lake Formation application, comme indiqué dans la procédure précédente.

1. Création de la base de données externe : l'administrateur crée une base de données externe pour le partage des données, en la référençant via son ARN. Voici un exemple qui montre comment procéder :

   ```
   CREATE DATABASE "redshift_external_db" FROM ARN 'arn:aws:glue:us-
   east-1:123456789012:database/redshift_external_db-iad' WITH NO DATA CATALOG SCHEMA;
   ```

   Dans ce cas d'utilisation, où vous utilisez AWS IAM Identity Center avec Redshift pour la gestion des identités, le rôle IAM n'est pas inclus.

2. L'administrateur définit les autorisations : après avoir créé une base de données, l'administrateur en accorde l'utilisation à un groupe AWS IAM Identity Center. Cela accorde des autorisations sur les ressources Redshift :

   ```
   GRANT USAGE ON DATABASE "my_external_db" to "MYCO:sales";
   ```

   L'administrateur accorde également à Lake Formation des autorisations sur les objets, à l'aide de l'interface de ligne de commande AWS :

   ```
   aws lakeformation grant-permissions ...
   ```

3. Les utilisateurs exécutent des requêtes : un utilisateur du groupe de vente peut interroger une table figurant dans la base de données, en fonction des autorisations attribuées :

   ```
   select * from redshift_external_db.public.employees;
   ```

Pour plus d'informations sur l'octroi d'autorisations sur un lac de données et sur l'octroi d'autorisations sur les partages de données, consultez Octroi d'autorisations aux utilisateurs et aux

groupes. Pour plus d'informations sur l'octroi de l'autorisation d'utilisation à un schéma ou à une base de données, consultez GRANT.

Intégration de votre application ou de votre outil à OAuth à l'aide d'un émetteur de jetons approuvé

Vous pouvez ajouter des fonctionnalités aux outils clients que vous créez pour vous connecter à Redshift via la connexion AWS IAM Identity Center. Si vous avez déjà configuré l'intégration de Redshift à AWS IAM Identity Center, utilisez les propriétés détaillées dans cette section pour configurer une connexion.

Plugin d'authentification pour se connecter à Redshift à l'aide de AWS IAM Identity Center

Vous pouvez utiliser AWS IAM Identity Center pour vous connecter à Amazon Redshift à l'aide des plug-ins de pilote suivants :

- `BrowserIdcAuthPlugin`— Ce plug-in facilite l'intégration fluide de l'authentification unique avec AWS IAM Identity Center. Il crée une fenêtre de navigateur permettant aux utilisateurs de se connecter avec les informations d'identification définies dans leurs fournisseurs d'identité d'entreprise.
- `IdpTokenAuthPlugin`— Ce plug-in doit être utilisé par les applications qui souhaitent gérer elles-mêmes le flux d'authentification, au lieu de laisser le pilote Amazon Redshift ouvrir une fenêtre de navigateur pour l'authentification AWS IAM Identity Center. Il accepte un jeton d'accès automatique AWS IAM Identity Center ou un jeton Web JSON (JWT) OpenID Connect (OIDC) provenant de tout fournisseur d'identité Web connecté à AWS IAM Identity Center, tel qu'Okta PingOne, et Microsoft Entra ID (Azure AD). L'application cliente est chargée de générer cet accès requis token/JWT.

Authentification avec **`BrowserIdcAuthPlugin`**

Utilisez les noms de plug-in suivants pour vous connecter à l'aide de `BrowserIdcAuthPlugin`, en fonction de votre pilote Amazon Redshift.

Pilote	Clé d'option de connexion	Value	Remarques
JDBC	`plugin_name`	com.amazon.redshift.plugin. BrowserIdcAuthPlugin	Vous devez saisir le nom de classe complet du plug-in

Pilote	Clé d'option de connexion	Value	Remarques
			lorsque vous vous connectez.
ODBC	`plugin_name`	BrowserIdcAuthPlugin	
Python	`credentials_provider`	BrowserIdcAuthPlugin	Aucune option `plugin_name` n'est disponible pour le pilote Python. Utilisez à la place `credentials_provider` .

Le plug-in `BrowserIdcAuthPlugin` possède les options de connexion supplémentaires suivantes :

Nom d'option	Obligatoire ?	Description	Exemple
idc_region	Obligatoire	L' Région AWS endroit où se trouve l'instance AWS IAM Identity Center.	us-east-1
issuer_url	Obligatoire	Point de terminaison de l'instance du serveur AWS IAM Identity Center. Vous pouvez trouver cette valeur à l'aide de la console AWS IAM Identity Center.	https://identitycenter.amazonaws.com/ssoins-g5j2k70sn4yc5nsc
listen_port	Facultatif	Port utilisé par le pilote Amazon Redshift pour recevoir la `auth_code`	7890

Nom d'option	Obligatoire ?	Description	Exemple
		réponse d' AWS IAM Identity Center via la redirection du navigateur.	
idc_client_display_name	Facultatif	Nom que le client AWS IAM Identity Center utilise pour l'application dans la fenêtre contextuelle de consentement à l'authentification unique de l' AWS IAM Identity Center.	Pilote Amazon Redshift
idp_response_timeout	Facultatif	Durée, en secondes, pendant laquelle le pilote Redshift attend la fin du flux d'authentification.	60

Vous devez entrer ces valeurs dans les propriétés de connexion de l'outil que vous créez et utilisez pour vous connecter. Pour plus d'informations, consultez la documentation relative aux options de connexion pour chaque pilote :

- Options de configuration du pilote JDBC version 2.x
- Options du pilote ODBC
- Options de configuration du connecteur Amazon Redshift Python

Authentification avec **`IdpTokenAuthPlugin`**

Utilisez les noms de plug-in suivants pour vous connecter à l'aide de `IdpTokenAuthPlugin`, en fonction de votre pilote Amazon Redshift.

Pilote	Clé d'option de connexion	Value	Remarques
JDBC	`plugin_name`	com.amazon.redshift.plugin. IdpTokenAuthPlugin	Vous devez saisir le nom de classe complet du plug-in lorsque vous vous connectez.
ODBC	`plugin_name`	IdpTokenAuthPlugin	
Python	`credentials_provider`	IdpTokenAuthPlugin	Aucune option `plugin_name` n'est disponible pour le pilote Python. Utilisez à la place `credentials_provider` .

Le plug-in `IdpTokenAuthPlugin` possède les options de connexion supplémentaires suivantes :

Nom d'option	Obligatoire ?	Description
jeton	Obligatoire	Un jeton d'accès automatique AWS IAM Identity Center ou un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d'identité Web connecté à IAM Identity Center. AWS Votre application doit générer ce jeton en authentifiant l'utilisateur de votre application auprès d' AWS IAM Identity Center ou d'un fournisseur d'identité connecté à AWS IAM Identity Center.

Nom d'option	Obligatoire ?	Description
token_type	Obligatoire	Type de jeton utilisé pour `IdpTokenAuthPlugin` . Les valeurs possibles sont les suivantes : • ACCESS_TOKEN — Entrez ceci si vous utilisez un jeton d'accès fourni par AWS IAM Identity Center. • EXT_JWT — Entrez cette valeur si vous utilisez un jeton Web JSON (JWT) OpenID Connect (OIDC) fourni par un fournisseur d'identité Web connecté à IAM Identity Center. AWS

Vous devez entrer ces valeurs dans les propriétés de connexion de l'outil que vous créez et utilisez pour vous connecter. Pour plus d'informations, consultez la documentation relative aux options de connexion pour chaque pilote :

- Options de configuration du pilote JDBC version 2.x
- Options du pilote ODBC
- Options de configuration du connecteur Amazon Redshift Python

Résolution des problèmes de connexion à l'aide de Amazon Redshift Query Editor V2

Cette liste détaille les erreurs qui se produisent fréquemment et peut vous aider à vous connecter à votre base de données Redshift avec l'éditeur de requêtes v2, à l'aide d'une identité AWS IAM Identity Center.

- Error: Connection Issue: No Identity center session information available. — Lorsque cette erreur se produit, vérifiez les paramètres de sécurité et de confidentialité de votre navigateur. Ces paramètres du navigateur, en particulier ceux relatifs aux cookies sécurisés, tels que la

fonctionnalité Total Cookie Protection de Firefox, peuvent bloquer les tentatives de connexion entre Amazon Redshift Query Editor V2 et une base de données Redshift. Suivez les étapes de correction détaillées pour votre navigateur :

- Firefox : actuellement, les cookies tiers sont bloqués par défaut. Cliquez sur le bouclier dans la barre d'adresse du navigateur et activez le bouton pour désactiver la protection améliorée contre le suivi pour l'éditeur de requêtes v2.
- Mode navigation privée de Chrome : par défaut, le mode navigation privée de Chrome bloque les cookies tiers. Cliquez sur l'icône en forme d'œil dans la barre d'adresse pour autoriser les cookies tiers pour l'éditeur de requêtes v2. Après avoir modifié le paramètre pour autoriser les cookies, il est possible que l'icône en forme d'œil ne s'affiche pas dans la barre d'adresse.
- Safari : sur un Mac, ouvrez l'application Safari. Choisissez Paramètres, puis Paramètres avancés. Activez pour désactiver : Bloquer tous les cookies.
- Edge : choisissez Paramètres, puis choisissez Cookies et autorisations du site. Sélectionnez ensuite Gérer et supprimer les cookies et les données du site, puis désactivez Bloquer les cookies tiers.

Si vous essayez de vous connecter après avoir modifié les paramètres et que vous continuez à recevoir le message d'erreur Problème de connexion : aucune information de session du centre d'identité disponible, nous vous recommandons d'actualiser votre connexion avec AWS IAM Identity Center. Pour ce faire, cliquez avec le bouton droit sur votre instance de base de données Redshift et choisissez Actualiser. Une nouvelle fenêtre apparaît, dans laquelle vous pouvez vous authentifier.

- Error: Connection issue: Identity center session expired or invalid. — Suite à l'intégration d'un cluster provisionné par Redshift ou d'un groupe de travail sans serveur avec AWS IAM Identity Center, un utilisateur peut recevoir cette erreur lorsqu'il tente de se connecter à une base de données Redshift depuis l'éditeur de requêtes v2. Cela peut faire suite à des tentatives de connexion réussies. Dans ce cas, nous vous recommandons de vous authentifier à nouveau. Pour ce faire, cliquez avec le bouton droit sur votre instance de base de données Redshift et choisissez Actualiser. Une nouvelle fenêtre apparaît, dans laquelle vous pouvez vous authentifier.
- Error: Invalid scope. User credentials are not authorized to connect to Redshift. — Suite à l'intégration d'un cluster provisionné par Redshift ou d'un groupe de travail sans serveur avec AWS IAM Identity Center pour la gestion des identités, un utilisateur peut recevoir cette erreur lorsqu'il tente de se connecter à une base de données Redshift depuis l'éditeur de requêtes v2. Dans ce cas, pour que l'éditeur de requêtes v2 puisse connecter et authentifier correctement un utilisateur via AWS IAM Identity Center pour accéder aux ressources appropriées, un administrateur doit affecter l'utilisateur à l'application Redshift AWS IAM Identity Center via la console Redshift. Ceci

est effectué dans le cadre des Connexions IAM Identity Center. Ensuite, l'utilisateur peut établir une connexion réussie au bout d'une heure, ce qui correspond à la limite de la mise en cache des sessions AWS IAM Identity Center.

- Error: Databases couldn't be listed. FATAL: Failed query when cluster is auto paused. — Lorsqu'une base de données Amazon Redshift Serverless est inactive et ne traite aucune charge de travail, elle peut rester en pause lorsque vous vous connectez avec une identité AWS IAM Identity Center. Pour y remédier, connectez-vous à l'aide d'une autre méthode d'authentification afin de reprendre le groupe de travail sans serveur. Connectez-vous ensuite à la base de données avec votre identité AWS IAM Identity Center.
- Error: An error occurred during the attempt to federate with AWS IAM Identity Center. Un administrateur Amazon Redshift doit supprimer et recréer l'application AWS IAM Identity Center QEV2 à l'aide de la console Redshift. — Cette erreur se produit généralement lorsque l'instance d'application AWS IAM Identity Center associée à l'éditeur de requêtes v2 est supprimée. Pour y remédier, un administrateur Amazon Redshift doit supprimer et recréer les applications Redshift et Query Editor v2 pour AWS IAM Identity Center. Cela peut être effectué sur la console Redshift ou à l'aide de la commande CLI https://docs.aws.amazon.com/cli/latest/reference/redshift/delete-redshift-idc-application.html.

Utilisation des rôles liés à un service pour Amazon Redshift

Amazon Redshift utilise des rôles liés à un Gestion des identités et des accès AWS service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Amazon Redshift. Service-linked les rôles sont prédéfinis par Amazon Redshift et incluent toutes les autorisations requises par le service pour appeler AWS des services au nom de votre cluster Amazon Redshift.

Un rôle lié à un service facilite la configuration d'Amazon Redshift, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Le rôle est lié aux cas d'utilisation d'Amazon Redshift et dispose de permissions prédéfinies. Seul Amazon Redshift peut endosser le rôle, et seul le rôle lié au service peut utiliser la stratégie d'autorisations prédéfinie. Amazon Redshift crée un rôle lié à un service dans votre compte la première fois que vous créez un cluster ou un point de terminaison VPC. Redshift-managed Vous ne pouvez supprimer le rôle lié au service qu'après avoir supprimé tous les clusters Amazon Redshift ou points de terminaison Redshift-managed VPC de votre compte. Vos ressources Amazon Redshift sont ainsi protégées, car vous ne pouvez pas involontairement supprimer les autorisations nécessaires pour y accéder.

Amazon Redshift prend en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Régions et points de terminaison AWS.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la valeur est Oui dans la Service-Linked colonne Rôle. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Service-linked autorisations de rôle pour Amazon Redshift

Amazon Redshift utilise le rôle lié au service nommé — Permet à AWSServiceRoleForRedshiftAmazon Redshift d'appeler les services en votre nom. AWS Ce rôle lié à un service est attaché à la politique gérée suivante : `AmazonRedshiftServiceLinkedRolePolicy`. Pour obtenir des mises à jour de cette stratégie, consultez Stratégies (prédéfinies) gérées par AWS pour Amazon Redshift.

Le rôle AWSServiceRoleForRedshift lié au service fait confiance uniquement **`redshift.amazonaws.com`** pour assumer le rôle.

La politique d'autorisation des rôles AWSServiceRoleForRedshift liés au service permet à Amazon Redshift d'effectuer les opérations suivantes sur toutes les ressources associées :

- `ec2:DescribeVpcs`
- `ec2:DescribeSubnets`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeAddress`
- `ec2:AssociateAddress`
- `ec2:DisassociateAddress`
- `ec2:CreateNetworkInterface`
- `ec2:DeleteNetworkInterface`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:CreateVpcEndpoint`
- `ec2:DeleteVpcEndpoints`
- `ec2:DescribeVpcEndpoints`
- `ec2:ModifyVpcEndpoint`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeSecurityGroups`

- `ec2:DescribeInternetGateways`
- `ec2:DescribeSecurityGroupRules`
- `ec2:DescribeAvailabilityZones`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:AssignIpv6Addresses`
- `ec2:UnassignIpv6Addresses`

Autorisations pour les ressources réseau

Les autorisations suivantes permettent d'effectuer des actions de création et de gestion de règles de groupe de sécurité dans Amazon EC2. Ces groupes et règles de sécurité sont spécifiquement associés à la balise de ressource Amazon Redshift `aws:RequestTag/Redshift`. Cela permet de limiter l'étendue des autorisations à des ressources Amazon Redshift spécifiques.

- `ec2:CreateSecurityGroup`
- `ec2:AuthorizeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`
- `ec2:ModifySecurityGroupRules`
- `ec2:DeleteSecurityGroup`

Autorisations pour les quotas de service

Les autorisations suivantes permettent à l'appelant d'obtenir des quotas de service.

`servicequotas:GetServiceQuota`

Le fragment JSON suivant montre l'action et l'étendue des ressources pour les quotas de service.

```
{
   "Sid": "ServiceQuotasToCheckCustomerLimits",
   "Effect": "Allow",
```

```
   "Action": [
      "servicequotas:GetServiceQuota"
   ],
   "Resource": [
      "arn:aws:servicequotas:*:*:ec2/L-0263D0A3",
      "arn:aws:servicequotas:*:*:vpc/L-29B6F2EB"
   ]
}
```

Les codes de quota sont les suivants :

- L-0263D0A3— Le code de quota pour les adresses IP EC2-VPC élastiques.
- L-29B6F2EB— Le code de quota pour les points de terminaison VPC d'interface par VPC.

Pour plus d’informations, consultez Quotas de service AWS.

Actions pour la journalisation des audits

Les actions répertoriées avec le préfixe `logs` concernent la journalisation des audits et les fonctions associées. Plus précisément, la création et la gestion de groupes de journaux et de flux de journaux.

- `logs:CreateLogGroup`
- `logs:PutRetentionPolicy`
- `logs:CreateLogStream`
- `logs:PutLogEvents`
- `logs:DescribeLogStreams`
- `logs:GetLogEvents`

Le fichier JSON suivant affiche la portée des actions et des ressources, à Amazon Redshift, pour la journalisation des audits.

```
[
    {
        "Sid": "EnableCreationAndManagementOfRedshiftCloudwatchLogGroups",
        "Effect": "Allow",
        "Action": [
            "logs:CreateLogGroup",
            "logs:PutRetentionPolicy"
```

```
        ],
        "Resource": [
            "arn:aws:logs:*:*:log-group:/aws/redshift/*"
        ]
    },
    {
        "Sid": "EnableCreationAndManagementOfRedshiftCloudwatchLogStreams",
        "Effect": "Allow",
        "Action": [
            "logs:CreateLogStream",
            "logs:PutLogEvents",
            "logs:DescribeLogStreams",
            "logs:GetLogEvents"
        ],
        "Resource": [
            "arn:aws:logs:*:*:log-group:/aws/redshift/*:log-stream:*"
        ]
    }
]
```

Pour plus d'informations sur les rôles liés à un service et leur fonction dans AWS, consultez la section Utilisation des rôles liés à un service. Pour plus d’informations sur des actions spécifiques et d’autres ressources IAM pour Amazon Redshift, consultez Actions, ressources et clés de condition pour Amazon Redshift.

Actions de gestion des informations d'identification d'administrateur avec AWS Secrets Manager

Les actions répertoriées avec le préfixe `secretsmanager` concernent l’utilisation d’Amazon Redshift pour gérer vos informations d’identification d’administrateur. Ces actions permettent à Amazon Redshift de créer et AWS Secrets Manager de gérer les secrets de vos identifiants d'administrateur.

Le JSON suivant indique les actions et l'étendue des ressources, pour Amazon Redshift, pour gérer les informations d'identification d'administrateur avec. AWS Secrets Manager

```
[
    {
        "Effect": "Allow",
        "Action": [
            "secretsmanager:DescribeSecret",
            "secretsmanager:DeleteSecret",
            "secretsmanager:PutSecretValue",
            "secretsmanager:UpdateSecret",
```

```
            "secretsmanager:UpdateSecretVersionStage",
            "secretsmanager:RotateSecret"
        ],
        "Resource": [
            "arn:aws:secretsmanager:*:*:secret:redshift!*"
        ],
        "Condition": {
            "StringEquals": {
                "secretsmanager:ResourceTag/aws:secretsmanager:owningService":
 "redshift"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetRandomPassword"
        ],
        "Resource": "*"
    }
]
```

Actions pour enregistrer des clusters et des espaces de noms sans serveur dans le AWS Glue Data Catalog

Les actions répertoriées avec le `glue` préfixe concernent l'accès aux catalogues créés à partir de l'enregistrement de clusters provisionnés AWS Glue Data Catalog ou d'espaces de noms sans serveur. Pour plus d'informations, consultez Compatibilité d'Apache Iceberg pour Amazon Redshift dans le Guide du développeur de base de données Amazon Redshift.

Le fichier JSON suivant affiche la portée des actions et des ressources, à Amazon Redshift, pour accéder aux catalogues dans le AWS Glue Data Catalog :

```
[
    {
        "Sid": "DiscoverRedshiftCatalogs",
        "Effect": "Allow",
        "Action": [
            "glue:GetCatalogs",
            "glue:GetCatalog"
        ],
        "Resource": [
            "arn:aws:glue:*:*:catalog",
```

```
            "arn:aws:glue:*:*:catalog/*"
        ],
   "Condition":
    {
        "Bool":
        {
            "glue:EnabledForRedshiftAutoDiscovery": "true"
        },
        "StringEquals": {
             "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
 },
 {
    "Sid": "LakeFormationGetMetadataAccessForFederatedCatalogs",
    "Effect": "Allow",
    "Action": [
        "lakeformation:GetDataAccess"
    ],
    "Resource": [ "*" ],
    "Condition":
    {
        "Bool":
        {
            "lakeformation:EnabledOnlyForMetaDataAccess":"true"
        },
        "StringEquals": {
             "aws:ResourceAccount": "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals":
        {
            "aws:CalledVia": "glue.amazonaws.com"
        }
    }
 }
    }
]
```

Les autorisations `glue:GetCatalog` et `glue:GetCatalogs` sont soumises à une condition `glue:EnabledForRedshiftAutoDiscovery:true`, ce qui signifie qu'Amazon Redshift accorde l'accès à IAM pour la découverte automatique des catalogues. Pour vous désinscrire, ajoutez une politique de ressources AWS Glue au niveau du compte afin de refuser de manière sélective l'accès aux catalogues aux rôles liés au service. Étant donné que le rôle lié au service comporte déjà une

action d'autorisation explicite dans la politique, la politique de désinscription doit explicitement refuser cette action. Prenez l'exemple suivant, où une politique supplémentaire refuse la découverte automatique pour Amazon Redshift :

JSON

```
{
  "Version":"2012-10-17",
  "Statement" : {
            "Effect": "Deny",
            "Action": [
                "glue:GetCatalog",
                "glue:GetCatalogs"
            ],
            "Principal" : {
            "AWS" : "arn:aws:iam::111122223333:role/aws-service-role/
redshift.amazonaws.com/AWSServiceRoleForRedshift"
            },
            "Resource": [
                "arn:aws:glue:*:*:catalog/<s3_table_catalog_name>",
                "arn:aws:glue:*:*:catalog/<s3_table_catalog_name>/*"
            ]
        }
}
```

Pour autoriser une entité IAM à créer des rôles liés à un AWSServiceRoleForRedshift service

```
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "arn:aws:iam::<AWS-account-ID>:role/aws-service-role/
redshift.amazonaws.com/AWSServiceRoleForRedshift",
    "Condition": {"StringLike": {"iam:AWSServiceName": "redshift.amazonaws.com"}}
}
```

Pour autoriser une entité IAM à supprimer des rôles liés à un AWSServiceRoleForRedshift service

Ajoutez la déclaration de stratégie suivante aux autorisations de cette entité IAM :

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::<AWS-account-ID>:role/aws-service-role/
redshift.amazonaws.com/AWSServiceRoleForRedshift",
    "Condition": {"StringLike": {"iam:AWSServiceName": "redshift.amazonaws.com"}}
}
```

Vous pouvez également utiliser une politique AWS gérée pour fournir un accès complet à Amazon Redshift.

Création d'un rôle lié à un service pour Amazon Redshift

Il n'est pas nécessaire de créer manuellement un rôle AWSServiceRoleForRedshift lié à un service. Amazon Redshift crée automatiquement le rôle lié au service. Si le rôle AWSServiceRoleForRedshift lié au service a été supprimé de votre compte, Amazon Redshift le crée lorsque vous lancez un nouveau cluster Amazon Redshift.

> **Important**
>
> Si vous avez utilisé le service Amazon Redshift avant le 18 septembre 2017, date à laquelle il a commencé à prendre en charge les rôles liés au service, Amazon Redshift a créé le rôle dans votre compte. AWSServiceRoleForRedshift Pour en savoir plus, consultez Un nouveau rôle est apparu dans mon compte IAM.

Modification d'un rôle lié à un service pour Amazon Redshift

Amazon Redshift ne vous permet pas de modifier le rôle lié au AWSServiceRoleForRedshift service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Vous pouvez toutefois modifier la description du rôle à l'aide de la console IAM, du AWS Command Line Interface (AWS CLI) ou de l'API IAM. Pour plus d'informations, consultez Modification d'un rôle dans le Guide de l'utilisateur IAM.

Suppression d’un rôle lié à un service pour Amazon Redshift

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.

Avant de pouvoir supprimer un rôle lié à un service pour un compte, vous devez arrêter et supprimer tous les clusters du compte. Pour de plus amples informations, veuillez consulter Arrêt et suppression d’un cluster.

Vous pouvez utiliser la console IAM AWS CLI, ou l'API IAM pour supprimer un rôle lié à un service. Pour plus d’informations, consultez la section Suppression d’un rôle lié à un service dans le Guide de l’utilisateur IAM.

Utilisation de l’authentification IAM pour générer des informations d’identification de l’utilisateur de base de données

Vous pouvez générer des informations d'identification de base de données temporaires basées sur les autorisations accordées par le biais d'une politique d'autorisations Gestion des identités et des accès AWS (IAM) pour gérer l'accès de vos utilisateurs à votre base de données Amazon Redshift.

Généralement, les utilisateurs de base de données Amazon Redshift se connectent à la base de données en fournissant un nom d'utilisateur de base de données et un mot de passe. Toutefois, vous n'avez pas à conserver les noms d'utilisateur et les mots de passe dans votre base de données Amazon Redshift. Vous pouvez également configurer votre système de manière à permettre aux utilisateurs de créer des informations d'identification utilisateur et de se connecter aux bases de données en fonction de leurs informations d'identification IAM.

Amazon Redshift fournit l'opération d'GetClusterCredentialsAPI permettant de générer des informations d'identification utilisateur temporaires pour la base de données. Vous pouvez configurer votre client SQL avec les pilotes Amazon Redshift JDBC ou ODBC qui gèrent le processus d'appel de l'opération `GetClusterCredentials`. Pour ce faire, ils récupèrent les informations d'identification de l'utilisateur de la base de données et établissent une connexion entre votre client SQL et votre base de données Amazon Redshift. Vous pouvez également utiliser votre application de base de données pour appeler par programmation l'opération `GetClusterCredentials`, récupérer les informations d'identification de l'utilisateur de base de données et vous connecter à la base de données.

Si vous gérez déjà les identités des utilisateurs en externe AWS, vous pouvez utiliser un fournisseur d'identité (IdP) conforme au langage SAML (Security Assertion Markup Language) 2.0 pour gérer l'accès aux ressources Amazon Redshift. Vous pouvez configurer votre IdP de manière à permettre à vos utilisateurs fédérés d'accéder à un rôle IAM. Avec ce rôle IAM, vous pouvez générer des informations d'identification temporaires de base de données et vous connecter aux bases de données Amazon Redshift.

Votre client SQL a besoin d'une autorisation pour appeler l'opération `GetClusterCredentials` pour vous. Vous gérez ces autorisations en créant un rôle IAM et en attachant une politique d'autorisations IAM qui accorde ou restreint l'accès à l'opération `GetClusterCredentials` et aux actions associées. Il est recommandé d'associer des politiques d'autorisation à un rôle IAM, puis de l'attribuer à des utilisateurs et à des groupes, le cas échéant. Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift.

La politique accorde ou restreint également l'accès à des ressources spécifiques, telles que des clusters Amazon Redshift, des bases de données, des noms d'utilisateur de base de données et des noms de groupes d'utilisateurs.

> **Note**
>
> Nous vous recommandons d'utiliser les pilotes Amazon Redshift JDBC ou ODBC pour gérer le processus d'appel de l'opération `GetClusterCredentials` et de connexion à la base de données. Pour plus de simplicité, nous supposons que vous utilisez un client SQL avec les pilotes JDBC ou ODBC dans cette rubrique.
> Pour des détails spécifiques et des exemples d'utilisation de l'`GetClusterCredentials`opération ou de la commande `get-cluster-credentials` CLI parallèle, consultez GetClusterCredentials et get-cluster-credentials.

Pour gérer l'authentification et l'autorisation de manière centralisée, Amazon Redshift prend en charge l'authentification de base de données avec IAM, ce qui permet l'authentification des utilisateurs via la fédération d'entreprise. Au lieu de créer un utilisateur, vous pouvez utiliser des identités existantes provenant de AWS Directory Service votre répertoire d'utilisateurs d'entreprise ou d'un fournisseur d'identité Web. Ces utilisateurs sont connus sous le nom d'utilisateurs fédérés. AWS attribue un rôle à un utilisateur fédéré lorsque l'accès est demandé via un IdP.

Pour fournir un accès fédéré à un utilisateur ou une application client dans votre organisation pour appeler les opérations de l'API Amazon Redshift, vous pouvez également utiliser le pilote JDBC

ou ODBC avec la prise en charge de SAML 2.0 pour demander l'authentification de l'IdP de votre organisation. Dans ce cas, les utilisateurs de l'organisation ne disposent pas d'un accès direct à Amazon Redshift.

Pour plus d'informations, veuillez consulter la rubrique Fournisseurs d'identité et fédération dans le Guide de l'utilisateur IAM.

Création d'informations d'identification temporaires IAM

Dans cette section, vous trouverez comment configurer votre système pour générer des informations d'identification utilisateur de IAM-based base de données temporaires et pour vous connecter à votre base de données à l'aide des nouvelles informations d'identification.

Au niveau général, le processus se déroule comme suit :

1. Étape 1 : créer un rôle IAM pour un accès IAM par authentification unique

   (Facultatif) Vous pouvez authentifier des utilisateurs pour l'accès à une base de données Amazon Redshift en intégrant l'authentification IAM et un fournisseur d'identité (IdP) tiers.
2. Étape 2 : Configurer des assertions SAML pour votre IdP

   (Facultatif) Pour utiliser l'authentification IAM à l'aide d'un IdP, vous devez définir une règle de demande dans votre application d'IdP qui mappe des utilisateurs ou des groupes de votre organisation au rôle IAM. Le cas échéant, vous pouvez inclure des éléments d'attribut pour définir des paramètres `GetClusterCredentials`.
3. Étape 3 : créer un rôle IAM avec l'autorisation d'appeler ou GetClusterCredentialsWithIAM GetClusterCredentials

   Votre application client SQL assume l'utilisateur lorsqu'elle appelle l'opération `GetClusterCredentials`. Si vous avez créé un rôle IAM pour l'accès au fournisseur d'identité, vous pouvez ajouter l'autorisation nécessaire à ce rôle.
4. Étape 4 : Créer un utilisateur de base de données et des groupes de bases de données

   (Facultatif) Par défaut, `GetClusterCredentials` renvoie les informations d'identification pour créer un nouvel utilisateur si le nom d'utilisateur n'existe pas. Vous pouvez également choisir de spécifier les groupes d'utilisateurs que les utilisateurs rejoignent lors de la connexion. Par défaut, les utilisateurs de base de données rejoignent le groupe PUBLIC.
5. Étape 5 : Configurer une connexion JDBC ou ODBC pour utiliser des informations d'identification IAM

Afin de vous connecter à votre base de données Amazon Redshift, vous configurez votre client SQL pour utiliser un pilote Amazon Redshift JDBC ou ODBC .

Étape 1 : créer un rôle IAM pour un accès IAM par authentification unique

Si vous n'utilisez pas de fournisseur d'identité pour l'accès avec authentification unique, vous pouvez ignorer cette étape.

Si vous gérez déjà les identités des utilisateurs en dehors de AWS, vous pouvez authentifier les utilisateurs pour accéder à une base de données Amazon Redshift en intégrant l'authentification IAM et un fournisseur d' SAML-2.0 identité tiers (IdP).

Pour plus d'informations, veuillez consulter la rubrique Fournisseurs d'identité et fédération dans le Guide de l'utilisateur IAM.

Avant de pouvoir utiliser l'authentification Amazon Redshift IdP, créez un fournisseur d'identité AWS SAML. Vous créez un IdP dans la console IAM pour fournir des AWS informations sur l'IdP et sa configuration. Cela permet d'établir une relation de confiance entre votre AWS compte et l'IdP. Pour connaître les étapes de création d'un rôle, veuillez consulter la rubrique Création d'un rôle pour la fédération SAML 2.0 (Console) dans le Guide de l'utilisateur IAM.

Étape 2 : Configurer des assertions SAML pour votre IdP

Une fois que vous avez créé le rôle IAM, vous définissez une règle de demande dans votre application d'IdP qui mappe des utilisateurs ou des groupes de votre organisation au rôle IAM. Pour plus d'informations, veuillez consulter la rubrique Configuration des assertions SAML pour la réponse d'authentification dans le Guide de l'utilisateur IAM.

Si vous choisissez d'utiliser les paramètres `GetClusterCredentials` facultatifs `DbUser`, `AutoCreate` et `DbGroups`, vous avez deux options. Vous pouvez définir les valeurs des paramètres avec votre connexion JDBC ou ODBC, ou vous pouvez définir les valeurs en ajoutant des éléments d'attribut SAML à votre IdP. Pour plus d'informations sur les paramètres `DbUser`, `AutoCreate` et `DbGroups`, consultez Étape 5 : Configurer une connexion JDBC ou ODBC pour utiliser des informations d'identification IAM.

> **Note**
>
> Si vous utilisez la variable de politique IAM `${redshift:DbUser}`, comme décrit dans Politiques relatives aux ressources pour GetClusterCredentials, la valeur pour `DbUser`

est remplacée par la valeur récupérée par le contexte de demande de l'opération d'API. Les pilotes Amazon Redshift utilisent la valeur de la variable `DbUser` fournie par l'URL de connexion, plutôt que la valeur fournie comme attribut SAML.
Pour sécuriser cette configuration, nous vous recommandons d'utiliser une condition dans une politique IAM pour valider la valeur `DbUser` en utilisant `RoleSessionName`. Vous pouvez trouver des exemples montrant comment définir une condition dans une politique IAM dans Exemple 8 : politique IAM pour l'utilisation GetClusterCredentials.

Pour configurer votre IdP pour définir les paramètres `DbUser`, `AutoCreate` et `DbGroups`, incluez les éléments `Attribute` suivants :

- Un `Attribute` élément dont l'`Name`attribut est défini sur « https://redshift.amazon.com/SAML/Attributes/DbUser »

  Définissez l'élément `AttributeValue` sur le nom d'un utilisateur qui se connectera à la base de données Amazon Redshift.

  La valeur de l'élément `AttributeValue` doit être en minuscules, commencer par une lettre, contenir seulement des caractères alphanumériques, des traits de soulignement ('_'), des signes plus ('+'), des points ('.'), des arobases ('@') ou des tirets ('-') et comporter moins de 128 caractères. Généralement, le nom d'utilisateur et un ID utilisateur (par exemple, bobsmith) ou une adresse e-mail (par exemple bobsmith@example.com). La valeur ne peut pas contenir d'espace (par exemple, un nom complet d'utilisateur comme Bob Smith).

  ```
  <Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbUser">
      <AttributeValue>user-name</AttributeValue>
  </Attribute>
  ```

- Un élément d'attribut dont l'attribut Name est défini sur « https://redshift.amazon.com/SAML/Attributes/AutoCreate »

  Définissez l' AttributeValue élément sur true pour créer un nouvel utilisateur de base de données s'il n'en existe pas. Définissez la valeur AttributeValue sur false pour spécifier que l'utilisateur de la base de données doit exister dans la base de données Amazon Redshift.

  ```
  <Attribute Name="https://redshift.amazon.com/SAML/Attributes/AutoCreate">
      <AttributeValue>true</AttributeValue>
  </Attribute>
  ```

- Un `Attribute` élément dont l'`Name`attribut est défini sur « https://redshift.amazon.com/SAML/Attributes/DbGroups »

  Cet élément contient un ou plusieurs éléments `AttributeValue`. Définissez chaque élément `AttributeValue` sur un nom de groupe de bases de données que `DbUser` rejoint pendant la durée de la séance lorsqu'il se connecte à la base de données Amazon Redshift.

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbGroups">
    <AttributeValue>group1</AttributeValue>
    <AttributeValue>group2</AttributeValue>
    <AttributeValue>group3</AttributeValue>
</Attribute>
```

Étape 3 : créer un rôle IAM avec l'autorisation d'appeler ou GetClusterCredentialsWithIAM GetClusterCredentials

Votre client SQL a besoin d'une autorisation pour appeler l'`GetClusterCredentials`opération `GetClusterCredentialsWithIAM` ou en votre nom. Pour fournir cette autorisation, vous créez un utilisateur ou un rôle et vous attachez une politique qui accorde les autorisations nécessaires. Les deux opérations sont disponibles pour obtenir les informations d'identification du cluster, mais leur méthode d'authentification diffère. `GetClusterCredentialsWithIAM`utilise un rôle IAM, créant automatiquement un utilisateur de base de données qui correspond au rôle, ce qui est utile pour gérer les autorisations au niveau du rôle IAM, tout en `GetClusterCredentials` fournissant des informations d'identification pour un nom d'utilisateur donné dans la base de données.

Pour créer un rôle IAM avec des autorisations d'appel GetClusterCredentialsWithIAM

1. A l'aide du service IAM, créez un utilisateur ou un rôle. Vous pouvez aussi utiliser un utilisateur ou un rôle existant. Par exemple, si vous avez créé un rôle IAM pour l'accès au fournisseur d'identité, vous pouvez attacher les politiques IAM nécessaires à ce rôle.
2. Attachez une politique d'autorisation avec l'autorisation d'appeler l'opération `redshift:GetClusterCredentialsWithIAM`. L'exemple de politique suivant présente les options permettant d'autoriser le fonctionnement d'un cluster et d'une base de données spécifiques, de n'importe quelle base de données d'un cluster et de n'importe quelle base de données d'un cluster.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "SpecificClusterAndDBName",
            "Effect": "Allow",
            "Action": "redshift:GetClusterCredentialsWithIAM",
            "Resource": [
                "arn:aws:redshift:us-east-1:123456789012:dbname:testcluster/
testdatabase"
            ]
        },
        {
            "Sid": "SpecificClusterAndAnyDBName",
            "Effect": "Allow",
            "Action": "redshift:GetClusterCredentialsWithIAM",
            "Resource": "arn:aws:redshift:us-
east-1:123456789012:dbname:examplecluster/*",
        },
        {
            "Sid": "AnyClusterAnyDatabase",
            "Effect": "Allow",
            "Action": "redshift:GetClusterCredentialsWithIAM",
            "Resource": "*"
        }
    ]
}
```

Pour créer un rôle IAM avec des autorisations d'appel GetClusterCredentials

1. A l'aide du service IAM, créez un utilisateur ou un rôle. Vous pouvez aussi utiliser un utilisateur ou un rôle existant. Par exemple, si vous avez créé un rôle IAM pour l'accès au fournisseur d'identité, vous pouvez attacher les politiques IAM nécessaires à ce rôle.
2. Attachez une politique d'autorisation avec l'autorisation d'appeler l'opération `redshift:GetClusterCredentials`. En fonction des paramètres facultatifs que vous spécifiez, vous pouvez aussi autoriser ou restreindre des actions et des ressources supplémentaires dans votre politique :

   - Pour permettre à votre client SQL de récupérer l'ID, AWS la région et le port du cluster, incluez l'autorisation d'appeler l'`redshift:DescribeClusters`opération avec la ressource de cluster Redshift.

- Si vous utilisez l'option `AutoCreate`, incluez l'autorisation d'appeler `redshift:CreateClusterUser` avec la ressource `dbuser`. L'Amazon Resource Name (ARN) suivant spécifie le `dbuser` Amazon Redshift. Remplacez *`regionaccount-id`*, et par *`cluster-name`* les valeurs de votre AWS région, de votre compte et de votre cluster. Pour *`dbuser-name`*, spécifiez le nom d'utilisateur à utiliser pour se connecter à la base de données de cluster.

  ```
  arn:aws:redshift:region:account-id:dbuser:cluster-name/dbuser-name
  ```

- (Facultatif) Ajoutez un ARN qui spécifie la ressource Amazon Redshift `dbname` dans le format suivant. Remplacez *`regionaccount-id`*, et par *`cluster-name`* les valeurs de votre AWS région, de votre compte et de votre cluster. Pour *`database-name`*, spécifiez le nom d'une base de données à laquelle l'utilisateur se connectera.

  ```
  arn:aws:redshift:region:account-id:dbname:cluster-name/database-name
  ```

- Si vous utilisez l'option `DbGroups`, incluez la permission d'appeler l'opération `redshift:JoinGroup` avec la ressource Amazon Redshift `dbgroup` au format suivant. Remplacez *`regionaccount-id`*, et par *`cluster-name`* les valeurs de votre AWS région, de votre compte et de votre cluster. Pour *`dbgroup-name`*, spécifiez le nom d'un groupe d'utilisateurs que l'utilisateur rejoint lors de la connexion.

  ```
  arn:aws:redshift:region:account-id:dbgroup:cluster-name/dbgroup-name
  ```

Pour plus d'informations et d'exemples, consultez Politiques relatives aux ressources pour GetClusterCredentials.

Étape 4 : Créer un utilisateur de base de données et des groupes de bases de données

Vous pouvez aussi créer un utilisateur de base de données que vous utilisez pour vous connecter à la base de données de cluster. Si vous créez des informations d'identification utilisateur temporaires pour un utilisateur existant, vous pouvez désactiver le mot de passe de l'utilisateur pour forcer ce dernier à se connecter à l'aide du mot de passe temporaire. Vous pouvez aussi utiliser l'option `GetClusterCredentials` Autocreate pour créer automatiquement un utilisateur de base de données.

Vous pouvez créer les groupes d'utilisateurs de bases de données avec les autorisations que vous souhaitez que l'utilisateur de base de données IAM rejoigne lors de la connexion. Lorsque vous appelez l'opération `GetClusterCredentials`, vous pouvez spécifier une liste de noms de groupes d'utilisateurs que le nouvel utilisateur rejoint lors de la connexion. Ces appartenances à des groupes sont valides uniquement pour les séances créées avec les informations d'identification générées à l'aide de la demande donnée.

Pour créer un utilisateur de base de données et des groupes de bases de données

1. Connectez-vous à votre base de données Amazon Redshift et créez un utilisateur de base de données en utilisant CREATE USER ou modifiez un utilisateur existant en utilisant ALTER USER.
2. Vous pouvez aussi spécifier l'option PASSWORD DISABLE pour empêcher l'utilisateur d'utiliser un mot de passe. Lorsque le mot de passe d'un utilisateur est désactivé, l'utilisateur peut se connecter uniquement à l'aide d'informations d'identification temporaires. Si le mot de passe n'est pas désactivé, l'utilisateur peut se connecter avec le mot de passe ou à l'aide d'informations d'identification temporaires. Vous ne pouvez pas désactiver le mot de passe d'un super-utilisateur.

   Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec des AWS personnes extérieures au Console de gestion AWS. La manière d'accorder l'accès par programmation dépend du type d'utilisateur qui accède AWS.

   Pour accorder aux utilisateurs un accès programmatique, choisissez l’une des options suivantes.

Quel utilisateur a besoin d’un accès programmatique ?	À	Méthode
IAM	(Recommandé) Utilisez les informations d'identification de la console comme informations d'identification temporaires pour signer les AWS CLI demandes programmatiques adressées aux AWS SDK ou AWS aux API.	Suivez les instructions de l’interface que vous souhaitez utiliser. • Pour cela AWS CLI, consultez la section Connexion pour le développement AWS local dans le Guide de AWS

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
		Command Line Interface l'utilisateur. • Pour les AWS kits de développement, consultez la section Connexion pour le développement AWS local dans le Guide de référence AWS des kits de développement logiciel et des outils.
Identité de la main-d'œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, reportez-vous AWS CLI à la section Configuration de l'utilisation AWS IAM Identity Center dans le Guide de AWS Command Line Interface l'utilisateur. • Pour les AWS kits de développement logiciel, les outils et les AWS API, consultez la section Authentification IAM Identity Center dans le Guide de référence AWS des kits de développement logiciel et des outils.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de la section Utilisation des informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer des demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, consultez la section Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS kits de développement logiciel et les outils, consultez la section Authentification à l'aide d'informations d'identification à long terme dans le Guide de référence AWS des kits de développement logiciel et des outils. • Pour les AWS API, consultez la section Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

L'exemple suivant crée un utilisateur dont le mot de passe est désactivé.

```
create user temp_creds_user password disable;
```

L'exemple suivant désactive le mot de passe pour un utilisateur existant.

```
alter user temp_creds_user password disable;
```

3. Créez des groupes d'utilisateurs de bases de données à l'aide de CREATE GROUP.
4. Utilisez la commande GRANT pour définir les privilèges d'accès pour les groupes.

Étape 5 : Configurer une connexion JDBC ou ODBC pour utiliser des informations d'identification IAM

Vous pouvez configurer votre client SQL avec un pilote Amazon Redshift JDBC ou ODBC. Ce pilote gère le processus de création des informations d'identification de l'utilisateur de la base de données et l'établissement d'une connexion entre votre client SQL et votre base de données Amazon Redshift.

Si vous utilisez un fournisseur d'identité pour l'authentification, spécifiez le nom d'un plugin de fournisseur d'informations d'identification. Les pilotes JDBC et ODBC Amazon Redshift incluent des plug-ins pour les fournisseurs d'identité suivants : SAML-based

- Active Directory Federation Services (AD FS)
- PingOne
- Okta
- Microsoft Azure AD

  Pour savoir comment configurer Microsoft Azure AD en tant que fournisseur d'identité, consultez Configuration de l’authentification unique JDBC ou ODBC.

Pour configurer une connexion JDBC pour utiliser des informations d'identification IAM

1. Téléchargez la dernière version du pilote JDBC d'Amazon Redshift depuis la page Configuration d’une connexion pour la version 2.x du pilote JDBC pour Amazon Redshift.
2. Créez une URL JDBC avec les options d'informations d'identification IAM dans un des formats suivants. Pour utiliser l'authentification IAM, ajoutez `iam:` à l'URL Amazon Redshift JDBC après `jdbc:redshift:`, comme indiqué dans l'exemple suivant.

   ```
   jdbc:redshift:iam://
   ```

   Ajoutez `cluster-name`, `region` et `account-id`. Le pilote JDBC utilise les informations de votre compte IAM et le nom du cluster pour récupérer l'ID et la région du cluster.

AWS Pour ce faire, votre utilisateur ou rôle doit être autorisé à appeler l'opération `redshift:DescribeClusters` avec le cluster spécifié. Si votre utilisateur ou votre rôle n'est pas autorisé à appeler l'`redshift:DescribeClusters`opération, incluez l'ID du cluster, AWS la région et le port, comme indiqué dans l'exemple suivant. Le numéro de port est facultatif.

```
jdbc:redshift:iam://examplecluster.abc123xyz789.us-
west-2.redshift.amazonaws.com:5439/dev
```

3. Ajoutez des options JDBC pour fournir des informations d'identification IAM. Vous utilisez différentes combinaisons d'options JDBC pour fournir des informations d'identification IAM. Pour en savoir plus, consultez Options JDBC et ODBC pour la création d'informations d'identification de l'utilisateur de base de données.

   L'URL suivante indique l' AccessKeyidentifiant et SecretAccessKey le nom d'un utilisateur.

   ```
   jdbc:redshift:iam://examplecluster:us-west-2/dev?
   AccessKeyID=AKIAIOSFODNN7EXAMPLE&SecretAccessKey=wJalrXUtnFEMI/K7MDENG/
   bPxRfiCYEXAMPLEKEY
   ```

   L'exemple suivant spécifie un profil nommé qui contient les informations d'identification IAM.

   ```
   jdbc:redshift:iam://examplecluster:us-west-2/dev?Profile=user2
   ```

4. Ajoutez les options JDBC que le pilote JDBC utilise pour appeler l'opération d'API `GetClusterCredentials`. N'incluez pas ces options si vous appelez l'opération d'API `GetClusterCredentials` par programmation.

   L'exemple suivant inclut les options JDBC `GetClusterCredentials`.

   ```
   jdbc:redshift:iam://examplecluster:us-west-2/dev?
   plugin_name=com.amazon.redshift.plugin.AzureCredentialsProvider&UID=user&PWD=password&idp_t
   ```

Pour configurer une connexion ODBC pour utiliser des informations d'identification IAM

Dans la procédure suivante, vous pouvez rechercher uniquement les étapes de configuration de l'authentification IAM. Pour connaître les étapes permettant d'utiliser l'authentification standard, avec un nom d'utilisateur de base de données et un mot de passe, consultez Configuration d'une connexion pour le pilote ODBC version 2.x pour Amazon Redshift.

1. Installez et configurez le dernier pilote OBDC Amazon Redshift pour votre système d'exploitation. Pour plus d'informations, consultez Configuration d'une connexion pour le pilote ODBC version 2.x pour Amazon Redshift.

   > **Important**
   >
   > La version du pilote ODBC Amazon Redshift doit être 1.3.6.1000 ou une version ultérieure.

2. Suivez les étapes pour votre système d'exploitation afin de configurer les paramètres de connexion.
3. Sur les systèmes d'exploitation Microsoft Windows, accédez à la fenêtre de configuration DNS du pilote ODBC Amazon Redshift.

   a. Sous Paramètres de connexion, saisissez les informations suivantes :

      - Nom de la source de données
      - Server (Serveur) (facultatif)
      - Port (facultatif)
      - Base de données

      Si votre utilisateur ou rôle est autorisé à appeler l'opération `redshift:DescribeClusters`, seuls le nom de la source de données et la base de données sont requis. Amazon Redshift utilise ClusterId une région pour obtenir le serveur et le port en appelant l'`DescribeCluster`opération.

      Si votre utilisateur ou rôle n'a pas l'autorisation d'appeler l'opération `redshift:DescribeClusters`, spécifiez Serveur et Port.

   b. Sous Authentication (Authentification), choisissez une valeur pour Auth Type (Type d'authentification).

      Pour chaque type d'authentification, entrez les valeurs suivantes :

      AWS Profile

      Entrez les informations suivantes :

      - ClusterID

- Région
- Profile name (Nom de profil)

  Entrez le nom d'un profil dans un fichier de AWS configuration contenant les valeurs des options de connexion ODBC. Pour de plus amples informations, veuillez consulter Utilisation d’un profil de configuration.

(Facultatif) Fournissez des détails sur les options que le pilote ODBC utilise pour appeler l'opération d'API `GetClusterCredentials` :

- DbUser
- Utilisateur AutoCreate
- DbGroups

  Pour de plus amples informations, veuillez consulter Options JDBC et ODBC pour la création d’informations d’identification de l’utilisateur de base de données.

Informations d’identification IAM

Entrez les informations suivantes :

- ClusterID
- Région
- AccessKeyID et SecretAccessKey

  ID de clé d'accès et clé d'accès secrète pour le rôle IAM ou l'utilisateur configurées pour l'authentification de base de données IAM.
- SessionToken

  SessionTokenest obligatoire pour un rôle IAM avec des informations d'identification temporaires. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires.

Fournissez des détails sur les options que le pilote ODBC utilise pour appeler l'opération d'API `GetClusterCredentials` :

- DbUser (obligatoire)
- Utilisateur AutoCreate (facultatif)
- DbGroups (facultatif)

Pour de plus amples informations, veuillez consulter Options JDBC et ODBC pour la création d'informations d'identification de l'utilisateur de base de données.

Identity Provider (Fournisseur d'identité) : AD FS

Pour l'authentification Windows intégrée avec AD FS, laissez User (Utilisateur) et Password (Mot de passe) vides.

Fournissez les détails sur l'IdP :

- IdP Host (Hôte IdP)

  Nom de l'hôte du fournisseur d'identité d'entreprise. Ce nom ne doit pas inclure de barre oblique (/).

- IdP Port (Port IdP) (facultatif)

  Port utilisé par le fournisseur d'identité. La valeur par défaut est 443.

- Preferred Role (Rôle préféré)

  Un Amazon Resource Name (ARN) pour le rôle IAM provenant des éléments `AttributeValue` pour l'attribut `Role` dans l'assertion SAML. Collaborez avec votre administrateur IdP pour rechercher la valeur appropriée pour le rôle préféré. Pour plus d'informations, consultez Étape 2 : Configurer des assertions SAML pour votre IdP.

(Facultatif) Fournissez des détails sur les options que le pilote ODBC utilise pour appeler l'opération d'API `GetClusterCredentials` :

- DbUser
- Utilisateur AutoCreate
- DbGroups

Pour de plus amples informations, veuillez consulter Options JDBC et ODBC pour la création d'informations d'identification de l'utilisateur de base de données.

Fournisseur d'identité : PingFederate

Pour User (Utilisateur) et Password (Mot de passe), entrez le nom d'utilisateur et le mot de passe de votre IdP.

Fournissez les détails sur l'IdP :

- IdP Host (Hôte IdP)

  Nom de l'hôte du fournisseur d'identité d'entreprise. Ce nom ne doit pas inclure de barre oblique (/).

- IdP Port (Port IdP) (facultatif)

  Port utilisé par le fournisseur d'identité. La valeur par défaut est 443.

- Preferred Role (Rôle préféré)

  Un Amazon Resource Name (ARN) pour le rôle IAM provenant des éléments `AttributeValue` pour l'attribut `Role` dans l'assertion SAML. Collaborez avec votre administrateur IdP pour rechercher la valeur appropriée pour le rôle préféré. Pour plus d'informations, consultez Étape 2 : Configurer des assertions SAML pour votre IdP.

(Facultatif) Fournissez des détails sur les options que le pilote ODBC utilise pour appeler l'opération d'API `GetClusterCredentials` :

- DbUser
- Utilisateur AutoCreate
- DbGroups

Pour de plus amples informations, veuillez consulter Options JDBC et ODBC pour la création d'informations d'identification de l'utilisateur de base de données.

Identity Provider (Fournisseur d'identité) : Okta

Pour User (Utilisateur) et Password (Mot de passe), entrez le nom d'utilisateur et le mot de passe de votre IdP.

Fournissez les détails sur l'IdP :

- IdP Host (Hôte IdP)

  Nom de l'hôte du fournisseur d'identité d'entreprise. Ce nom ne doit pas inclure de barre oblique (/).

- IdP Port (Port IdP)

  Cette valeur n'est pas utilisée par Okta.

- Preferred Role (Rôle préféré)

  Un Amazon Resource Name (ARN) pour le rôle IAM provenant des éléments `AttributeValue` pour l'attribut `Role` dans l'assertion SAML. Collaborez avec votre administrateur IdP pour rechercher la valeur appropriée pour le rôle préféré. Pour plus d'informations, consultez Étape 2 : Configurer des assertions SAML pour votre IdP.

- Okta App ID (ID de l'application Okta)

  ID d'une application Okta. La valeur de l'ID d'application suit "amazon_aws" dans le lien intégré de l'application Okta. Collaborez avec votre administrateur IdP pour obtenir cette valeur.

(Facultatif) Fournissez des détails sur les options que le pilote ODBC utilise pour appeler l'opération d'API `GetClusterCredentials` :

- DbUser
- Utilisateur AutoCreate
- DbGroups

Pour de plus amples informations, veuillez consulter Options JDBC et ODBC pour la création d'informations d'identification de l'utilisateur de base de données.

Fournisseur d'identité : Azure AD

Pour User (Utilisateur) et Password (Mot de passe), entrez le nom d'utilisateur et le mot de passe de votre IdP.

Pour Cluster ID (ID de cluster) et Region (Région), entrez l'ID de cluster et la région AWS de votre cluster Amazon Redshift.

Pour Database (Base de données), entrez la base de données que vous avez créée pour votre cluster Amazon Redshift.

Fournissez les détails sur l'IdP :

- IdP Tenant (Locataire IdP)

  Le locataire utilisé pour Azure AD.

- Azure Client Secret (Secret client Azure)

Le secret client de l'application d'entreprise Amazon Redshift dans Azure.

- Azure Client ID (ID client Azure)

  L'ID du client (ID de l'application) de l'application d'entreprise Amazon Redshift dans Azure.

(Facultatif) Fournissez des détails sur les options que le pilote ODBC utilise pour appeler l'opération d'API `GetClusterCredentials` :

- DbUser
- Utilisateur AutoCreate
- DbGroups

Pour de plus amples informations, veuillez consulter Options JDBC et ODBC pour la création d'informations d'identification de l'utilisateur de base de données.

Options visant à fournir des informations d'identification IAM

Pour fournir des informations d'identification IAM pour une connexion JDBC ou ODBC, choisissez une des options suivantes.

- AWS profile

  Au lieu de saisir les valeurs d'informations d'identification sous la forme de paramètres JDBC ou ODBC, vous pouvez inclure les valeurs dans un profil nommé. Pour plus d'informations, consultez Utilisation d'un profil de configuration.

- Informations d'identification IAM

  Fournissez des valeurs pour AccessKey ID et SecretAccessKey, éventuellement, SessionToken sous la forme de paramètres JDBC ou ODBC. SessionToken n'est requis que pour un rôle IAM avec des informations d'identification temporaires. Pour de plus amples informations, veuillez consulter Options JDBC et ODBC visant à fournir des informations d'identification IAM.

- Fédération du fournisseur d'identité

  Lorsque vous utilisez la fédération de fournisseurs d'identité pour permettre aux utilisateurs d'un fournisseur d'identité de s'authentifier auprès d'Amazon Redshift, spécifiez le nom d'un plugin de fournisseur d'informations d'identification. Pour de plus amples informations, veuillez consulter Plug-in de fournisseur d'informations.

Les pilotes JDBC et ODBC Amazon Redshift incluent des plug-ins pour les fournisseurs d'informations d'identification de fédération SAML-based d'identité suivants :

- Microsoft Active Identity Federation Services (AD FS)
- PingOne
- Okta
- Microsoft Azure Active Directory (Azure AD)

Vous pouvez fournir le nom de plugin et les valeurs associées sous la forme de paramètres JDBC ou ODBC ou en utilisant un profil. Pour plus d'informations, consultez Options de configuration du pilote JDBC version 2.x.

Pour plus d'informations, consultez Étape 5 : Configurer une connexion JDBC ou ODBC pour utiliser des informations d'identification IAM.

Utilisation d'un profil de configuration

Vous pouvez fournir les options et `GetClusterCredentials` options d'identification IAM sous forme de paramètres dans les profils nommés de votre fichier AWS de configuration. Fournissez le nom de profil, utilisez l'option Profil JDBC. La configuration est stockée dans un fichier nommé `config` ou un fichier nommé `credentials` dans un dossier nommé `.aws` dans votre répertoire personnel.

Pour un plug-in de fournisseur SAML-based d'informations d'identification inclus dans un pilote JDBC ou ODBC Amazon Redshift, vous pouvez utiliser les paramètres décrits ci-dessus dans. Plug-in de fournisseur d'informations Si `plugin_name` n'est pas utilisé, les autres options sont ignorées.

L'exemple suivant montre le ~/. aws/credentials fichier avec deux profils.

```
[default]
aws_access_key_id=AKIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

[user2]
aws_access_key_id=AKIAI44QH8DHBEXAMPLE
aws_secret_access_key=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
session_token=AQoDYXdzEPT//////////
wEXAMPLEtc764bNrC9SAPBSM22wDOk4x4HIZ8j4FZTwdQWLWsKWHGBuFqwAeMicRXmxfpSPfIeoIYRqTflfKD8YUuwthAx7
qkPpKPi/kMcGd
QrmGdeehM4IC1NtBmUpp2wUE8phUZampKsburEDy0KPkyQDYwT7WZ0wq5VSXDvp75YU
```

```
9HFvlRd8Tx6q6fE8YQcHNVXAkiY9q6d+xo0rKwT38xVqr7ZD0u0iPPkUL64lIZbqBAz
+scqKmlzm8FDrypNC9Yjc8fPOLn9FX9KSYvKTr4rvx3iSIlTJabIQwj2ICCR/oLxBA==
```

Pour utiliser les informations d'identification pour l'exemple `user2`, spécifiez `Profile=user2` dans l'URL JDBC.

Pour plus d'informations sur l'utilisation des profils, consultez la section Configuration et paramètres des fichiers d'identification dans le Guide de l' AWS Command Line Interface utilisateur.

Pour plus d'informations sur l'utilisation des profils pour le pilote JDBC, consultez Spécification des profils.

Pour plus d'informations sur l'utilisation des profils pour le pilote ODBC, consultez Méthodes d’authentification.

Options JDBC et ODBC visant à fournir des informations d’identification IAM

Le tableau suivant répertorie les Options JDBC et ODBC visant à fournir des informations d'identification IAM.

Option	Description
`Iam`	A utiliser uniquement dans une chaîne de connexion ODBC. Définissez cette valeur sur 1 pour utiliser l'authentification IAM.

`AccessKeyID`
 	
`SecretAccessKey`
 	
`SessionToken`
	ID de clé d'accès et clé d'accès secrète pour le rôle IAM ou l'utilisateur configuré pour l'authentification de la base de données IAM. `SessionToken` n'est requis que pour un rôle IAM avec des informations d'identification temporaires. SessionToken n'est pas utilisé pour un utilisateur. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires.

`plugin_name`	Nom complet d'une classe qui implémente un fournisseur d'informations d'identification. Le pilote JDBC Amazon Redshift inclut des plug-ins de fournisseur SAML-based d'informations d'identification. Si vous fournissez `plugin_name` , vous pouvez également fournir d'autres options connexes. Pour de plus amples informations, veuillez consulter Plug-in de fournisseur d’informations.

Option	Description
`Profile`	Le nom d'un profil dans un fichier d' AWS informations d'identification ou de configuration contenant des valeurs pour les options de connexion JDBC. Pour de plus amples informations, veuillez consulter Utilisation d’un profil de configuration.

Options JDBC et ODBC pour la création d’informations d’identification de l’utilisateur de base de données

Pour utiliser le pilote JDBC ou ODBC Amazon Redshift pour créer des informations d'identification de l'utilisateur de base de données, fournissez le nom de l'utilisateur de la base de données en tant qu'option JDBC ou ODBC. Vous pouvez aussi faire en sorte que le pilote crée un nouvel utilisateur de base de données s'il n'en existe pas, et vous pouvez spécifier une liste de groupes d'utilisateurs de bases de données que l'utilisateur rejoint lors de la connexion.

Si vous utilisez un fournisseur d'identité (IdP), collaborez avec votre administrateur IdP pour déterminer les valeurs correctes pour ces options. Votre administrateur IdP peut aussi configurer votre IdP pour fournir ces options, auquel cas il n'est pas nécessaire que vous les fournissiez en tant qu'options JDBC ou ODBC. Pour plus d’informations, consultez Étape 2 : Configurer des assertions SAML pour votre IdP.

> **Note**
>
> Si vous utilisez la variable de politique IAM `${redshift:DbUser}`, comme décrit dans Politiques relatives aux ressources pour GetClusterCredentials, la valeur pour `DbUser` est remplacée par la valeur récupérée par le contexte de demande de l'opération d'API. Les pilotes Amazon Redshift utilisent la valeur de la variable `DbUser` fournie par l'URL de connexion, plutôt que la valeur fournie comme attribut SAML.
> Pour sécuriser cette configuration, nous vous recommandons d'utiliser une condition dans une politique IAM pour valider la valeur `DbUser` avec le `RoleSessionName`. Vous pouvez trouver des exemples montrant comment définir une condition dans une politique IAM dans Exemple 8 : politique IAM pour l'utilisation GetClusterCredentials.

Le tableau suivant répertorie les options à utiliser la création d'informations d'identification de l'utilisateur de base de données.

Option	Description
DbUser	Nom d'un utilisateur de la base de données. Si un utilisateur nommé DbUser existe dans la base de données, les informations d'identification temporaires disposent des mêmes autorisations que l'utilisateur existant. S'il DbUser n'existe pas dans la base de données et AutoCreate s'il est vrai, un nouvel utilisateur nommé DbUser est créé. Vous pouvez aussi désactiver le mot de passe d'un utilisateur existant. Pour plus d'informations, consultez ALTER_USER
AutoCreate	Spécifiez `true` de créer un utilisateur de base de données avec le nom spécifié DbUser s'il n'en existe pas. La valeur par défaut est false.
`DbGroups`	Liste séparée par des virgules des noms d'un ou plusieurs groupes de bases de données existants que l'utilisateur de la base de données rejoint pour la séance en cours. Par défaut, le nouvel utilisateur est ajouté uniquement à PUBLIC.

Plug-in de fournisseur d’informations

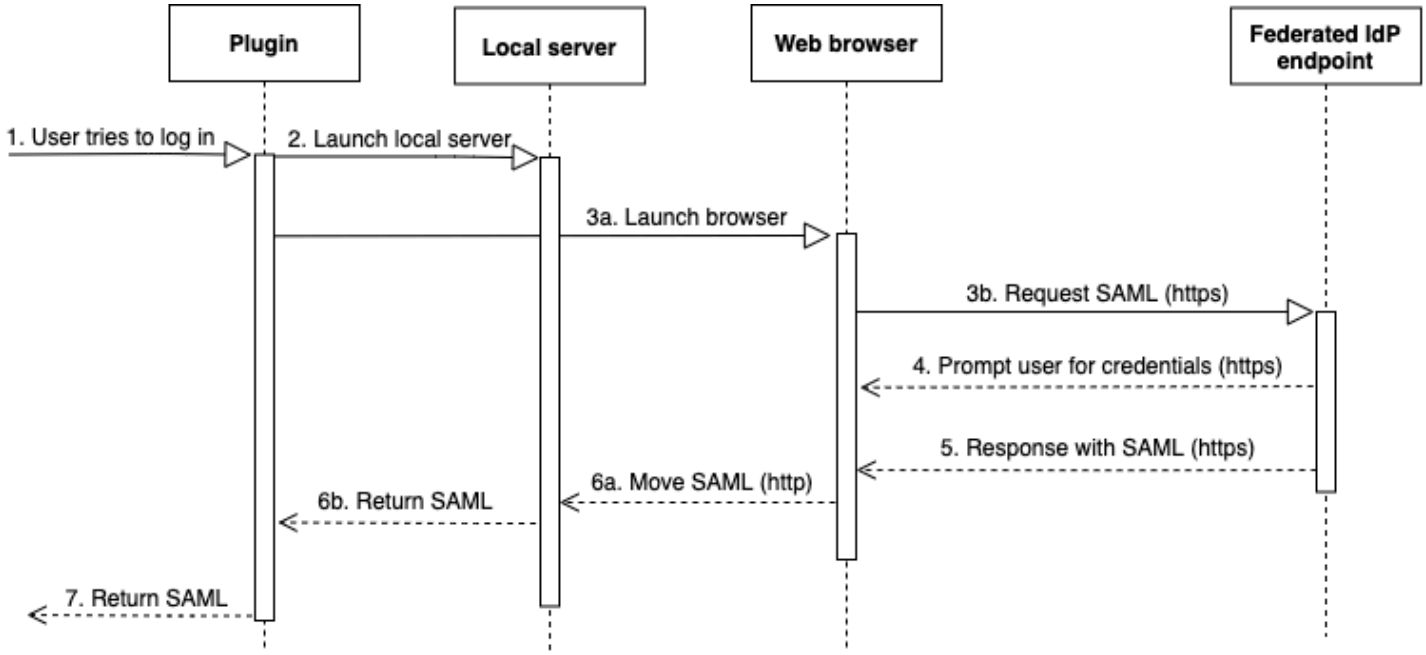
Amazon Redshift utilise des plugins de fournisseur d'informations d'identification pour l'authentification unique.

Pour prendre en charge l'authentification unique, Amazon Redshift fournit le plugin Azure AD pour Microsoft Azure Active Directory. Pour plus d'informations sur la configuration de ce plugin, consultez Configuration de l’authentification unique JDBC ou ODBC.

Multi-factor authentication
Multi-factor authentication

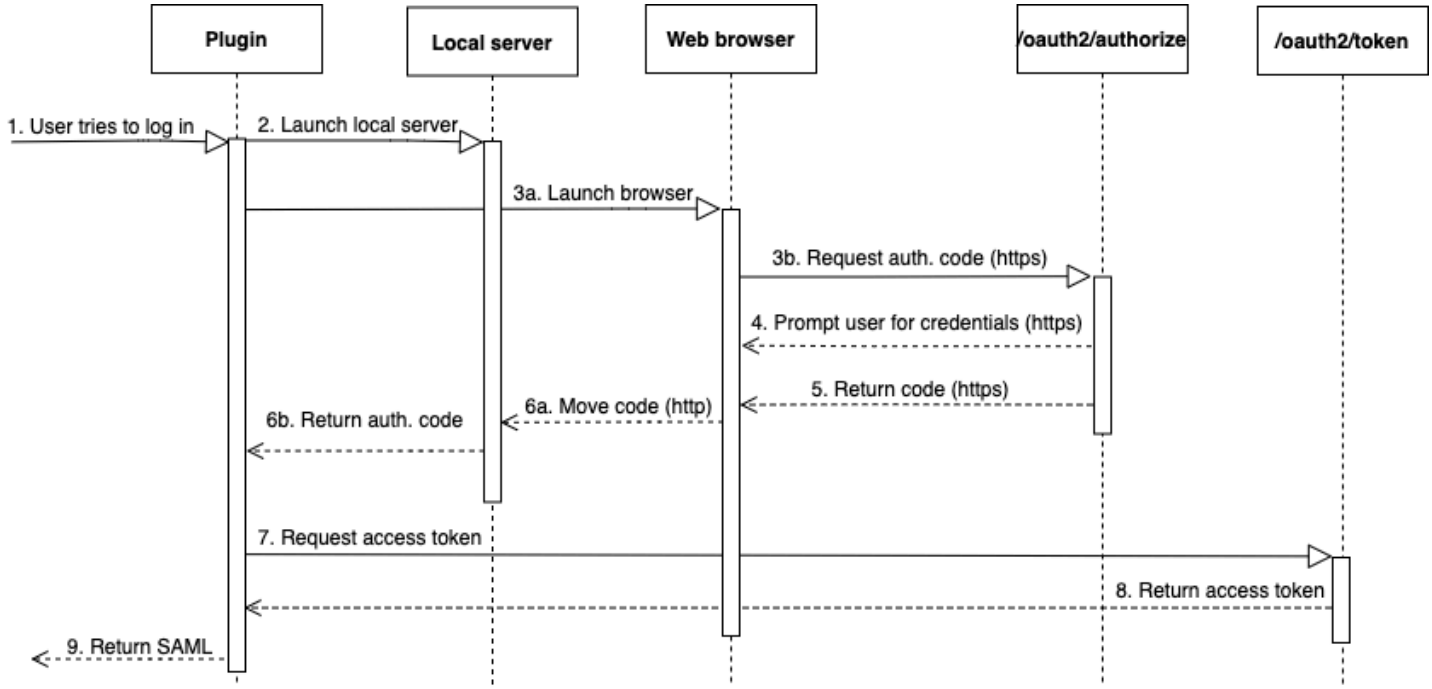
Pour prendre en charge l'authentification multifacteur (MFA), Amazon Redshift fournit des plugins basés sur un navigateur. Utilisez le plug-in SAML du navigateur pour Okta et PingOne le plug-in Azure AD du navigateur pour Microsoft Azure Active Directory.

Avec le plugin SAML du navigateur, l’authentification OAuth s’effectue comme ceci :



1. Un utilisateur essaie de se connecter.
2. Le plugin lance un serveur local pour écouter les connexions entrantes sur le localhost.
3. Le plugin lance un navigateur Web pour demander une réponse SAML via HTTPS à partir du point de terminaison du fournisseur d'identité fédérée d'URL de connexion par authentification unique spécifié.
4. Le navigateur web suit le lien et invite l'utilisateur à entrer des informations d'identification.
5. Une fois que l'utilisateur s'authentifie et accorde son consentement, le point de terminaison du fournisseur d'identité fédérée renvoie une réponse SAML sur HTTPS à l'URI indiqué par `redirect_uri`.
6. Le navigateur web déplace le message de réponse avec la réponse SAML au `redirect_uri` indiqué.
7. Le serveur local accepte la connexion entrante et le plugin récupère la réponse SAML et la transmet à Amazon Redshift.

Avec le plugin Azure AD du navigateur, l'authentification SAML s'effectue comme suit :



1. Un utilisateur essaie de se connecter.
2. Le plugin lance un serveur local pour écouter les connexions entrantes sur le localhost.
3. Le plugin lance un navigateur web pour demander un code d'autorisation à partir du point de terminaison `oauth2/authorize` Azure AD.
4. Le navigateur web suit le lien généré via HTTPS et invite l'utilisateur à entrer des informations d'identification. Le lien est généré à l'aide des propriétés de configuration, telles que le locataire et client_id.
5. Une fois que l'utilisateur s'est authentifié et a accordé son consentement, le point de terminaison `oauth2/authorize` Azure AD est renvoyé et envoie une réponse via HTTPS avec le code d'autorisation au `redirect_uri` indiqué.
6. Le navigateur web déplace le message de réponse avec la réponse SAML au `redirect_uri` indiqué.
7. Le serveur local accepte la connexion entrante et le plugin demande et récupère le code d'autorisation et envoie une requête POST au point de terminaison `oauth2/token` Azure AD.
8. Le point de terminaison `oauth2/token` Azure AD renvoie une réponse avec un jeton d'accès au `redirect_uri` indiqué.
9. Le plugin récupère la réponse SAML et la transmet à Amazon Redshift.

Examinez les sections suivantes :

- Active Directory Federation Services (AD FS)

  Pour de plus amples informations, veuillez consulter Configuration de l’authentification unique JDBC ou ODBC.
- PingOne (Ping)

  Le ping n'est pris en charge qu'avec l'adaptateur PingOne IdP prédéterminé utilisant l'authentification par formulaires.

  Pour de plus amples informations, veuillez consulter Configuration de l’authentification unique JDBC ou ODBC.
- Okta

  Okta n'est pris en charge que pour l' Okta-supplied application utilisée avec le Console de gestion AWS.

  Pour de plus amples informations, veuillez consulter Configuration de l’authentification unique JDBC ou ODBC.
- Microsoft Azure Active Directory (Azure AD)

  Pour plus d’informations, consultez Configuration de l’authentification unique JDBC ou ODBC.

Options de plug-in
Options de plug-in

Pour utiliser un plug-in de fournisseur SAML-based d'informations d'identification, spécifiez les options suivantes à l'aide des options JDBC ou ODBC ou dans un profil nommé. Si `plugin_name` n'est pas spécifié, les autres options sont ignorées.

Option	Description
`plugin_name`	Pour JDBC, nom de classe qui implémente un fournisseur d'informations d'identification. Spécifiez l’un des éléments suivants : • Pour Active Directory Federation Services `com.amazon.redshift.plugin.AdfsCredentialsProvider` • Pour Okta

Option	Description

	`com.amazon.redshift.plugin.OktaCredentialsProvider`
	• Pour PingFederate
	`com.amazon.redshift.plugin.PingCredentialsProvider`
	• Pour Microsoft Azure Active Directory
	`com.amazon.redshift.plugin.AzureCredentialsProvider`
	• Pour SAML MFA
	`com.amazon.redshift.plugin.BrowserSamlCredentialsProvider`
	• Pour une authentification unique Microsoft Azure Active Directory avec MFA
	`com.amazon.redshift.plugin.BrowserAzureCredentialsProvider`
	
	Pour ODBC, spécifiez l'un des éléments suivants :
	• Pour Active Directory Federation Services : `adfs`
	• Pour Okta : `okta`
	• Pour PingFederate : `ping`
	• Pour Microsoft Azure Active Directory : `azure`
	• Pour MFA SAML : `browser saml`
	• Pour une authentification unique Microsoft Azure Active Directory avec MFA : `browser azure ad`

`idp_host`	Nom de l'hôte du fournisseur d'identité d'entreprise. Ce nom ne doit pas inclure de barre oblique ('/'). Pour un fournisseur d'identité Okta, la valeur pour `idp_host` doit se terminer par `.okta.com` .
`idp_port`	Port utilisé par le fournisseur d'identité. La valeur par défaut est 443. Ce port est ignoré pour Okta.

Option	Description
`preferred_role`	Amazon Resource Name (ARN) du rôle provenant des éléments `AttributeValue` pour l'attribut `Role` dans l'assertion SAML. Collaborez avec votre administrateur IdP pour rechercher la valeur appropriée pour le rôle préféré. Pour plus d'informations, consultez Étape 2 : Configurer des assertions SAML pour votre IdP.
`user`	nom d'utilisateur d'entreprise, incluant le domaine, le cas échéant. Par exemple, pour Active Directory, le nom de domaine au format domaine\nom d'utilisateur est requis.
mot de passe	Mot de passe de l'utilisateur d'entreprise. Nous vous recommandons de ne pas utiliser cette option. A la place, utilisez votre client SQL pour fournir le mot de passe.
`app_id`	ID d'une application Okta. Utilisé uniquement avec Okta. La valeur de `app_id` suit `amazon_aws` dans le lien intégré de l'application Okta. Collaborez avec votre administrateur IdP pour obtenir cette valeur. Voici un exemple de lien intégré d'application : `https://example.okta.com/home/amazon_aws/0oa2hylwrpM8UGehd1t7/272`
`idp_tenant`	Locataire utilisé pour Azure AD. Utilisé uniquement avec Azure.
`client_id`	ID client de l'application métier Amazon Redshift dans Azure AD. Utilisé uniquement avec Azure.

Génération d'informations d'identification de base de données pour une identité IAM à l'aide de la CLI ou de l'API d'Amazon Redshift

Pour générer par programmation des informations d'identification utilisateur de base de données temporaires, Amazon Redshift fournit la commande get-cluster-credentials pour l'opération () et l'API. AWS Command Line Interface AWS CLI GetClusterCredentials Ou vous pouvez configurer votre client SQL avec les pilotes Amazon Redshift JDBC ou ODBC qui gèrent le processus d'appel de l'opération `GetClusterCredentials`, la récupération des informations d'identification de l'utilisateur de la base de données et l'établissement d'une connexion entre votre client SQL et votre base de données Amazon Redshift. Pour plus d'informations, consultez Options JDBC et ODBC pour la création d'informations d'identification de l'utilisateur de base de données.

> **Note**
>
> Nous vous recommandons d'utiliser les pilotes JDBC ou ODBC d'Amazon Redshift pour générer les informations d'identification des utilisateurs de la base de données.

Dans cette section, vous trouverez des étapes concernant l'appel par programmation de l'opération `GetClusterCredentials` ou de la commande or get-cluster-credentials, la récupération des informations d'identification de l'utilisateur de base de données et la connexion à la base de données.

Pour générer et utiliser des informations d'identification temporaires de base de données

1. Créez ou modifiez un utilisateur ou un rôle avec les autorisations requises. Pour plus d'informations sur les autorisations IAM, consultez Étape 3 : créer un rôle IAM avec l'autorisation d'appeler ou GetClusterCredentialsWithIAM GetClusterCredentials.
2. En tant qu'utilisateur ou rôle que vous avez autorisé à l'étape précédente, exécutez la commande de la CLI get-cluster-credentials ou appelez l'opération d'API `GetClusterCredentials`, puis fournissez les valeurs suivantes :
   - Identifiant du cluster – Le nom du cluster qui contient la base de données.
   - Nom d'utilisateur de la base de données – Le nom d'un utilisateur de base de données, existant ou nouveau.
     - Si l'utilisateur n'existe pas dans la base de données et AutoCreate que c'est vrai, un nouvel utilisateur est créé avec le MOT DE PASSE désactivé.
     - Si l'utilisateur n'existe pas et AutoCreate qu'il est faux, la demande échoue.
     - Pour cet exemple, le nom de l'utilisateur de la base de données est `temp_creds_user`.
   - Autocreate – (Facultatif) Créez un utilisateur si le nom de l'utilisateur de la base de données n'existe pas.
   - Nom de base de données – (Facultatif) Le nom de la base de données à laquelle l'utilisateur est autorisé à se connecter. Si aucun nom de base de données n'est spécifié, l'utilisateur peut se connecter à n'importe quelle base de données de cluster.
   - Groupes de bases de données – (Facultatif) Une liste des groupes d'utilisateurs de bases de données existants. Lorsque la connexion réussit, l'utilisateur de base de données est ajouté aux groupes d'utilisateurs spécifiés. Si aucun groupe n'est spécifié, l'utilisateur dispose uniquement des autorisations PUBLIC. Les noms de groupe d'utilisateurs doivent

correspondre aux ARN de ressources dbgroup spécifiés dans la politique IAM attachée à l'utilisateur ou au rôle.

- Durée d'expiration – (Facultatif) La durée, en secondes, après laquelle les informations d'identification temporaires expirent. Vous pouvez spécifier une valeur comprise entre 900 secondes (15 minutes) et 3 600 secondes (60 minutes). Le durée par défaut est 900 secondes.

3. Amazon Redshift vérifie que l'utilisateur dispose de l'autorisation pour appeler l'opération `GetClusterCredentials` avec les ressources spécifiées.
4. Amazon Redshift renvoie un mot de passe temporaire et le nom de l'utilisateur de la base de données.

   L'exemple suivant utilise Amazon Redshift CLI pour générer des informations d'identification temporaires de base de données pour un utilisateur existant nommé `temp_creds_user`.

```
aws redshift get-cluster-credentials --cluster-identifier examplecluster --db-user
 temp_creds_user --db-name exampledb --duration-seconds 3600
```

   Le résultat est le suivant.

```
{
  "DbUser": "IAM:temp_creds_user",
  "Expiration": "2016-12-08T21:12:53Z",
  "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM8OyxpDHwXVPyJYBDm/
gqX2Eeaq6P3DgTzgPg=="
}
```

   L'exemple suivant utilise Amazon Redshift CLI avec autocreate pour générer des informations d'identification temporaires de base de données pour un nouvel utilisateur et l'ajouter au groupe `example_group`.

```
aws redshift get-cluster-credentials --cluster-identifier examplecluster --db-user
 temp_creds_user --auto-create --db-name exampledb --db-groups example_group --
duration-seconds 3600
```

   Le résultat est le suivant.

```
{
  "DbUser": "IAMA:temp_creds_user:example_group",
```

```
  "Expiration": "2016-12-08T21:12:53Z",
  "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM8OyxpDHwXVPyJYBDm/
gqX2Eeaq6P3DgTzgPg=="
}
```

5. Établissez une connexion avec authentification SSL (Secure Socket Layer) avec le cluster Amazon Redshift et envoyez une demande de connexion avec le nom d'utilisateur et le mot de passe fournis par la réponse `GetClusterCredentials`. Incluez le préfixe `IAM:` ou `IAMA:` avec le nom d'utilisateur, par exemple, `IAM:temp_creds_user` ou `IAMA:temp_creds_user`.

   > **Important**
   >
   > Configurez votre client SQL pour exiger SSL. Sinon, si votre client SQL tente automatiquement de se connecter avec SSL, il peut utiliser à nouveau une connexion non-SSL en cas d'échec. Dans ce cas, la première tentative de connexion peut échouer parce que les informations d'identification ont expiré ou ne sont pas valides, et une seconde tentative de connexion peut échouer parce que la connexion n'est pas de type SSL. Si cela se produit, le premier message d'erreur peut être manqué. Pour plus d'informations sur la connexion à votre cluster à l'aide de SSL, consultez Configuration des options de sécurité des connexions.

6. Si la connexion n'utilise pas SSL, la tentative de connexion échoue.
7. Le cluster envoie une demande `authentication` au client SQL.
8. Le client SQL envoie le mot de passe temporaire au cluster.
9. Si le mot de passe est valide et n'a pas expiré, le cluster établit la connexion.

Configuration de l’authentification unique JDBC ou ODBC

Vous pouvez tirer parti de fournisseurs d'identité externes (IdPs) pour authentifier et autoriser les utilisateurs accédant à votre cluster Amazon Redshift, simplifiant ainsi la gestion des utilisateurs et renforçant la sécurité. Cela permet une gestion centralisée des utilisateurs, un contrôle d’accès basé sur les rôles et des fonctionnalités d’audit sur plusieurs services. Les cas d’utilisation courants incluent la rationalisation de l’authentification pour différents groupes d’utilisateurs, l’application de stratégies d’accès cohérentes et le respect des exigences réglementaires.

Les pages suivantes vous guident dans la configuration de l’intégration d’IdP avec votre cluster Redshift. Pour plus d'informations sur la configuration AWS en tant que fournisseur de services pour

l'IdP, consultez Configuration de votre IdP SAML 2.0 avec Relying Party Trust et Adding Claims dans le guide de l'utilisateur IAM.

AD FS

Ce didacticiel vous montre comment vous pouvez utiliser AD FS en tant que fournisseur d'identité (IdP) pour accéder à votre cluster Amazon Redshift.

Étape 1 : configurer AD FS et votre AWS compte pour se faire confiance

La procédure suivante explique comment configurer une relation d'approbation.

1. Créez ou utilisez un cluster Amazon Redshift existant pour que vos utilisateurs AD FS puissent se connecter. Pour configurer la connexion, certaines propriétés de ce cluster sont nécessaires, telles que l'identifiant de cluster. Pour de plus amples informations, veuillez consulter Création d'un cluster.
2. Configurez AD FS pour contrôler l'accès à Amazon Redshift sur la Console de gestion Microsoft :
    1. Choisissez ADFS 2.0, puis choisissez Ajouter l'approbation de partie de confiance. Dans la page Assistant Ajout d'approbation de partie de confiance, choisissez Démarrer.
    2. Sur la page Sélectionner une source de données, choisissez Importer des données sur la partie de confiance publiées en ligne ou sur un réseau local.
    3. Pour Adresse de métadonnées de fédération (nom d'hôte ou URL), entrez **`https://signin.aws.amazon.com/saml-metadata.xml`**. Le fichier XML de métadonnées est un document de métadonnées SAML standard décrit AWS comme une partie utilisatrice.
    4. Dans la page Spécifier un nom d'affichage, entrez une valeur pour Nom d'affichage.
    5. Sur la page Choisir des règles d'autorisation d'émission, choisissez une règle d'autorisation d'émission pour autoriser ou refuser à tous les utilisateurs l'accès à cette partie de confiance.
    6. Dans la page Prêt à ajouter l'approbation, vérifiez vos paramètres.
    7. Sur la page Terminer, choisissez Ouvrir la boîte de dialogue Modifier les règles de revendication pour cette approbation de partie de confiance lorsque l'Assistant se ferme.
    8. Dans le menu contextuel (clic droit), choisissez Parties de confiance.
    9. Pour votre partie de confiance, ouvrez le menu contextuel (clic droit) et choisissez Modifier les règles de réclamation. Dans la page Modifier les règles de réclamation, choisissez Ajouter une règle.
    10. Pour le modèle de règle de réclamation, choisissez Transformer une réclamation entrante, puis sur la NameId page Modifier la règle —, procédez comme suit :

- Dans le champ Nom de la règle de réclamation, entrez NameId.
- Pour Nom de la réclamation entrante, choisissez Nom du compte Windows.
- Pour Nom de la réclamation sortante, choisissez ID nom.
- Pour Format d'ID de nom sortant, choisissez Identifiant persistant.
- Choisissez Transférer toutes les valeurs de réclamation.

11. Dans la page Modifier les règles de réclamation, choisissez Ajouter une règle. Dans la page Sélectionner un modèle de règle, pour le Modèle de règle de réclamation, choisissez Envoyer les attributs LDAP en tant que réclamations.
12. Sur la page Configurer une règle, exécutez les opérations suivantes :
    - Pour Claim rule name (Nom de la règle de revendication), saisissez RoleSessionName.
    - Pour Attribute store (Magasin d'attributs), choisissez Active Directory.
    - Dans Attribut LDAP, sélectionnez Adresses e-mail.
    - Pour Outgoing Claim Type (Type de demande sortante), sélectionnez https://aws.amazon.com/SAML/Attributes/RoleSessionName.
13. Dans la page Modifier les règles de réclamation, choisissez Ajouter une règle. Dans la page Sélectionner un modèle de règle, pour le Modèle de règle de réclamation, choisissez Envoyer des réclamations à l'aide d'une règle personnalisée.
14. Dans la page Modifier la règle — Obtenir les groupes AD pour le Nom de la règle de réclamation, entrez Obtenir les groupes AD.
15. Pour Règle personnalisée, entrez ce qui suit.

```
c:[Type ==
                                    "http://schemas.microsoft.com/ws/2008/06/
identity/claims/windowsaccountname",
                                    Issuer == "AD AUTHORITY"] => add(store =
 "Active Directory",
                                    types = ("http://temp/variable"), query =
 ";tokenGroups;{0}",
                                    param = c.Value);
```

16. Dans la page Modifier les règles de réclamation, choisissez Ajouter une règle. Dans la page Sélectionner un modèle de règle, pour le Modèle de règle de réclamation, choisissez Envoyer des réclamations à l'aide d'une règle personnalisée.
17. Dans la page Modifier une règle — Rôles pour Nom de la règle de réclamation, entrez Rôles.
18. Pour Règle personnalisée, entrez ce qui suit.

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-"] =>
 issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-", "arn:aws:iam::123456789012:saml-provider/
ADFS,arn:aws:iam::123456789012:role/ADFS-"));
```

Notez les ARN du fournisseur et du rôle SAML à assumer. Dans cet exemple, `arn:aws:iam:123456789012:saml-provider/ADFS` est l'ARN du fournisseur SAML et `arn:aws:iam:123456789012:role/ADFS-` est l'ARN du rôle.

3. Assurez-vous que vous avez téléchargé le fichier `federationmetadata.xml`. Vérifiez que le contenu du document n'a pas de caractères non valides. Il s'agit du fichier de métadonnées que vous utilisez lors de la configuration de la relation d'approbation avec AWS.
4. Créez un fournisseur d’identité SAML IAM sur la console IAM. Le document de métadonnées que vous fournissez est le fichier XML de métadonnées de fédération que vous avez enregistré lorsque vous avez configuré Azure Enterprise Application. Pour des étapes détaillées, veuillez consulter la rubrique Création et gestion d'un fournisseur d'identité IAM (Console) dans le Guide de l'utilisateur IAM.
5. Créez un rôle IAM pour la fédération SAML 2.0 sur la console IAM. Pour des étapes détaillées, voir Création d'un rôle pour SAML dans le Guide de l'utilisateur IAM.
6. Créez une politique IAM que vous pouvez attacher au rôle IAM que vous avez créé pour la fédération SAML 2.0 sur la console IAM. Pour connaître la marche à suivre en détail, consultez Création de politiques IAM (console) dans le Guide de l’utilisateur IAM. Pour obtenir un exemple Azure AD, consultez Configuration de l’authentification unique JDBC ou ODBC.

Étape 2 : pour configurer JDBC ou ODBC pour l’authentification aux services AD FS

JDBC

La procédure suivante explique comment configurer une relation JDBC avec AD FS.

- Configurez votre client de base de données pour qu'il se connecte à votre cluster via JDBC à l'aide de l'authentification unique AD FS.

  Vous pouvez utiliser n'importe quel client qui utilise un pilote JDBC pour vous connecter à l'aide de l'authentification unique AD FS ou utiliser un langage comme Java pour vous connecter à l'aide d'un script. Pour plus d’informations sur l’installation et la configuration,

consultez Configuration d'une connexion pour la version 2.x du pilote JDBC pour Amazon Redshift.

Par exemple, vous pouvez l'utiliser SQLWorkbench/J en tant que client. Lors de la configuration SQLWorkbench/J, l'URL de votre base de données utilise le format suivant.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Si vous l'utilisez SQLWorkbench/J en tant que client, procédez comme suit :

a. Démarrez SQL Workbench/J. Dans la page Sélectionner un profil de connexion, ajoutez un Groupe de profils, par exemple **ADFS**.

b. Dans Profil de connexion, entrez le nom de votre profil de connexion, par exemple **ADFS**.

c. Choisissez Manage Drivers (Gérer les pilotes), puis Amazon Redshift. Choisissez l'icône Open Folder (Ouvrir le dossier) en regard de Library (Bibliothèque), puis choisissez le fichier JDBC .jar approprié.

d. Dans la page Select Connection Profile (Sélectionner un profil de connexion) ajoutez les informations suivantes au profil de connexion :

   - Pour Utilisateur, entrez votre nom d'utilisateur AD FS. Il s'agit du nom d'utilisateur du compte que vous utilisez pour l'authentification unique et qui a la permission du cluster que vous essayez d'utiliser pour vous authentifier.
   - Pour Mot de passe, entrez votre mot de passe AD FS.
   - Pour Drivers (Pilotes), choisissez Amazon Redshift (com.amazon.redshift.jdbc.Driver).
   - Pour URL, entrez **jdbc:redshift:iam://*your-cluster-identifier*:*your-cluster-region*/*your-database-name***.

e. Sélectionnez Extended Properties (Propriétés étendues). Pour plugin_name, entrez **com.amazon.redshift.plugin.AdfsCredentialsProvider**. Cette valeur spécifie au pilote d'utiliser l'authentification unique Azure AD comme méthode d'authentification.

ODBC

Pour configurer ODBC pour l'authentification aux services AD FS

- Configurez votre client de base de données pour qu'il se connecte à votre cluster via ODBC à l'aide de l'authentification unique AD FS.

  Amazon Redshift fournit des pilotes ODBC pour les systèmes d'exploitation Linux, Windows et macOS. Avant d'installer un pilote ODBC, déterminez si votre outil client SQL est en 32 bits ou en 64 bits. Installez le pilote ODBC qui correspond aux exigences de votre outil client SQL.

  Sous Windows, dans la page Amazon Redshift ODBC Driver DSN Setup (Configuration DSN du pilote ODBC Amazon Redshift), sous Connection Settings (Paramètres de connexion), entrez les informations suivantes :

  - Pour Data Source Name (Nom de la source de données), entrez ***your-DSN***. Cela indique le nom de la source de données utilisé comme nom de profil ODBC.
  - Pour Auth type (Type d'authentification), sélectionnez Identity Provider: SAML (Fournisseur d'identité : SAML). Il s'agit de la méthode d'authentification utilisée par le pilote ODBC pour s'authentifier par authentification unique AD FS.
  - Pour Cluster ID (ID de cluster), entrez ***your-cluster-identifier***.
  - Pour Region (Région), entrez ***your-cluster-region***.
  - Pour Database (Base de données), entrez ***your-database-name***.
  - Pour Utilisateur, entrez ***your-adfs-username***. Il s'agit du nom d'utilisateur du compte AD FS que vous utilisez pour l'authentification unique, qui a l'autorisation d'accéder au cluster que vous essayez d'utiliser pour vous authentifier. Utilisez cette option uniquement si le Type d'authentification est Fournisseur d'identité : SAML.
  - Pour Mot de passe, entrez ***your-adfs-password***. Utilisez cette option uniquement si le Type d'authentification est Fournisseur d'identité : SAML.

  Sous macOS et Linux, modifiez le fichier `odbc.ini` comme suit :

  > **Note**
  >
  > Toutes les entrées sont insensibles à la casse.

- Pour clusterid, entrez ***your-cluster-identifier***. Il s'agit du nom du cluster Amazon Redshift qui a été créé.
- Pour region (région), entrez ***your-cluster-region***. Il s'agit de la AWS région du cluster Amazon Redshift créé.
- Pour database (base de données), entrez ***your-database-name***. Il s'agit du nom de la base de données à laquelle vous essayez d'accéder sur le cluster Amazon Redshift.
- Pour locale (paramètres régionaux), entrez **en-us**. Il s'agit de la langue dans laquelle les messages d'erreur s'affichent.
- Pour iam, entrez **1**. Cette valeur spécifie au pilote de s'authentifier à l'aide des informations d'identification IAM.
- Pour plugin_name, effectuez l'une des opérations suivantes :
  - Pour la configuration de l'authentification unique AD FS avec MFA, entrez **BrowserSAML**. Il s'agit de la méthode d'authentification utilisée par le pilote ODBC pour s'authentifier auprès des services AD FS.
  - Pour la configuration de l'authentification unique AD FS, entrez **ADFS**. Il s'agit de la méthode d'authentification utilisée par le pilote ODBC pour s'authentifier à l'aide de l'authentification unique Azure AD.
- Pour uid, entrez ***your-adfs-username***. Il s'agit du nom d'utilisateur du compte Microsoft Azure que vous utilisez pour l'authentification unique qui a l'autorisation sur le cluster sur lequel vous essayez de vous authentifier. Utilisez ceci uniquement lorsque plugin_name est ADFS.
- Pour pwd, entrez ***your-adfs-password***. Utilisez ceci uniquement lorsque plugin_name est ADFS.

Sous mac OS et Linux, modifiez également les paramètres de profil pour ajouter les exportations suivantes.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Azure

Vous pouvez utiliser Microsoft Azure AD en tant que fournisseur d'identité (IdP) pour accéder à votre cluster Amazon Redshift. Ce didacticiel vous montre comment vous pouvez utiliser Azure en tant que fournisseur d'identité (IdP) pour accéder à votre cluster Amazon Redshift.

Regardez la vidéo suivante pour apprendre à fédérer l'accès Amazon Redshift avec l'authentification unique Microsoft Azure AD : Fédérer l'accès à Amazon Redshift avec l'authentification unique Microsoft Azure AD.

Étape 1 : configurer Azure et votre AWS compte pour se faire confiance

La procédure suivante explique comment configurer une relation d'approbation.

Pour configurer Azure AD et votre AWS compte pour se faire confiance

1. Créez ou utilisez un cluster Amazon Redshift existant pour que vos utilisateurs Azure AD puissent se connecter. Pour configurer la connexion, certaines propriétés de ce cluster sont nécessaires, telles que l'identifiant de cluster. Pour de plus amples informations, veuillez consulter Création d'un cluster.
2. Configurez un Azure Active Directory, des groupes et des utilisateurs utilisés AWS sur le portail Microsoft Azure.
3. Ajoutez Amazon Redshift en tant qu'application d'entreprise sur le portail Microsoft Azure à utiliser pour l'authentification unique à la AWS console et la connexion fédérée à Amazon Redshift. Choisissez Application Entreprise.
4. Choisissez +Nouvelle application. La page Ajouter une application apparaît.
5. Recherchez **AWS** dans le champ de recherche.
6. Choisissez Amazon Web Services (AWS) et choisissez Ajouter. Cela crée l'application AWS .
7. Sous Gérer, choisissez Single Sign-On.
8. Choisissez SAML. La SAML-based Sign-on page Amazon Web Services (AWS) | s'affiche.
9. Choisissez Oui pour accéder à la page Configurer Single Sign-On avec SAML. Cette page affiche la liste des attributs préconfigurés associés à l'authentification unique.
10. Pour Configuration SAML de base, choisissez l'icône Modifier et choisissez Enregistrer.
11. Lorsque vous configurez plusieurs applications, indiquez une valeur d'identificateur. Par exemple, saisissez ***https://signin.aws.amazon.com/saml#2***. Notez qu'à partir de la deuxième application, utilisez ce format avec un signe # pour spécifier une valeur SPN unique.
12. Dans la section Attributs utilisateur et réclamations sélectionnez l'icône Modifier.

Par défaut, l'identifiant utilisateur unique (UID) RoleSessionName, le rôle et les SessionDuration revendications sont préconfigurés.

13. Choisissez + Ajouter une nouvelle réclamation pour ajouter une revendication pour les utilisateurs de la base de données.

    Pour Nom, saisissez **`DbUser`**.

    Pour Espace de noms, saisissez **`https://redshift.amazon.com/SAML/Attributes`**.

    Pour Source, choisissez Attribut.

    Pour Attribut source, choisissez user.userprincipalname. Ensuite, choisissez Enregistrer.

14. Choisissez + Ajouter une nouvelle réclamation pour laquelle ajouter une réclamation AutoCreate.

    Pour Nom, saisissez **`AutoCreate`**.

    Pour Espace de noms, saisissez **`https://redshift.amazon.com/SAML/Attributes`**.

    Pour Source, choisissez Attribut.

    Pour Attribut source, choisissez « true ». Ensuite, choisissez Enregistrer.

    Ici, *`123456789012`* correspond à votre compte AWS , *`AzureSSO`* correspond à un rôle IAM que vous avez créé et *`AzureADProvider`* correspond au fournisseur IAM.

Nom de la demande	Value
Identifiant utilisateur unique (ID de nom)	user.userprincipalname
https://aws.amazon.com/SAML/Attributes/SessionDuration	900
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam : :role/, arn:aws:iam : ::saml-provider/ *`123456789012 AzureSSO 123456789012 AzureADProvider`*
https://aws.amazon.com/SAML/Attributes/RoleSessionName	user.userprincipalname

Nom de la demande	Value
https://redshift.amazon.com/SAML/Attributes/AutoCreate	"true"
https://redshift.amazon.com/SAML/Attributes/DbGroups	user.assignedroles
https://redshift.amazon.com/SAML/Attributes/DbUser	user.userprincipalname

15. Sous Enregistrement de l'application > ***your-application-name*** > Authentification, ajoutez Application mobile et de bureau. Spécifiez l'URL comme http://localhost/redshift/.
16. Dans la section Certificat de signature SAML, choisissez Télécharger pour télécharger et enregistrer le fichier XML de métadonnées de fédération à utiliser lorsque vous créez un fournisseur d'identité SAML IAM. Ce fichier est utilisé pour créer l'identité fédérée d'authentification unique.
17. Créez un fournisseur d’identité SAML IAM sur la console IAM. Le document de métadonnées que vous fournissez est le fichier XML de métadonnées de fédération que vous avez enregistré lorsque vous avez configuré Azure Enterprise Application. Pour des étapes détaillées, veuillez consulter la rubrique Création et gestion d'un fournisseur d'identité IAM (Console) dans le Guide de l'utilisateur IAM.
18. Créez un rôle IAM pour la fédération SAML 2.0 sur la console IAM. Pour des étapes détaillées, voir Création d'un rôle pour SAML dans le Guide de l'utilisateur IAM.
19. Créez une politique IAM que vous pouvez attacher au rôle IAM que vous avez créé pour la fédération SAML 2.0 sur la console IAM. Pour connaître la marche à suivre en détail, consultez Création de politiques IAM (console) dans le Guide de l’utilisateur IAM.

    Modifiez la politique suivante (au format JSON) pour votre environnement :

    - Remplacez la AWS région de votre cluster par*us-west-1*.
    - Remplacez votre AWS compte par*123456789012*.
    - Remplacez votre identifiant de cluster (ou * pour tous les clusters) par *cluster-identifier*.
    - Remplacez votre base de données (ou * pour toutes les bases de données) par *dev*.
    - Remplacez *AR0AJ2UCCR6DPCEXAMPLE* par l'identifiant unique de votre rôle IAM.

- Remplacez *example.com* par le domaine de messagerie de votre locataire ou de votre entreprise.
- Remplacez *my_dbgroup* par le groupe de base de données auquel vous comptez affecter l'utilisateur

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "redshift:GetClusterCredentials",
            "Resource": [
                "arn:aws:redshift:us-west-1:123456789012:dbname:cluster-
identifier/dev",
                "arn:aws:redshift:us-west-1:123456789012:dbuser:cluster-identifier/
${redshift:DbUser}",
                "arn:aws:redshift:us-west-1:123456789012:cluster:cluster-
identifier"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:userid": "AROAJ2UCCR6DPCEXAMPLE:
${redshift:DbUser}@example.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "redshift:CreateClusterUser",
            "Resource": "arn:aws:redshift:us-west-1:123456789012:dbuser:cluster-
identifier/${redshift:DbUser}"
        },
        {
            "Effect": "Allow",
            "Action": "redshift:JoinGroup",
            "Resource": "arn:aws:redshift:us-west-1:123456789012:dbgroup:cluster-
identifier/my_dbgroup"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "redshift:DescribeClusters",
                "iam:ListRoles"
            ],
            "Resource": "*"
        }
    ]
}
```

Cette politique accorde les autorisations suivantes :

- La première section accorde à l'opération d'API `GetClusterCredentials` l'autorisation d'obtenir des informations d'identification temporaires pour le cluster spécifié. Dans cet exemple, la ressource est *`cluster-identifier`* avec la base de données *`dev`*, dans le compte *`123456789012`* et la région AWS *`us-west-1`*. La clause `${redshift:DbUser}` autorise uniquement les utilisateurs qui correspondent à la valeur `DbUser` spécifiée dans Azure AD à se connecter.
- La clause de condition impose que seuls certains utilisateurs obtiennent des informations d'identification temporaires. Il s'agit des utilisateurs sous le rôle spécifié par l'ID unique de rôle *`AROAJ2UCCR6DPCEXAMPLE`* dans le compte IAM identifié par une adresse e-mail dans le domaine de messagerie de votre entreprise. Pour plus d'informations sur les ID uniques, consultez la rubrique Identifiants uniques dans le Guide de l'utilisateur IAM.

  Votre configuration avec votre IdP (dans ce cas, Azure AD) détermine la manière dont la clause de condition est écrite. Si l'adresse e-mail de votre employé est `johndoe@example.com`, commencez par définir `${redshift:DbUser}` dans le champ correspondant au nom d'utilisateur de l'employé `johndoe`. Ensuite, pour que cette condition fonctionne, définissez ensuite le champ AWS SAML `RoleSessionName` sur le champ correspondant à l'e-mail de l'employé `johndoe@example.com`. Lorsque vous adoptez cette approche, tenez compte des éléments suivants :

  - Si vous définissez `${redshift:DbUser}` comme étant l'e-mail de l'employé, supprimez `@example.com` dans l'exemple de fichier JSON pour correspondre à `RoleSessionName`.
  - Si vous définissez `RoleSessionId` comme étant uniquement le nom d'utilisateur de l'employé, supprimez `@example.com` dans l'exemple pour correspondre à `RoleSessionName`.
  - Dans l'exemple de fichier JSON, `${redshift:DbUser}` et `RoleSessionName` sont tous deux définis sur l'e-mail de l'employé. Cet exemple de fichier JSON utilise le nom

d'utilisateur de base de données Amazon Redshift avec `@example.com` pour connecter l'utilisateur en vue d'accéder au cluster.

- La deuxième section accorde l'autorisation de créer un nom `dbuser` dans le cluster spécifié. Dans cet exemple de fichier JSON, la création est limitée à `${redshift:DbUser}`.
- La troisième section accorde l'autorisation de spécifier le `dbgroup` qu'un utilisateur peut rejoindre. Dans cet exemple de fichier JSON, un utilisateur peut rejoindre le groupe `my_dbgroup` dans le cluster spécifié.
- La quatrième section accorde l'autorisation pour des actions que l'utilisateur peut effectuer sur toutes les ressources. Dans cet exemple JSON, il permet aux utilisateurs d'appeler pour `redshift:DescribeClusters` obtenir des informations sur le cluster, telles que le point de terminaison, AWS la région et le port du cluster. Il permet également aux utilisateurs d'appeler `iam:ListRoles` pour vérifier les rôles qu'un utilisateur peut assumer.

Étape 2 : configurer JDBC ou ODBC pour l'authentification aux services Azure

JDBC

Pour configurer JDBC pour l'authentification à Microsoft Azure AD

- Configurez votre client de base de données pour qu'il se connecte à votre cluster via JDBC à l'aide de votre authentification unique Azure AD.

  Vous pouvez utiliser n'importe quel client qui utilise un pilote JDBC pour vous connecter à l'aide de l'authentification unique Azure AD ou utiliser un langage comme Java pour vous connecter à l'aide d'un script. Pour plus d'informations sur l'installation et la configuration, consultez Configuration d'une connexion pour la version 2.x du pilote JDBC pour Amazon Redshift.

  Par exemple, vous pouvez l'utiliser SQLWorkbench/J en tant que client. Lors de la configuration SQLWorkbench/J, l'URL de votre base de données utilise le format suivant.

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  Si vous l'utilisez SQLWorkbench/J en tant que client, procédez comme suit :

  a. Démarrez SQL Workbench/J. Dans la page Select Connection Profile (Sélectionner un profil de connexion), ajoutez un Profile group (Groupe de profils) appelé **`AzureAuth`**.

b. Pour Connection Profil (Profil de connexion), entrez **`Azure`**.

c. Choisissez Manage Drivers (Gérer les pilotes), puis Amazon Redshift. Choisissez l'icône Open Folder (Ouvrir le dossier) en regard de Library (Bibliothèque), puis choisissez le fichier JDBC .jar approprié.

d. Dans la page Select Connection Profile (Sélectionner un profil de connexion) ajoutez les informations suivantes au profil de connexion :

- Pour User (Utilisateur), entrez votre nom d'utilisateur Microsoft Azure. Il s'agit du nom d'utilisateur du compte Microsoft Azure que vous utilisez pour l'authentification unique et qui a la permission du cluster que vous essayez d'utiliser pour vous authentifier.
- Pour Password (Mot de passe), entrez votre mot de passe Microsoft Azure.
- Pour Drivers (Pilotes), choisissez Amazon Redshift (com.amazon.redshift.jdbc.Driver).
- Pour URL, entrez **`jdbc:redshift:iam://`*`your-cluster-identifier`*`:`*`your-cluster-region`*`/`*`your-database-name`**.

e. Choisissez Extended Properties (Propriétés étendues) pour ajouter des informations supplémentaires aux propriétés de connexion comme suit.

Pour la configuration de l'authentification unique Azure AD, ajoutez des informations supplémentaires, comme suit :

- Pour plugin_name, entrez **`com.amazon.redshift.plugin.AzureCredentialsProvider`**. Cette valeur indique au pilote d'utiliser Azure AD Single Sign-On comme méthode d'authentification.
- Pour idp_tenant, entrez ***`your-idp-tenant`***. Utilisé uniquement pour Microsoft Azure AD. Il s'agit du nom du locataire de votre entreprise configuré sur Azure AD. Cette valeur peut être le nom du locataire ou l'ID unique du locataire avec des traits d'union.
- Pour client_secret, entrez ***`your-azure-redshift-application-client-secret`***. Utilisé uniquement pour Microsoft Azure AD. Il s'agit du secret client de l'application Amazon Redshift que vous avez créée lors de la configuration de votre Sign-On configuration Azure Single. Cela ne s'applique qu'au plugin com.amazon.redshift.plugin. AzureCredentialsProviderplug-in.
- Pour client_id, entrez ***`your-azure-redshift-application-client-id`***. Utilisé uniquement pour Microsoft Azure AD. Il s'agit de l'ID client (avec tirets) de l'application Amazon Redshift que vous avez créée lors de la configuration de votre configuration Azure Single. Sign-On

Pour la configuration de l'authentification unique Azure AD avec MFA, ajoutez des informations supplémentaires aux propriétés de connexion, comme suit :

- Pour plugin_name, entrez **`com.amazon.redshift.plugin.BrowserAzureCredentialsProvider`**. Cette valeur spécifie au pilote d'utiliser l'authentification unique Azure AD avec MFA comme méthode d'authentification.
- Pour idp_tenant, entrez ***`your-idp-tenant`***. Utilisé uniquement pour Microsoft Azure AD. Il s'agit du nom du locataire de votre entreprise configuré sur Azure AD. Cette valeur peut être le nom du locataire ou l'ID unique du locataire avec des traits d'union.
- Pour client_id, entrez ***`your-azure-redshift-application-client-id`***. This option is used only for Microsoft Azure AD. Il s'agit de l'ID client (avec des traits d'union) de l'application Amazon Redshift que vous avez créé lors de la définition de votre configuration d'authentification unique Azure AD avec MFA.
- Pour listen_port, entrez ***`your-listen-port`***. C'est le port que le serveur local écoute. La valeur par défaut est 7890.
- Pour idp_response_timeout, entrez ***`the-number-of-seconds`***. Il s'agit du nombre de secondes à attendre avant l'expiration lorsque le serveur IdP renvoie une réponse. Le nombre minimum de secondes doit être de 10. Si l'établissement de la connexion dépasse ce seuil, la connexion est abandonnée.

ODBC

Pour configurer ODBC pour l'authentification à Microsoft Azure AD

- Configurez votre client de base de données pour qu'il se connecte à votre cluster via ODBC à l'aide de votre authentification unique Azure AD.

  Amazon Redshift fournit des pilotes ODBC pour les systèmes d'exploitation Linux, Windows et macOS. Avant d'installer un pilote ODBC, déterminez si votre outil client SQL est en 32 bits ou en 64 bits. Installez le pilote ODBC qui correspond aux exigences de votre outil client SQL.

  Sous Windows, dans la page Amazon Redshift ODBC Driver DSN Setup (Configuration DSN du pilote ODBC Amazon Redshift), sous Connection Settings (Paramètres de connexion), entrez les informations suivantes :

- Pour Data Source Name (Nom de la source de données), entrez ***your-DSN***. Cela indique le nom de la source de données utilisé comme nom de profil ODBC.
- Pour Auth type (Type d'authentification) de la configuration d'authentification unique Azure AD, choisissez **`Identity Provider: Azure AD`**. Il s'agit de la méthode d'authentification utilisée par le pilote ODBC pour s'authentifier à l'aide de l'authentification unique Azure.
- Pour Auth type (Type d'authentification) de la configuration d'authentification unique Azure AD avec MFA, choisissez **`Identity Provider: Browser Azure AD`**. Il s'agit de la méthode d'authentification utilisée par le pilote ODBC pour s'authentifier à l'aide de l'authentification unique Azure avec MFA.
- Pour Cluster ID (ID de cluster), entrez ***your-cluster-identifier***.
- Pour Region (Région), entrez ***your-cluster-region***.
- Pour Database (Base de données), entrez ***your-database-name***.
- Pour Utilisateur, entrez ***your-azure-username***. Il s'agit du nom d'utilisateur du compte Microsoft Azure que vous utilisez pour l'authentification unique et qui a la permission du cluster que vous essayez d'utiliser pour vous authentifier. Utiliser cette option uniquement lorsque Type d’authentification est Fournisseur d’identité : Azure AD.
- Pour Mot de passe, entrez ***your-azure-password***. Utiliser cette option uniquement lorsque Type d’authentification est Fournisseur d’identité : Azure AD.
- Pour IdP Tenant (Locataire IdP), entrez ***your-idp-tenant***. Il s’agit du nom du locataire de votre entreprise configuré sur votre IdP (Azure). Cette valeur peut être le nom du locataire ou l’ID unique du locataire avec des traits d’union.
- Pour Azure Client Secret (Secret client Azure), entrez ***your-azure-redshift-application-client-secret***. Il s'agit du secret client de l'application Amazon Redshift que vous avez créé lors de la définition de votre configuration d'authentification unique Azure.
- Pour Azure Client ID (ID client Azure), entrez ***your-azure-redshift-application-client-id***. Il s'agit de l'ID client (avec des traits d'union) de l'application Amazon Redshift que vous avez créé lors de la définition de votre configuration d'authentification unique Azure.
- Pour Port d’écoute, entrez ***your-listen-port***. Il s'agit du port d'écoute par défaut que le serveur local écoute. La valeur par défaut est 7890. Cela s'applique uniquement au plugin Navigateur Azure AD.

- Pour Délai de réponse, entrez ***the-number-of-seconds***. Il s'agit du nombre de secondes à attendre avant l'expiration lorsque le serveur IdP renvoie une réponse. Le nombre minimum de secondes doit être de 10. Si l'établissement de la connexion dépasse ce seuil, la connexion est abandonnée. Cette option s'applique uniquement au plugin du navigateur Azure AD.

Sous macOS et Linux, modifiez le fichier `odbc.ini` comme suit :

> **Note**
>
> Toutes les entrées sont insensibles à la casse.

- Pour clusterid, entrez ***your-cluster-identifier***. Il s'agit du nom du cluster Amazon Redshift qui a été créé.
- Pour region (région), entrez ***your-cluster-region***. Il s'agit de la AWS région du cluster Amazon Redshift créé.
- Pour database (base de données), entrez ***your-database-name***. Il s'agit du nom de la base de données à laquelle vous essayez d'accéder sur le cluster Amazon Redshift.
- Pour locale (paramètres régionaux), entrez **en-us**. Il s'agit de la langue dans laquelle les messages d'erreur s'affichent.
- Pour iam, entrez **1**. Cette valeur spécifie au pilote de s'authentifier à l'aide des informations d'identification IAM.
- Pour plugin_name de la configuration d'authentification unique Azure AD, entrez **AzureAD**. Cela indique au pilote d'utiliser Azure Single Sign-On comme méthode d'authentification.
- Pour plugin_name de la configuration d'authentification unique Azure AD avec MFA, entrez **BrowserAzureAD**. Cela indique au pilote d'utiliser Azure Single Sign-On avec MFA comme méthode d'authentification.
- Pour uid, entrez ***your-azure-username***. Il s'agit du nom d'utilisateur du compte Microsoft Azure que vous utilisez pour l'authentification unique qui a l'autorisation sur le cluster sur lequel vous essayez de vous authentifier. Utilisez ceci uniquement lorsque plugin_name est AzureAD.
- Pour pwd, entrez ***your-azure-password***. Utilisez ceci uniquement lorsque plugin_name est AzureAD.

- Pour idp_tenant, entrez ***your-idp-tenant***. Il s'agit du nom du locataire de votre entreprise configuré sur votre IdP (Azure). Cette valeur peut être le nom du locataire ou l'ID unique du locataire avec des traits d'union.
- Pour client_secret, entrez ***your-azure-redshift-application-client-secret***. Il s'agit du secret client de l'application Amazon Redshift que vous avez créé lors de la définition de votre configuration d'authentification unique Azure.
- Pour client_id, entrez ***your-azure-redshift-application-client-id***. Il s'agit de l'ID client (avec des traits d'union) de l'application Amazon Redshift que vous avez créé lors de la définition de votre configuration d'authentification unique Azure.
- Pour listen_port, entrez ***your-listen-port***. C'est le port que le serveur local écoute. La valeur par défaut est 7890. Cela s'applique au plugin Navigateur Azure AD.
- Pour idp_response_timeout, entrez ***the-number-of-seconds***. Il s'agit de la période spécifiée en secondes pour attendre la réponse d'Azure. Cette option s'applique au plugin du navigateur Azure AD.

Sous mac OS et Linux, modifiez également les paramètres de profil pour ajouter les exportations suivantes.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Résolution des problèmes

Pour résoudre les problèmes liés au plugin Browser Azure AD, tenez compte de ce qui suit.

- Pour utiliser le plugin Browser Azure AD, vous devez définir l'URL de réponse spécifiée dans la demande pour qu'elle corresponde à l'URL de réponse configurée pour votre application. Accédez à la page Configurer Single Sign-On avec SAML sur le portail Microsoft Azure. Vérifiez ensuite que l'URL de réponse est définie sur http://localhost/redshift/.
- Si vous obtenez une erreur de locataire IdP, vérifiez que le nom du Locataire IdP correspond au nom de domaine que vous avez utilisé initialement pour configurer Active Directory dans Microsoft Azure.

Sous Windows, accédez à la section Paramètres de connexion de la page Configuration du DSN ODBC d'Amazon Redshift. Vérifiez ensuite que le nom de locataire de votre société configurée sur votre IdP (Azure) correspond au nom de domaine que vous avez initialement utilisé pour configurer Active Directory dans Microsoft Azure.

Sous macOS et Linux, recherchez le fichier odbc.ini. Vérifiez ensuite que le nom de locataire de votre société configurée sur votre IdP (Azure) correspond au nom de domaine que vous avez initialement utilisé pour configurer Active Directory dans Microsoft Azure.

- Si vous obtenez une erreur indiquant que l'URL de réponse spécifiée dans la demande ne correspond pas aux URL de réponse configurées pour votre application, vérifiez que les URI de redirection sont identiques à l'URL de réponse.

  Accédez à la page Enregistrement de l'application de votre application sur le portail Microsoft Azure. Vérifiez ensuite que les URI de redirection correspondent à l'URL de réponse.
- Si vous obtenez la réponse inattendue : erreur non autorisée, vérifiez que vous avez terminé la configuration des Applications mobiles et de bureau.

  Accédez à la page Enregistrement de l'application de votre application sur le portail Microsoft Azure. Accédez ensuite à Authentification et vérifiez que vous avez configuré les applications mobiles et de bureau à utiliser http://localhost/redshift/ comme URI de redirection.

Ping Identity

Vous pouvez utiliser Ping Identity comme fournisseur d'identité (IdP) pour accéder à votre cluster Amazon Redshift. Ce didacticiel vous montre comment vous pouvez utiliser Ping Identity en tant que fournisseur d’identité (IdP) pour accéder à votre cluster Amazon Redshift.

Étape 1 : configurez Ping Identity et votre AWS compte pour se faire confiance

La procédure suivante décrit comment configurer une relation de confiance à l'aide du PingOne portail.

Pour configurer Ping Identity et votre AWS compte pour se faire confiance

1. Créez ou utilisez un cluster Amazon Redshift existant pour que vos utilisateurs Ping Identity puissent se connecter. Pour configurer la connexion, certaines propriétés de ce cluster sont nécessaires, telles que l’identifiant de cluster. Pour de plus amples informations, veuillez consulter Création d’un cluster.

2. Ajoutez Amazon Redshift en tant que nouvelle application SAML sur le PingOne portail. Pour obtenir des étapes détaillées, consultez la documentation Ping Identity.

   1. Accédez à Mes applications.
   2. Sous Ajouter une application, choisissez Nouvelle application SAML.
   3. Dans Application Name (Nom de l'application), saisissez **`Amazon Redshift`**.
   4. Pour Version de protocole, choisissez SAML v2.0.
   5. Pour Catégorie, choisissez ***`your-application-category`***.
   6. Pour Assertion Consumer Service (ACS), tapez ***`your-redshift-local-host-url`***. Il s'agit de l'hôte local et du port vers lesquels l'assertion SAML redirige.
   7. Pour Entity ID (ID d'entité), saisissez `urn:amazon:webservices`.
   8. Pour Signature, choisissez Signer l’assertion.
   9. Dans la section Mappage d'attributs SSO, créez les réclamations comme indiqué dans le tableau suivant.

Attribut de l'application	Attribut de pont d'identité de la valeur littérale
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam : :role/, arn:aws:iam : ::saml-provider/ *`123456789012 Ping 123456789012 PingProvider`*
https://aws.amazon.com/SAML/Attributes/RoleSessionName	e-mail
https://redshift.amazon.com/SAML/Attributes/AutoCreate	"true"
https://redshift.amazon.com/SAML/Attributes/DbUser	e-mail

Attribut de l'application	Attribut de pont d'identité de la valeur littérale
https://redshift.amazon.com/SAML/Attributes/DbGroups	Les groupes des attributs « DbGroups » contiennent le préfixe @directory. Pour supprimer cela, dans Identity Bridge (Pont d'identité), saisissez memberOf. Dans Fonction, choisissez ExtractByRegularExpression. Dans Expression, saisissez (.*)[\@](?:.*).

3. Pour Accès au groupe, configurez l'accès au groupe suivant, si nécessaire :
   - https://aws.amazon.com/SAML/Attributes/Role
   - https://aws.amazon.com/SAML/Attributes/RoleSessionName
   - https://redshift.amazon.com/SAML/Attributes/AutoCreate
   - https://redshift.amazon.com/SAML/Attributes/DbUser
4. Passez en revue votre configuration et apportez des modifications, si nécessaire.
5. Utilisez l'URL Initiate Single Sign-On (SSO) comme URL de connexion pour le plug-in SAML du navigateur.
6. Créez un fournisseur d’identité SAML IAM sur la console IAM. Le document de métadonnées que vous fournissez est le fichier XML de métadonnées de fédération que vous avez enregistré lorsque vous avez configuré Ping Identity. Pour des étapes détaillées, veuillez consulter la rubrique Création et gestion d'un fournisseur d'identité IAM (Console) dans le Guide de l'utilisateur IAM.
7. Créez un rôle IAM pour la fédération SAML 2.0 sur la console IAM. Pour des étapes détaillées, voir Création d'un rôle pour SAML dans le Guide de l'utilisateur IAM.
8. Créez une politique IAM que vous pouvez attacher au rôle IAM que vous avez créé pour la fédération SAML 2.0 sur la console IAM. Pour connaître la marche à suivre en détail, consultez Création de politiques IAM (console) dans le Guide de l’utilisateur IAM. Pour obtenir un exemple Azure AD, consultez Configuration de l’authentification unique JDBC ou ODBC.

Étape 2 : configurer JDBC ou ODBC pour l’authentification aux services Ping Identity

JDBC

Pour configurer JDBC pour l'authentification auprès de Ping Identity

- Configurez votre client de base de données pour vous connecter à votre cluster via JDBC à l'aide de l'authentification unique Ping Identity.

  Vous pouvez utiliser n'importe quel client qui utilise un pilote JDBC pour vous connecter à l'aide de l'authentification unique Ping Identity ou utiliser un langage comme Java pour vous connecter à l'aide d'un script. Pour plus d’informations sur l’installation et la configuration, consultez Configuration d’une connexion pour la version 2.x du pilote JDBC pour Amazon Redshift.

  Par exemple, vous pouvez l'utiliser SQLWorkbench/J en tant que client. Lors de la configuration SQLWorkbench/J, l'URL de votre base de données utilise le format suivant.

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  Si vous l'utilisez SQLWorkbench/J en tant que client, procédez comme suit :

  a. Démarrez SQL Workbench/J. Dans la page Sélectionner un profil de connexion, ajoutez un Groupe de profils, par exemple **`Ping`**.

  b. Pour Profil de connexion, entrez ***`your-connection-profile-name`***, par exemple **`Ping`**.

  c. Choisissez Manage Drivers (Gérer les pilotes), puis Amazon Redshift. Choisissez l’icône Open Folder (Ouvrir le dossier) en regard de Library (Bibliothèque), puis choisissez le fichier JDBC .jar approprié.

  d. Dans la page Select Connection Profile (Sélectionner un profil de connexion) ajoutez les informations suivantes au profil de connexion :

     - Dans le champ Utilisateur, entrez votre nom PingOne d'utilisateur. Il s'agit du nom d'utilisateur du compte PingOne que vous utilisez pour l'authentification unique et qui a la permission du cluster que vous essayez d'utiliser pour vous authentifier.
     - Pour Mot de passe, entrez votre PingOne mot de passe.
     - Pour Drivers (Pilotes), choisissez Amazon Redshift (com.amazon.redshift.jdbc.Driver).

- Pour URL, entrez **jdbc:redshift:iam://*your-cluster-identifier*:*your-cluster-region*/*your-database-name***.

e. Choisissez Propriétés étendues et effectuez l'une des opérations suivantes :

- Pour login_url, entrez ***your-ping-sso-login-url***. Cette valeur indique à l'URL d'utiliser l'authentification unique comme authentification pour se connecter.
- Pour Ping Identity, pour plugin_name, entrez **com.amazon.redshift.plugin.PingCredentialsProvider**. Cette valeur spécifie au pilote d'utiliser l'authentification unique Ping Identity comme méthode d'authentification.
- Pour Ping Identity avec l'authentification unique, pour plugin_name, entrez **com.amazon.redshift.plugin.BrowserSamlCredentialsProvider**. Cette valeur indique au pilote d'utiliser Ping Identity PingOne avec l'authentification unique comme méthode d'authentification.

ODBC

Pour configurer ODBC pour l'authentification à Ping Identity

- Configurez votre client de base de données pour qu'il se connecte à votre cluster via ODBC à l'aide de l'authentification PingOne unique Ping Identity.

  Amazon Redshift fournit des pilotes ODBC pour les systèmes d'exploitation Linux, Windows et macOS. Avant d'installer un pilote ODBC, déterminez si votre outil client SQL est en 32 bits ou en 64 bits. Installez le pilote ODBC qui correspond aux exigences de votre outil client SQL.

  Sous Windows, dans la page Amazon Redshift ODBC Driver DSN Setup (Configuration DSN du pilote ODBC Amazon Redshift), sous Connection Settings (Paramètres de connexion), entrez les informations suivantes :

  - Pour Data Source Name (Nom de la source de données), entrez ***your-DSN***. Cela indique le nom de la source de données utilisé comme nom de profil ODBC.
  - Pour Type d'authentification, effectuez l'une des actions suivantes :
    - Pour la configuration de Ping Identity, choisissez Fournisseur d'identité : Ping Federate. Il s'agit de la méthode d'authentification utilisée par le pilote ODBC pour s'authentifier à l'aide de l'authentification unique Ping Identity.

  - Pour la configuration de Ping Identity avec l'authentification unique, choisissez Identity Provider: Browser SAML (Fournisseur d'identité : navigateur SAML). Il s'agit de la méthode d'authentification utilisée par le pilote ODBC pour s'authentifier à l'aide de Ping Identity avec l'authentification unique.
- Pour Cluster ID (ID de cluster), entrez ***your-cluster-identifier***.
- Pour Region (Région), entrez ***your-cluster-region***.
- Pour Database (Base de données), entrez ***your-database-name***.
- Pour Utilisateur, entrez ***your-ping-username***. Il s'agit du nom d'utilisateur du PingOne compte que vous utilisez pour l'authentification unique et qui est autorisé à accéder au cluster à l'aide duquel vous essayez de vous authentifier. Utilisez-le uniquement pour le type d'authentification qui est Identity Provider : PingFederate.
- Pour Mot de passe, entrez ***your-ping-password***. Utilisez-le uniquement pour le type d'authentification qui est Identity Provider : PingFederate.
- Pour Port d'écoute, entrez ***your-listen-port***. C'est le port que le serveur local écoute. La valeur par défaut est 7890. Ceci s'applique uniquement au plugin du navigateur SAML.
- Pour Délai de réponse, entrez ***the-number-of-seconds***. Il s'agit du nombre de secondes à attendre avant l'expiration lorsque le serveur IdP renvoie une réponse. Le nombre minimum de secondes doit être de 10. Si l'établissement de la connexion dépasse ce seuil, la connexion est abandonnée. Ceci s'applique uniquement au plugin du navigateur SAML.
- Pour URL de connexion, entrez ***your-login-url***. Ceci s'applique uniquement au plugin du navigateur SAML.

Sous macOS et Linux, modifiez le fichier `odbc.ini` comme suit :

> **Note**
>
> Toutes les entrées sont insensibles à la casse.

- Pour clusterid, entrez ***your-cluster-identifier***. Il s'agit du nom du cluster Amazon Redshift qui a été créé.
- Pour region (région), entrez ***your-cluster-region***. Il s'agit de la AWS région du cluster Amazon Redshift créé.

- Pour database (base de données), entrez ***your-database-name***. Il s'agit du nom de la base de données à laquelle vous essayez d'accéder sur le cluster Amazon Redshift.
- Pour locale (paramètres régionaux), entrez **en-us**. Il s’agit de la langue dans laquelle les messages d’erreur s’affichent.
- Pour iam, entrez **1**. Cette valeur spécifie au pilote de s’authentifier à l’aide des informations d’identification IAM.
- Pour plugin_name, effectuez l’une des opérations suivantes :
  - Pour la configuration de Ping Identity, entrez **BrowserSAML**. Il s'agit de la méthode d'authentification utilisée par le pilote ODBC pour s'authentifier auprès de Ping Identity.
  - Pour la configuration de Ping Identity avec l'authentification unique, entrez **Ping**. Il s'agit de la méthode d'authentification utilisée par le pilote ODBC pour s'authentifier à l'aide de Ping Identity avec l'authentification unique.
- Pour uid, entrez ***your-ping-username***. Il s’agit du nom d’utilisateur du compte Microsoft Azure que vous utilisez pour l’authentification unique qui a l’autorisation sur le cluster sur lequel vous essayez de vous authentifier. Utilisez ceci uniquement lorsque plugin_name est Ping.
- Pour pwd, entrez ***your-ping-password***. Utilisez ceci uniquement lorsque plugin_name est Ping.
- Pour login_url, entrez ***your-login-url***. Il s'agit de l'URL de lancement de l'authentification unique qui renvoie la réponse SAML. Ceci s’applique uniquement au plugin du navigateur SAML.
- Pour idp_response_timeout, entrez ***the-number-of-seconds***. Il s'agit de la période spécifiée en secondes pour attendre la réponse d' PingOne Identity. Ceci s’applique uniquement au plugin du navigateur SAML.
- Pour listen_port, entrez ***your-listen-port***. C’est le port que le serveur local écoute. La valeur par défaut est 7890. Ceci s'applique uniquement au plugin du navigateur SAML.

Sous mac OS et Linux, modifiez également les paramètres de profil pour ajouter les exportations suivantes.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Okta

Vous pouvez utiliser Okta comme fournisseur d'identité (IdP) pour accéder à votre cluster Amazon Redshift. Ce didacticiel vous montre comment vous pouvez utiliser Okta en tant que fournisseur d'identité (IdP) pour accéder à votre cluster Amazon Redshift.

Étape 1 : configurez Okta et votre AWS compte pour se faire confiance

La procédure suivante explique comment configurer une relation d'approbation.

Pour configurer Okta et votre AWS compte pour se faire confiance

1. Créez ou utilisez un cluster Amazon Redshift existant pour que vos utilisateurs Okta puissent se connecter. Pour configurer la connexion, certaines propriétés de ce cluster sont nécessaires, telles que l'identifiant de cluster. Pour de plus amples informations, veuillez consulter Création d'un cluster.
2. Ajoutez Amazon Redshift comme nouvelle application sur le portail Okta. Pour les étapes détaillées, consultez la documentation Okta.
   - Choisissez Ajouter une application.
   - Sous Ajouter une application, choisissez Créer une nouvelle application.
   - Dans la page Créer une nouvelle intégration d'applications, pour Plateforme, choisissez Web.
   - Pour Méthode de connexion, choisissez SAML v2.0.
   - Dans la page Paramètres généraux, pour Nom de l'application, entrez ***your-redshift-saml-sso-name***. Il s'agit du nom de votre application.
   - Dans la page Paramètres SAML, pour URL d'authentification unique, entrez ***your-redshift-local-host-url***. Il s'agit de l'hôte local et du port vers lequel l'assertion SAML redirige, par exemple`http://localhost:7890/redshift/` .
3. Utilisez la valeur de l'URL de connexion unique comme URL du destinataire et URL de destination.
4. Pour Signature, choisissez Signer l'assertion.
5. Pour URI d'audience (ID d'entité SP), entrez **`urn:amazon:webservices`** pour les réclamations, comme indiqué dans le tableau suivant.
6. Dans la section Paramètres avancés, pour ID d'émetteur SAML, saisissez ***your-Identity-Provider-Issuer-ID***, que vous pouvez trouver dans la section Afficher les instructions de configuration.

7. Dans la section Instructions d'attribut, créez les réclamations comme indiqué dans le tableau suivant.

Nom de la demande	Value
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam : :role/, arn:aws:iam : ::saml-provider/ *123456789012 Okta 123456789012 Okta*
https://aws.amazon.com/SAML/Attributes/RoleSessionName	user.email
https://redshift.amazon.com/SAML/Attributes/AutoCreate	"true"
https://redshift.amazon.com/SAML/Attributes/DbUser	user.email

8. Dans la section Lien intégré de l'application, recherchez l'URL que vous pouvez utiliser comme URL de connexion pour le plugin SAML du navigateur.
9. Créez un fournisseur d’identité SAML IAM sur la console IAM. Le document de métadonnées que vous fournissez est le fichier XML de métadonnées de fédération que vous avez enregistré lorsque vous avez configuré Okta. Pour des étapes détaillées, veuillez consulter la rubrique Création et gestion d'un fournisseur d'identité IAM (Console) dans le Guide de l'utilisateur IAM.
10. Créez un rôle IAM pour la fédération SAML 2.0 sur la console IAM. Pour des étapes détaillées, voir Création d'un rôle pour SAML dans le Guide de l'utilisateur IAM.
11. Créez une politique IAM que vous pouvez attacher au rôle IAM que vous avez créé pour la fédération SAML 2.0 sur la console IAM. Pour connaître la marche à suivre en détail, consultez Création de politiques IAM (console) dans le Guide de l’utilisateur IAM. Pour obtenir un exemple Azure AD, consultez Configuration de l’authentification unique JDBC ou ODBC.

Étape 2 : configurer JDBC ou ODBC pour l’authentification aux services Otka

JDBC

Pour configurer JDBC pour l'authentification auprès d'Okta

- Configurez votre client de base de données pour qu'il se connecte à votre cluster via JDBC à l'aide de l'authentification unique Okta.

  Vous pouvez utiliser n'importe quel client qui utilise un pilote JDBC pour vous connecter à l'aide de l'authentification unique Okta ou utiliser un langage comme Java pour vous connecter à l'aide d'un script. Pour plus d’informations sur l’installation et la configuration, consultez Configuration d’une connexion pour la version 2.x du pilote JDBC pour Amazon Redshift.

  Par exemple, vous pouvez l'utiliser SQLWorkbench/J en tant que client. Lors de la configuration SQLWorkbench/J, l'URL de votre base de données utilise le format suivant.

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  Si vous l'utilisez SQLWorkbench/J en tant que client, procédez comme suit :

  a. Démarrez SQL Workbench/J. Dans la page Sélectionner un profil de connexion, ajoutez un Groupe de profils, par exemple **`Okta`**.

  b. Pour Profil de connexion, entrez ***`your-connection-profile-name`***, par exemple **`Okta`**.

  c. Choisissez Manage Drivers (Gérer les pilotes), puis Amazon Redshift. Choisissez l’icône Open Folder (Ouvrir le dossier) en regard de Library (Bibliothèque), puis choisissez le fichier JDBC .jar approprié.

  d. Dans la page Select Connection Profile (Sélectionner un profil de connexion) ajoutez les informations suivantes au profil de connexion :

     - Pour Utilisateur, entrez votre nom d'utilisateur Okta. Il s'agit du nom d'utilisateur du compte Okta que vous utilisez pour l'authentification unique et qui a la permission du cluster que vous essayez d'utiliser pour vous authentifier.
     - Pour Mot de passe, entrez votre mot de passe Okta.
     - Pour Drivers (Pilotes), choisissez Amazon Redshift (com.amazon.redshift.jdbc.Driver).

- Pour URL, entrez **jdbc:redshift:iam://*your-cluster-identifier*:*your-cluster-region*/*your-database-name***.

e. Choisissez Propriétés étendues et effectuez l'une des opérations suivantes :

- Pour login_url, entrez ***your-okta-sso-login-url***. Cette valeur indique à l'URL d'utiliser l'authentification unique comme authentification pour se connecter à Okta.
- Pour l'authentification unique Okta, pour plugin_name, entrez **com.amazon.redshift.plugin.OktaCredentialsProvider**. Cette valeur spécifie au pilote d'utiliser l'authentification unique Okta comme méthode d'authentification.
- Pour l'authentification unique Okta avec MFA, pour plugin_name, entrez **com.amazon.redshift.plugin.BrowserSamlCredentialsProvider**. Cette valeur spécifie au pilote d'utiliser l'authentification unique Okta avec MFA comme méthode d'authentification.

ODBC

Pour configurer ODBC pour l'authentification auprès d'Okta

- Configurez votre client de base de données pour qu'il se connecte à votre cluster via ODBC à l'aide de l'authentification unique Okta.

  Amazon Redshift fournit des pilotes ODBC pour les systèmes d'exploitation Linux, Windows et macOS. Avant d'installer un pilote ODBC, déterminez si votre outil client SQL est en 32 bits ou en 64 bits. Installez le pilote ODBC qui correspond aux exigences de votre outil client SQL.

  Sous Windows, dans la page Amazon Redshift ODBC Driver DSN Setup (Configuration DSN du pilote ODBC Amazon Redshift), sous Connection Settings (Paramètres de connexion), entrez les informations suivantes :

  - Pour Data Source Name (Nom de la source de données), entrez ***your-DSN***. Cela indique le nom de la source de données utilisé comme nom de profil ODBC.
  - Pour Type d'authentification, effectuez l'une des actions suivantes :
    - Pour la configuration de l'authentification unique Okta, choisissez **Identity Provider: Okta**. Il s'agit de la méthode d'authentification utilisée par le pilote ODBC pour s'authentifier à l'aide de l'authentification unique Okta.

    - Pour la configuration de l'authentification unique Okta avec MFA, choisissez **`Identity Provider: Browser SAML`**. Il s'agit de la méthode d'authentification utilisée par le pilote ODBC pour s'authentifier à l'aide de l'authentification unique Okta avec MFA.
- Pour Cluster ID (ID de cluster), entrez ***`your-cluster-identifier`***.
- Pour Region (Région), entrez ***`your-cluster-region`***.
- Pour Database (Base de données), entrez ***`your-database-name`***.
- Pour Utilisateur, entrez ***`your-okta-username`***. Il s'agit du nom d'utilisateur du compte Okta que vous utilisez pour l'authentification unique et qui a la permission d'accéder au cluster que vous essayez d'utiliser pour vous authentifier. Utilisez cette option uniquement si le Type d'authentification est Fournisseur d'identité : Okta.
- Pour Mot de passe, entrez ***`your-okta-password`***. Utilisez cette option uniquement si le Type d'authentification est Fournisseur d'identité : Okta.

Sous macOS et Linux, modifiez le fichier `odbc.ini` comme suit :

> **Note**
>
> Toutes les entrées sont insensibles à la casse.

- Pour clusterid, entrez ***`your-cluster-identifier`***. Il s'agit du nom du cluster Amazon Redshift qui a été créé.
- Pour region (région), entrez ***`your-cluster-region`***. Il s'agit de la AWS région du cluster Amazon Redshift créé.
- Pour database (base de données), entrez ***`your-database-name`***. Il s'agit du nom de la base de données à laquelle vous essayez d'accéder sur le cluster Amazon Redshift.
- Pour locale (paramètres régionaux), entrez **`en-us`**. Il s'agit de la langue dans laquelle les messages d'erreur s'affichent.
- Pour iam, entrez **`1`**. Cette valeur spécifie au pilote de s'authentifier à l'aide des informations d'identification IAM.
- Pour plugin_name, effectuez l'une des opérations suivantes :
    - Pour la configuration de l'authentification unique Okta avec MFA, entrez **`BrowserSAML`**. Il s'agit de la méthode d'authentification utilisée par le pilote ODBC pour s'authentifier via l'authentification unique Okta avec MFA.

    - Pour la configuration de l'authentification unique Okta, entrez **`Okta`**. Il s'agit de la méthode d'authentification utilisée par le pilote ODBC pour s'authentifier à l'aide de l'authentification unique Okta.
- Pour uid, entrez ***`your-okta-username`***. Il s'agit du nom d'utilisateur du compte Okta que vous utilisez pour l'authentification unique qui a l'autorisation d'accéder au cluster sur lequel vous essayez de vous authentifier. Utilisez ceci uniquement lorsque plugin_name est Okta.
- Pour pwd, entrez ***`your-okta-password`***. Utilisez ceci uniquement lorsque plugin_name est Okta.
- Pour login_url, entrez ***`your-login-url`***. Il s'agit de l'URL de lancement de l'authentification unique qui renvoie la réponse SAML. Ceci s'applique uniquement au plugin du navigateur SAML.
- Pour idp_response_timeout, entrez ***`the-number-of-seconds`***. Il s'agit de la période spécifiée en secondes pour attendre une réponse PingOne. Ceci s'applique uniquement au plugin du navigateur SAML.
- Pour listen_port, entrez ***`your-listen-port`***. C'est le port que le serveur local écoute. La valeur par défaut est 7890. Ceci s'applique uniquement au plugin du navigateur SAML.

Sous mac OS et Linux, modifiez également les paramètres de profil pour ajouter les exportations suivantes.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Autorisation d'accès à Amazon Redshift AWS services en votre nom

Certaines fonctionnalités d'Amazon Redshift nécessitent qu'Amazon Redshift accède à d'autres AWS services en votre nom. Par exemple, les commandes COPY et UNLOAD peuvent charger ou décharger les données de votre cluster Amazon Redshift à l'aide d'un compartiment Amazon S3. La commande CREATE EXTERNAL FUNCTION peut invoquer une fonction AWS Lambda à l'aide d'une fonction Lambda définie par l'utilisateur (UDF) scalaire. Amazon Redshift Spectrum peut utiliser un catalogue de données dans Amazon Athena ou. AWS Glue Pour que vos clusters Amazon Redshift agissent en votre nom, vous fournissez les informations d'identification de sécurité à vos

clusters. La méthode recommandée pour fournir des informations d'identification de sécurité consiste à spécifier un rôle Gestion des identités et des accès AWS (IAM). Pour COPY et UNLOAD, vous pouvez fournir des informations d'identification temporaires.

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec des AWS personnes extérieures au Console de gestion AWS. La manière d'accorder l'accès par programmation dépend du type d'utilisateur qui accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Recommandé) Utilisez les informations d'identification de la console comme informations d'identification temporaires pour signer les AWS CLI demandes programmatiques adressées aux AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, consultez la section Connexion pour le développement AWS local dans le Guide de AWS Command Line Interface l'utilisateur. • Pour les AWS kits de développement, consultez la section Connexion pour le développement AWS local dans le Guide de référence AWS des kits de développement logiciel et des outils.
Identité de la main-d'œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, reportez-vous AWS CLI à

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
		la section Configuration de l'utilisation AWS IAM Identity Center dans le Guide de AWS Command Line Interface l'utilisateur. • Pour les AWS kits de développement logiciel, les outils et les AWS API, consultez la section Authentification IAM Identity Center dans le Guide de référence AWS des kits de développement logiciel et des outils.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de la section Utilisation des informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer des demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, consultez la section Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS kits de développement logiciel et les outils, consultez la section Authentification à l'aide d'informations d'identification à long terme dans le Guide de référence AWS des kits de développement logiciel et des outils. • Pour les AWS API, consultez la section Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Découvrez ci-dessous comment créer un rôle IAM avec les autorisations appropriées pour accéder à d'autres AWS services. Vous devez également associer le rôle à votre cluster et spécifier l'Amazon Resource Name (ARN) du rôle lorsque vous exécutez la commande Amazon Redshift. Pour plus d'informations, consultez Autorisation des opérations COPY, UNLOAD, CREATE EXTERNAL FUNCTION et CREATE EXTERNAL SCHEMA à l'aide des rôles IAM.

De plus, un super-utilisateur peut accorder le privilège ASSUMEROLE à des utilisateurs et des groupes spécifiques pour fournir l'accès à un rôle pour les opérations COPY et UNLOAD. Pour plus d'informations, consultez la rubrique GRANT dans le Guide du développeur de la base de données Amazon Redshift.

Création d'un rôle IAM pour permettre à votre cluster Amazon Redshift d'accéder AWS services

Création d'un rôle IAM pour permettre à votre cluster Amazon Redshift d'accéder AWS services

Pour créer un rôle IAM afin d'autoriser votre cluster Amazon Redshift à communiquer avec d'autres services AWS en votre nom, procédez comme suit. Les valeurs utilisées dans cette section sont des exemples. Vous pouvez choisir des valeurs en fonction de vos besoins.

Pour créer un rôle IAM permettant à Amazon Redshift d'accéder AWS services

1. Ouvrez la console IAM.
2. Dans le panneau de navigation, choisissez Rôles.
3. Sélectionnez Create role (Créer un rôle).
4. Choisissez Service AWS , puis Redshift.
5. Sous Sélectionner votre cas d'utilisation, choisissez Redshift - Personnalisable, puis Suivant : Autorisations. La page Attacher une politique d'autorisations s'affiche.
6. Pour accéder à Amazon S3 à l'aide de COPY, par exemple, vous pouvez utiliser **`AmazonS3ReadOnlyAccess`** et l'ajouter. Pour accéder à Amazon S3 à l'aide de COPY ou UNLOAD, nous vous suggérons de créer des politiques gérées qui restreignent l'accès au compartiment souhaité et utilisent les préfixes appropriés en conséquence. Pour les opérations de lecture et d'écriture, nous vous recommandons d'appliquer les moindres privilèges, ainsi que de restreindre uniquement les compartiments Amazon S3 et les préfixes de clé requis par Amazon Redshift.

   Pour accéder à l'appel des fonctions Lambda pour la commande CREATE EXTERNAL FUNCTION, ajoutez **`AWSLambdaRole`**.

   Pour Redshift Spectrum, en plus de l'accès à Amazon S3, ajoutez **`AWSGlueConsoleFullAccess`** ou **`AmazonAthenaFullAccess`**.

   Choisissez Suivant : Balises.

7. La page Ajouter des balises s'affiche. Si vous le souhaitez, vous pouvez ajouter des balises. Choisissez Suivant : Vérification.
8. Pour Nom du rôle, indiquez le nom de votre rôle, par exemple **`RedshiftCopyUnload`**. Sélectionnez Create role (Créer un rôle).
9. Le nouveau rôle est disponible pour tous les utilisateurs des clusters qui utilisent ce rôle. Pour limiter l'accès à des utilisateurs spécifiques uniquement sur certains clusters, ou sur des clusters dans des régions spécifiques, modifiez la relation d'approbation de ce rôle. Pour plus d'informations, consultez Restriction de l'accès aux rôles IAM.
10. Associez le rôle à votre cluster. Vous pouvez associer un rôle IAM à un cluster lors de la création du cluster, ou vous pouvez ajouter le rôle à un cluster existant. Pour plus d'informations, consultez Association des rôles IAM aux clusters.

> **Note**
>
> Pour restreindre l'accès à des données spécifiques, utilisez un rôle IAM qui accorde les moindres privilèges requis.

Restriction de l'accès aux rôles IAM

Par défaut, les rôles IAM qui sont disponibles pour un cluster Amazon Redshift sont disponibles pour tous les utilisateurs de ce cluster. Vous pouvez choisir de restreindre les rôles IAM à des utilisateurs de base de données Amazon Redshift spécifiques sur des clusters spécifiques ou à des régions spécifiques.

Pour permettre uniquement aux utilisateurs de base de données spécifiques d'utiliser un rôle IAM, procédez comme suit.

Pour identifier les utilisateurs de base de données spécifiques avec accès à un rôle IAM

1. Identifiez l'Amazon Resource Name (ARN) pour les utilisateurs de base de données de votre cluster Amazon Redshift. L'ARN d'un utilisateur de base de données est au format : `arn:aws:redshift:`*`region`*`:`*`account-id`*`:dbuser:`*`cluster-name`*`/`*`user-name`*.

   Pour Amazon Redshift sans serveur, utilisez le format ARN suivant. `arn:aws:redshift:`*`region`*`:`*`account-id`*`:dbuser:serverless-`*`account-id`*`-`*`workgroup-id`*`/`*`user-name`*
2. Ouvrez la console IAM.

3. Dans le panneau de navigation, choisissez Rôles.
4. Sélectionnez le rôle IAM de votre choix pour restreindre l'accès aux utilisateurs de base de données Amazon Redshift spécifiques.
5. Choisissez l'onglet Relations d'approbation, puis Modifier la relation d'approbation. Un nouveau rôle IAM qui permet à Amazon Redshift d'accéder à d'autres AWS services en votre nom repose sur la relation de confiance suivante :

   JSON

   ```
   {
     "Version":"2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
           "Service": "redshift.amazonaws.com"
         },
         "Action": "sts:AssumeRole"
       }
     ]
   }
   ```

6. Ajoutez une condition à la section action `sts:AssumeRole` de la relation d'approbation qui limite le champ `sts:ExternalId` aux valeurs que vous spécifiez. Incluez un ARN pour chaque utilisateur de base de données auquel vous voulez accorder l'accès au rôle. L'ID externe peut être n'importe quelle chaîne unique.

   Par exemple, la relation d'approbation suivante spécifie seuls les utilisateurs de base de données `user1` et `user2` sur le cluster `my-cluster` de la région `us-west-2` ont l'autorisation d'utiliser ce rôle IAM.

   JSON

   ```
   {
     "Version":"2012-10-17",
     "Statement": [
     {
       "Effect": "Allow",
       "Principal": {
   ```

```
      "Service": "redshift.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "sts:ExternalId": [
          "arn:aws:redshift:us-west-2:123456789012:dbuser:my-cluster/user1",
          "arn:aws:redshift:us-west-2:123456789012:dbuser:my-cluster/user2"
        ]
      }
    }
  }]
}
```

7. Choisissez Mettre à jour la politique d'approbation.

Restreindre un rôle IAM à AWS Région

Vous pouvez restreindre l'accès à un rôle IAM uniquement dans une AWS région donnée. Par défaut, les rôles IAM pour Amazon Redshift ne sont pas limités à une seule région.

Pour limiter l'utilisation d'un rôle IAM par région, procédez comme suit.

Pour identifier les régions autorisées pour un rôle IAM

1. Ouvrez la console IAM à https://console.aws.amazon.com/ l'adresse.
2. Dans le panneau de navigation, choisissez Rôles.
3. Sélectionnez le rôle de votre choix pour modifier à l'aide de régions spécifiques.
4. Choisissez l'onglet Relations d'approbation, puis Modifier la relation d'approbation. Un nouveau rôle IAM qui permet à Amazon Redshift d'accéder à d'autres AWS services en votre nom repose sur la relation de confiance suivante :

   JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

5. Modifiez la liste `Service` pour `Principal` avec la liste des régions spécifiques pour lesquelles vous voulez permettre l'utilisation du rôle. Chaque région de la liste `Service` doit être au format suivant : `redshift.`*`region`*`.amazonaws.com`.

   Par exemple, la relation d'approbation modifiée suivante permet d'utiliser le rôle IAM dans les régions `us-east-1` et `us-west-2` uniquement.

   JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift.us-east-1.amazonaws.com",
          "redshift.us-west-2.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

6. Choisissez Mettre à jour la politique de confiance

Chaînage des rôles IAM dans Amazon Redshift

Lorsque vous attachez un rôle à votre cluster, celui-ci peut assumer ce rôle pour accéder à Amazon S3, Amazon Athena et en votre AWS Lambda nom. AWS Glue Si un rôle attaché à votre cluster n’a pas accès aux ressources nécessaires, vous pouvez créer une chaîne avec un autre rôle, lequel peut appartenir à un autre compte. Votre cluster endosse alors provisoirement le rôle relié par la chaîne afin d’accéder aux données. Vous pouvez également accorder des accès entre comptes en

créant des chaînes de rôles. Chaque rôle de la chaîne passe au rôle suivant, jusqu'à ce que le cluster endosse le dernier rôle de la chaîne. Le nombre maximal de rôles IAM que vous pouvez associer est soumis à un quota. Pour plus d'informations, consultez le quota « Rôles IAM de cluster pour Amazon Redshift afin d'accéder à d'autres AWS services » dans. Quotas pour les objets Amazon Redshift

> **Note**
>
> Vous devez spécifier les rôles IAM pour que la chaîne fonctionne correctement.

Par exemple, supposons que la société A souhaite accéder aux données d'un compartiment Amazon S3 appartenant à l'entreprise B. L'entreprise A crée un rôle de AWS service nommé pour Amazon Redshift `RoleA` et l'associe à son cluster. L'entreprise B crée un rôle nommé `RoleB` qui est autorisé à accéder aux données du compartiment de l'entreprise B. Pour accéder aux données dans le compartiment de l'entreprise B, l'entreprise A exécute une commande COPY à l'aide d'un paramètre `iam_role` qui relie par chaîne `RoleA` et `RoleB`. Pendant la durée de l'opération COPY, `RoleA` endosse temporairement `RoleB` pour accéder au compartiment Amazon S3.

Pour créer une chaîne de rôles, vous devez établir une relation d'approbation entre ces rôles. Un rôle qui endosse un autre rôle (par exemple, `RoleA`) doit disposer d'une politique d'autorisations qui l'autorise à endosser le rôle relié par la chaîne suivant (par exemple, `RoleB`). De même, le rôle qui transmet les autorisations (`RoleB`) doit avoir une politique d'approbation lui permettant de transmettre ses autorisations au rôle relié par la chaîne précédent (`RoleA`). Pour plus d'informations, consultez la rubrique Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Le premier rôle de la chaîne doit être attaché au cluster. Le premier rôle, et chaque rôle ultérieur qui endosse le rôle suivant dans la chaîne, doivent avoir une politique incluant une déclaration spécifique. Cette déclaration comprend l'effet `Allow` sur l'action `sts:AssumeRole` ainsi que l'Amazon Resource Name (ARN) du rôle suivant dans un élément `Resource`. Dans notre exemple, `RoleA` comporte la politique d'autorisation suivante, qui l'autorise à endosser `RoleB`, appartenant au compte AWS `210987654321`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "Stmt1487639602000",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/RoleB"
        }
    ]
}
```

Un rôle qui passe à un autre rôle doit établir une relation de confiance avec le rôle qui assume le rôle ou avec le AWS compte propriétaire du rôle. Dans notre exemple, `RoleB` possède la politique d'approbation suivante pour établir une relation d'approbation avec `RoleA`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/RoleA"
      }
    }
  ]
}
```

La politique de confiance suivante établit une relation de confiance avec le propriétaire du `RoleA` AWS compte`123456789012`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      }
    }
  ]
}
```

> **Note**
>
> Pour restreindre l'autorisation de chaînage de rôles à des utilisateurs spécifiques, définissez une condition. Pour plus d'informations, consultez Restriction de l'accès aux rôles IAM.

Lorsque vous exécutez une commande UNLOAD, COPY, CREATE EXTERNAL FUNCTION ou CREATE EXTERNAL SCHEMA, vous enchaînez les rôles en incluant une liste d'ARN de rôles, séparés par des virgules, dans le paramètre `iam_role`. L'exemple suivant montre la syntaxe d'une chaîne de rôles dans le paramètre `iam_role`.

```
unload ('select * from venue limit 10')
to 's3://acmedata/redshift/venue_pipe_'
IAM_ROLE 'arn:aws:iam::<aws-account-id-1>:role/<role-name-1>[,arn:aws:iam::<aws-account-id-2>:role/<role-name-2>][,...]';
```

> **Note**
>
> L'intégralité de la chaîne de rôle est placée entre guillemets simples et ne doit pas contenir d'espaces.

Dans les exemples suivants, `RoleA` est attaché au cluster appartenant au compte AWS `123456789012`. `RoleB`, qui appartient au compte `210987654321`, a l'autorisation d'accéder au compartiment nommé `s3://companyb/redshift/`. L'exemple suivant permet d'`RoleA`enchaîner et `RoleB` de DÉCHARGER les données dans le compartiment s3 ://companyb/redshift/.

```
unload ('select * from venue limit 10')
to 's3://companyb/redshift/venue_pipe_'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

L'exemple suivant utilise une commande COPY pour charger les données qui ont été déchargées dans l'exemple précédent.

```
copy venue
from 's3://companyb/redshift/venue_pipe_'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

Dans l'exemple suivant, CREATE EXTERNAL SCHEMA utilise des rôles reliés par chaîne pour endosser le rôle `RoleB`.

```
create external schema spectrumexample from data catalog
database 'exampledb' region 'us-west-2'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

Dans l'exemple suivant, CREATE EXTERNAL FUNCTION utilise des rôles reliés par chaîne pour endosser le rôle `RoleB`.

```
create external function lambda_example(varchar)
returns varchar
volatile
lambda 'exampleLambdaFunction'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

Autorisation des opérations COPY, UNLOAD, CREATE EXTERNAL FUNCTION et CREATE EXTERNAL SCHEMA à l'aide des rôles IAM

Vous pouvez utiliser la commande COPY pour charger (ou importer) des données dans Amazon Redshift et la commande UNLOAD pour décharger (ou exporter) des données depuis Amazon Redshift. Vous pouvez utiliser la commande CREATE EXTERNAL FUNCTION pour créer des fonctions définies par l'utilisateur qui invoquent des fonctions depuis. AWS Lambda

Lorsque vous utilisez Amazon Redshift Spectrum, vous utilisez la commande CREATE EXTERNAL SCHEMA pour spécifier l'emplacement d'un compartiment Amazon S3 qui contient vos données. Lorsque vous exécutez les commandes COPY, UNLOAD ou CREATE EXTERNAL SCHEMA, vous fournissez des informations d'identification de sécurité. Ces informations d'identification autorisent votre cluster Amazon Redshift à lire ou écrire des données vers et depuis votre destination cible, comme un compartiment Amazon S3.

Lorsque vous exécutez CREATE EXTERNAL FUNCTION, vous fournissez des informations d'identification de sécurité à l'aide du paramètre de rôle IAM. Ces informations d'identification

autorisent votre cluster Amazon Redshift à invoquer des fonctions Lambda depuis. AWS Lambda La méthode préférée pour fournir des informations d'identification de sécurité consiste à spécifier un rôle Gestion des identités et des accès AWS (IAM). Pour COPY et UNLOAD, vous pouvez fournir des informations d'identification temporaires. Pour plus d'informations sur la création d'un rôle IAM, consultez Autorisation d'accès à Amazon Redshift AWS services en votre nom.

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec des AWS personnes extérieures au Console de gestion AWS. La manière d'accorder l'accès par programmation dépend du type d'utilisateur qui accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Recommandé) Utilisez les informations d'identification de la console comme informations d'identification temporaires pour signer les AWS CLI demandes programmatiques adressées aux AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, consultez la section Connexion pour le développement AWS local dans le Guide de AWS Command Line Interface l'utilisateur. • Pour les AWS kits de développement, consultez la section Connexion pour le développement AWS local dans le Guide de référence AWS des kits de développement logiciel et des outils.
Identité de la main-d'œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées	Suivez les instructions de l'interface que vous souhaitez utiliser.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
	aux AWS CLI AWS SDK ou AWS aux API.	• Pour cela AWS CLI, reportez-vous AWS CLI à la section Configuration de l'utilisation AWS IAM Identity Center dans le Guide de AWS Command Line Interface l'utilisateur. • Pour les AWS kits de développement logiciel, les outils et les AWS API, consultez la section Authentification IAM Identity Center dans le Guide de référence AWS des kits de développement logiciel et des outils.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de la section Utilisation des informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer des demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour cela AWS CLI, consultez la section Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS kits de développement logiciel et les outils, consultez la section Authentification à l'aide d'informations d'identification à long terme dans le Guide de référence AWS des kits de développement logiciel et des outils. • Pour les AWS API, consultez la section Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Les étapes de l'utilisation d'un rôle IAM sont les suivantes :

- Créer un rôle IAM à utiliser avec votre cluster Amazon Redshift.
- Associer le rôle IAM au cluster.
- Incluez l'ARN du rôle IAM lorsque vous appelez la commande COPY, UNLOAD, CREATE EXTERNAL SCHEMA ou CREATE EXTERNAL FUNCTION.

Association des rôles IAM aux clusters

Après avoir créé un rôle IAM qui autorise Amazon Redshift à accéder à d'autres services AWS pour vous, vous devez associer ce rôle à un cluster Amazon Redshift. Vous devez le faire avant de pouvoir utiliser le rôle pour charger ou décharger des données.

Autorisations requises pour associer un rôle IAM à un cluster

Pour associer un rôle IAM à un cluster, un utilisateur doit avoir l'autorisation `iam:PassRole` pour ce rôle IAM. Cette autorisation permet à un administrateur de restreindre les rôles IAM qu'un utilisateur peut associer aux clusters Amazon Redshift. Il est recommandé d'associer des politiques d'autorisation à un rôle IAM, puis de l'attribuer à des utilisateurs et à des groupes, le cas échéant. Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift.

L'exemple suivant illustre une politique IAM qui peut être attachée à un utilisateur et qui permet à l'utilisateur d'exécuter ces actions :

- Obtenez les détails de tous les clusters Amazon Redshift détenus par ce compte d'utilisateur.
- Associez l'un des trois rôles IAM à l'un ou l'autre des deux clusters Amazon Redshift.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "redshift:DescribeClusters",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "redshift:ModifyClusterIamRoles",
                 "redshift:CreateCluster"
            ],
            "Resource": [
                 "arn:aws:redshift:us-east-1:123456789012:cluster:my-redshift-
cluster",
                 "arn:aws:redshift:us-east-1:123456789012:cluster:my-second-
redshift-cluster"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::123456789012:role/MyRedshiftRole",
                "arn:aws:iam::123456789012:role/SecondRedshiftRole",
                "arn:aws:iam::123456789012:role/ThirdRedshiftRole"
             ]
        }
    ]
}
```

Une fois qu'un utilisateur dispose des autorisations appropriées, cet utilisateur peut associer un rôle IAM à un cluster Amazon Redshift. Le rôle IAM est ensuite prêt à utiliser la commande COPY ou UNLOAD, ou d'autres commandes Amazon Redshift.

Pour plus d'informations sur les politiques IAM, consultez Présentation des politiques IAM dans le Guide de l'utilisateur IAM.

Gestion de l'association d'un rôle IAM à un cluster

Vous pouvez associer un rôle IAM à un cluster Amazon Redshift lorsque vous créez le cluster. Ou vous pouvez modifier un cluster existant ou ajouter ou supprimer une ou plusieurs associations de rôle IAM.

Tenez compte des points suivants :

- Le nombre maximal de rôles IAM que vous pouvez associer est soumis à un quota.
- Un rôle IAM peut être associé à plusieurs clusters Amazon Redshift.
- Un rôle IAM peut être associé à un cluster Amazon Redshift uniquement si le rôle IAM et le cluster appartiennent au même compte. AWS

Vous pouvez gérer les associations de rôle IAM d'un cluster avec la console à l'aide de la procédure suivante.

Pour gérer les associations de rôles IAM

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters, puis le cluster que vous souhaitez mettre à jour.
3. Pour Actions, choisissez Gérer les rôles IAM pour afficher la liste actuelle des rôles IAM associés au cluster.
4. Sur la page Gérer les rôles IAM, choisissez les rôles IAM à ajouter, puis Ajouter un rôle IAM.
5. Choisissez Terminé pour enregistrer les changements.

Vous pouvez gérer les associations de rôles IAM pour un cluster AWS CLI en utilisant les approches suivantes.

Pour associer un rôle IAM à un cluster lors de la création du cluster, spécifiez l'Amazon Resource Name (ARN) du rôle IAM comme paramètre `--iam-role-arns` de la commande `create-cluster`. Le nombre maximal de rôles IAM que vous pouvez ajouter lorsque vous appelez la commande `create-cluster` est soumis à un quota.

L'association et la dissociation des rôles IAM avec les clusters Amazon Redshift constitue un processus asynchrone. Vous pouvez obtenir le statut de toutes les associations de rôle IAM et de cluster en appelant la commande `describe-clusters`.

L'exemple suivant associe deux rôles IAM avec le cluster nouvellement créé nommé `my-redshift-cluster`.

```
aws redshift create-cluster \
    --cluster-identifier "my-redshift-cluster" \
    --node-type "ra3.4xlarge" \
    --number-of-nodes 16 \
    --iam-role-arns "arn:aws:iam::123456789012:role/RedshiftCopyUnload" \
                    "arn:aws:iam::123456789012:role/SecondRedshiftRole"
```

Pour associer un rôle IAM à un cluster Amazon Redshift existant, spécifiez l'Amazon Resource Name (ARN) du rôle IAM comme paramètre `--add-iam-roles` de la commande `modify-cluster-iam-roles`. Le nombre maximal de rôles IAM que vous pouvez ajouter lorsque vous appelez la commande `modify-cluster-iam-roles` est soumis à un quota.

L'exemple suivant associe un rôle IAM à un cluster existant nommé `my-redshift-cluster`.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier "my-redshift-cluster" \
    --add-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

Pour dissocier un rôle IAM d'un cluster, spécifiez l'ARN du rôle IAM comme paramètre `--remove-iam-roles` de la commande `modify-cluster-iam-roles`. `modify-cluster-iam-roles` Le nombre maximal de rôles IAM que vous pouvez supprimer lorsque vous appelez la commande `modify-cluster-iam-roles` est soumis à un quota.

L'exemple suivant supprime l'association d'un rôle IAM pour le `123456789012` AWS compte d'un cluster nommé`my-redshift-cluster`.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier "my-redshift-cluster" \
    --remove-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

Répertorier les associations de rôles IAM pour un cluster à l'aide du AWS CLI

Pour afficher tous les rôles IAM associés à un cluster Amazon Redshift et l'état de l'association de rôle IAM, appelez la commande `describe-clusters`. L'ARN de chaque rôle IAM associé au cluster est retourné dans la liste `IamRoles` comme illustré dans l'exemple de sortie suivant.

Les rôles qui ont été associés au cluster affichent l'état `in-sync`. Les rôles qui sont en cours d'association au cluster affichent l'état `adding`. Les rôles qui sont en cours de dissociation du cluster affichent l'état `removing`.

```
{
    "Clusters": [
        {
            "ClusterIdentifier": "my-redshift-cluster",
            "NodeType": "ra3.4xlarge",
            "NumberOfNodes": 16,
            "IamRoles": [
                {
                    "IamRoleArn": "arn:aws:iam::123456789012:role/MyRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                },
```

```
                {
                    "IamRoleArn": "arn:aws:iam::123456789012:role/SecondRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                }
            ],
            ...
        },
        {
            "ClusterIdentifier": "my-second-redshift-cluster",
            "NodeType": "ra3.4xlarge",
            "NumberOfNodes": 10,
            "IamRoles": [
                {
                    "IamRoleArn": "arn:aws:iam::123456789012:role/MyRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                },
                {
                    "IamRoleArn": "arn:aws:iam::123456789012:role/SecondRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                },
                {
                    "IamRoleArn": "arn:aws:iam::123456789012:role/ThirdRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                }
            ],
            ...
        }
    ]
}
```

Pour plus d'informations sur l'utilisation du AWS CLI, consultez le Guide de AWS CLI l'utilisateur .

Création d'un rôle IAM par défaut pour Amazon Redshift

Lorsque vous créez des rôles IAM via la console Redshift, Amazon Redshift crée les rôles par programmation dans votre environnement Compte AWS et y associe automatiquement les politiques gérées existantes AWS . Cette approche signifie que vous pouvez rester dans la console Redshift et que vous n'avez pas besoin de passer à la console IAM pour créer des rôles. Pour un contrôle plus détaillé des autorisations pour un rôle IAM existant créé dans la console Amazon Redshift, vous pouvez attacher une politique gérée personnalisée au rôle IAM.

Rôles IAM créés dans la console

Lorsque vous utilisez la console Amazon Redshift pour créer des rôles IAM, Amazon Redshift suit tous les rôles IAM créés via la console. Amazon Redshift présélectionne le rôle IAM par défaut le plus récent pour créer tous les clusters et restaurer des clusters à partir d'instantanés.

Vous pouvez créer un rôle IAM via la console disposant d'une politique avec les autorisations nécessaires pour exécuter des commandes SQL. Ces commandes incluent COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL TABLE, CREATE EXTERNAL SCHEMA, CREATE MODEL ou CREATE LIBRARY. Vous pouvez également obtenir un contrôle plus détaillé de l'accès des utilisateurs à vos ressources AWS en créant et en attachant des politiques personnalisées au rôle IAM.

Lorsque vous avez créé un rôle IAM et que vous le définissez comme rôle par défaut pour le cluster à l'aide de la console, vous n'avez pas besoin de fournir l'Amazon Resource Name (ARN) du rôle IAM pour effectuer l'authentification et l'autorisation.

Le rôle IAM que vous créez via la console pour votre cluster a la politique gérée `AmazonRedshiftAllCommandsFullAccess` attachée automatiquement. Ce rôle IAM permet à Amazon Redshift de copier, de décharger, d'interroger et d'analyser les données relatives aux AWS ressources de votre compte IAM. La politique gérée permet d'accéder aux opérations COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL SCHEMA, CREATE MODEL et CREATE LIBRARY. La politique accorde également l'autorisation d'exécuter des instructions SELECT pour AWS des services connexes, tels qu'Amazon S3, Amazon CloudWatch Logs, Amazon SageMaker AI et AWS Glue.

Les commandes CREATE EXTERNAL FUNCTION, CREATE EXTERNAL SCHEMA, CREATE MODEL et CREATE LIBRARY possèdent un mot clé `default`. En ce qui concerne ce mot clé pour ces commandes, Amazon Redshift utilise le rôle IAM défini par défaut et associé au cluster lors de l'exécution de la commande. Vous pouvez exécuter la commande DEFAULT_IAM_ROLE pour vérifier le rôle IAM par défaut actuel attaché au cluster.

Pour contrôler les privilèges d'accès du rôle IAM créé et défini par défaut pour votre cluster Redshift, utilisez le privilège ASSUMEROLE. Ce contrôle d'accès s'applique aux utilisateurs et aux groupes de bases de données lorsqu'ils exécutent des commandes telles que celles répertoriées précédemment. Après avoir accordé le privilège ASSUMEROLE à un utilisateur ou un groupe pour un rôle IAM, l'utilisateur ou le groupe peut assumer ce rôle lors de l'exécution de ces commandes. Le privilège ASSUMEROLE vous permet d'accorder l'accès aux commandes appropriées selon vos besoins.

Vous pouvez effectuer les actions suivantes à l'aide de la console Amazon Redshift :

- Création d'un rôle IAM comme rôle IAM par défaut
- Suppression de rôles IAM de votre cluster
- Association de rôles IAM à votre cluster
- Définition d'un rôle IAM comme rôle par défaut
- Faire en sorte qu'un rôle IAM ne soit plus par défaut pour votre cluster

Autorisations de la politique AmazonRedshiftAllCommandsFullAccess gérée

L'exemple suivant illustre les autorisations dans la politique gérée `AmazonRedshiftAllCommandsFullAccess` qui autorise certaines actions pour le rôle IAM défini par défaut pour votre cluster. Le rôle IAM avec des politiques d'autorisation attachées autorise les actions pouvant être effectuées ou non par un utilisateur ou un groupe. Compte tenu de ces autorisations, vous pouvez exécuter la commande COPY depuis Amazon S3, exécuter la commande UNLOAD et utiliser la commande CREATE MODEL.

```
{
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetBucketAcl",
                "s3:GetBucketCors",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:PutBucketCors",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload",
                "s3:CreateBucket"
            ],
            "Resource": [
                "arn:aws:s3:::redshift-downloads",
                "arn:aws:s3:::redshift-downloads/*",
                "arn:aws:s3:::*redshift*",
                "arn:aws:s3:::*redshift*/*"
            ]
```

```
}
```

L'exemple suivant illustre les autorisations de la politique gérée `AmazonRedshiftAllCommandsFullAccess` qui autorise certaines actions pour le rôle IAM défini par défaut pour le cluster. Le rôle IAM avec des politiques d'autorisation attachées autorise les actions pouvant être effectuées ou non par un utilisateur ou un groupe. Compte tenu des autorisations suivantes, vous pouvez exécuter la commande CREATE EXTERNAL FUNCTION.

```
{
    "Action": [
        "lambda:InvokeFunction"
    ],
    "Resource": "arn:aws:lambda:*:*:function:*redshift*"
}
```

L’exemple suivant illustre les autorisations de la politique gérée `AmazonRedshiftAllCommandsFullAccess` qui autorise certaines actions pour le rôle IAM défini par défaut pour le cluster. Le rôle IAM avec des politiques d'autorisation attachées autorise les actions pouvant être effectuées ou non par un utilisateur ou un groupe. Compte tenu des autorisations suivantes, vous pouvez exécuter les commandes CREATE EXTERNAL SCHEMA et CREATE EXTERNAL TABLE nécessaires pour Amazon Redshift Spectrum.

```
{
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:DeleteDatabase",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:DeleteTable",
                "glue:BatchDeleteTable",
                "glue:UpdateTable",
                "glue:GetTable",
                "glue:GetTables",
                "glue:BatchCreatePartition",
                "glue:CreatePartition",
                "glue:DeletePartition",
                "glue:BatchDeletePartition",
                "glue:UpdatePartition",
```

```
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:BatchGetPartition"
            ],
            "Resource": [
                "arn:aws:glue:*:*:table/*redshift*/*",
                "arn:aws:glue:*:*:catalog",
                "arn:aws:glue:*:*:database/*redshift*"
            ]
}
```

L'exemple suivant illustre les autorisations de la politique gérée `AmazonRedshiftAllCommandsFullAccess` qui autorise certaines actions pour le rôle IAM défini par défaut pour le cluster. Le rôle IAM avec des politiques d'autorisation attachées autorise les actions pouvant être effectuées ou non par un utilisateur ou un groupe. Compte tenu des autorisations suivantes, vous pouvez exécuter la commande CREATE EXTERNAL SCHEMA à l'aide de requêtes fédérées.

```
{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetResourcePolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret",
                "secretsmanager:ListSecretVersionIds"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:*Redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetRandomPassword",
                "secretsmanager:ListSecrets"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "secretsmanager:ResourceTag/Redshift": "true"
                }
            }
```

```
},
```

Gestion des rôles IAM créés pour un cluster à l'aide de la console

Pour créer, modifier et supprimer des rôles IAM créés à partir de la console Amazon Redshift, reportez-vous à la section Clusters dans la console.

Création d'un rôle IAM comme rôle IAM par défaut

Sur la console, vous pouvez créer un rôle IAM pour votre cluster avec la politique `AmazonRedshiftAllCommandsFullAccess` attachée automatiquement. Le nouveau rôle IAM que vous créez permet à Amazon Redshift de copier, de charger, d'interroger et d'analyser des données provenant des ressources Amazon dans votre compte IAM.

Il ne peut y avoir qu'un seul rôle IAM défini comme valeur par défaut pour le cluster. Si vous créez un autre rôle IAM en tant que rôle par défaut du cluster lorsqu'un rôle IAM existant est actuellement attribué par défaut, le nouveau rôle IAM remplace l'autre rôle comme valeur par défaut.

Pour créer un cluster et un rôle IAM défini comme valeur par défaut pour le nouveau cluster

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters. Les clusters actuels de votre compte Région AWS sont répertoriés. Un sous-ensemble des propriétés de chaque cluster s’affiche dans les colonnes de la liste.
3. Choisissez Créer un cluster pour créer un cluster.
4. Suivez les instructions sur la page de la console pour entrer les propriétés dans Configuration du cluster. Pour plus d’informations sur cette étape, consultez Création d’un cluster.
5. (Facultatif) Choisissez Load sample data (Chargement des exemples de données) pour charger l'exemple de jeu de données sur votre cluster Amazon Redshift afin de commencer à utiliser l'éditeur de requête pour interroger des données.

   Si vous êtes derrière un pare-feu, le port de la base de données doit être ouvert et accepter les connexions entrantes.
6. Suivez les instructions sur la page de la console pour entrer les propriétés dans Configurations de la base de données.
7. Sous Cluster permissions (Autorisations de cluster), depuis Manage IAM roles (Gérer les rôles IAM), choisissez Create IAM role (Créer un rôle IAM).

8. Spécifiez un compartiment Amazon S3 auquel le rôle IAM doit accéder en choisissant l'une des méthodes suivantes :

   - Choisissez No additional Amazon S3 bucket (Pas de compartiment Amazon S3 supplémentaire)pour créer le rôle IAM sans spécifier de compartiments Amazon S3 spécifiques.
   - Choisissez Any Amazon S3 bucket (N'importe quel compartiment Amazon S3)pour permettre aux utilisateurs qui ont accès à votre cluster Amazon Redshift d'accéder également à n'importe quel compartiment Amazon S3 et à son contenu dans votre Compte AWS.
   - Choisissez Specific Amazon S3 buckets (Compartiments Amazon S3 spécifiques) pour spécifier un ou plusieurs compartiments Amazon S3 auxquels le rôle IAM en cours de création est autorisé à accéder. Choisissez ensuite un ou plusieurs compartiments Amazon S3 dans le tableau.
9. Choisissez Create IAM role as default (Créer un rôle IAM par défaut). Amazon Redshift crée et définit automatiquement le rôle IAM comme rôle par défaut pour votre cluster.
10. Choisissez Créer un cluster pour créer le cluster. Le cluster peut prendre plusieurs minutes pour être prêt à être utilisé.

Suppression de rôles IAM de votre cluster

Vous pouvez supprimer un ou plusieurs rôles IAM de votre cluster.

Pour supprimer des rôles IAM de votre cluster

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters. Les clusters actuels de votre compte Région AWS sont répertoriés. Un sous-ensemble des propriétés de chaque cluster s’affiche dans les colonnes de la liste.
3. Choisissez le cluster pour lequel vous souhaitez supprimer le rôle IAM.
4. Sous Cluster permissions (Autorisations de cluster), choisissez un ou plusieurs rôles IAM que vous souhaitez supprimer du cluster.
5. Depuis Manage IAM roles (Gérer les rôles IAM), choisissez Remove IAM roles (Supprimer des rôles IAM).

Association de rôles IAM à votre cluster

Vous pouvez associer un ou plusieurs rôles IAM à votre cluster.

Pour associer des rôles IAM à votre cluster

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters. Les clusters actuels de votre compte Région AWS sont répertoriés. Un sous-ensemble des propriétés de chaque cluster s'affiche dans les colonnes de la liste.
3. Choisissez le cluster auquel vous souhaitez associer des rôles IAM.
4. Sous Cluster permissions (Autorisations de cluster), choisissez un ou plusieurs rôles IAM que vous souhaitez associer au cluster.
5. Depuis Manage IAM roles (Gérer les rôles IAM), choisissez Associate IAM roles (Associer des rôles IAM).
6. Choisissez un ou plusieurs rôles IAM à associer à votre cluster.
7. Ensuite, choisissez Associate IAM roles (Associer des rôles IAM).

Définition d'un rôle IAM comme rôle par défaut

Vous pouvez définir un rôle IAM comme rôle par défaut pour votre cluster.

Pour faire d'un rôle IAM le rôle par défaut de votre cluster

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters. Les clusters actuels de votre compte Région AWS sont répertoriés. Un sous-ensemble des propriétés de chaque cluster s'affiche dans les colonnes de la liste.
3. Choisissez le cluster pour lequel vous souhaitez définir un rôle IAM par défaut.
4. Sous Cluster permissions (Autorisations de cluster) depuis Associated IAM roles (Rôles IAM associés), choisissez un rôle IAM que vous souhaitez définir comme rôle par défaut pour le cluster.
5. Sous Set Default (Définir par défaut), choisissez Make default (Configuration par défaut).

6. À l'invite, choisissez Set Default (Définir par défaut) pour confirmer que le rôle IAM spécifié est défini par défaut.

Faire en sorte qu'un rôle IAM ne soit plus par défaut pour votre cluster

Vous pouvez faire en sorte qu'un rôle IAM ne soit plus le rôle par défaut de votre cluster.

Pour supprimer un rôle IAM comme rôle par défaut pour votre cluster

1. Connectez-vous à Console de gestion AWS et ouvrez la console Amazon Redshift à https://console.aws.amazon.com/redshiftv2/ l'adresse.
2. Dans le menu de navigation, choisissez Clusters. Les clusters actuels de votre compte Région AWS sont répertoriés. Un sous-ensemble des propriétés de chaque cluster s'affiche dans les colonnes de la liste.
3. Choisissez le cluster auquel vous souhaitez associer des rôles IAM.
4. Sous Cluster permissions (Autorisations de cluster), depuis Associated IAM roles (Rôles IAM associés), choisissez le rôle IAM par défaut.
5. Sous Set Default (Définir par défaut), choisissez Clear default (Effacer la valeur par défaut).
6. À l'invite, choisissez Clear default (Effacer la valeur par défaut) pour confirmer que le rôle IAM spécifié est effacé par défaut.

Gestion des rôles IAM créés sur le cluster à l'aide du AWS CLI

Vous pouvez gérer les rôles IAM créés sur le cluster à l'aide de la AWS CLI.

Pour créer un cluster Amazon Redshift avec un jeu de rôles IAM par défaut

Pour créer un cluster Amazon Redshift avec un rôle IAM, définissez-le comme valeur par défaut pour le cluster, utilisez la `aws redshift create-cluster` AWS CLI commande.

La AWS CLI commande suivante crée un cluster Amazon Redshift et le rôle IAM nommé myrole1. La AWS CLI commande définit également myrole1 comme valeur par défaut pour le cluster.

```
aws redshift create-cluster \
    --node-type dc2.large \
    --number-of-nodes 2 \
    --master-username adminuser \
    --master-user-password TopSecret1 \
    --cluster-identifier mycluster \
```

```
    --iam-roles 'arn:aws:iam::012345678910:role/myrole1'
 'arn:aws:iam::012345678910:role/myrole2' \
    --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole1'
```

L'extrait suivant représente un exemple de réponse.

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
        "NodeType": "dc2.large",
        "MasterUsername": "adminuser",
        "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
        "IamRoles": [
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
                "ApplyStatus": "adding"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
                "ApplyStatus": "adding"
            }
        ]
        ...
    }
}
```

Pour ajouter un ou plusieurs rôles IAM à un cluster Amazon Redshift

Pour ajouter un ou plusieurs rôles IAM associés au cluster, utilisez la `aws redshift modify-cluster-iam-roles` AWS CLI commande.

La AWS CLI commande suivante ajoute `myrole3` et `myrole4` au cluster.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --add-iam-roles 'arn:aws:iam::012345678910:role/myrole3'
 'arn:aws:iam::012345678910:role/myrole4'
```

L’extrait suivant représente un exemple de réponse.

```
{
    "Cluster": {
```

```
        "ClusterIdentifier": "mycluster",
        "NodeType": "dc2.large",
        "MasterUsername": "adminuser",
        "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
        "IamRoles": [
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
                "ApplyStatus": "in-sync"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
                "ApplyStatus": "in-sync"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole3",
                "ApplyStatus": "adding"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole4",
                "ApplyStatus": "adding"
            }
        ],
        ...
    }
}
```

Pour supprimer un ou plusieurs rôles IAM d'un cluster Amazon Redshift

Pour supprimer un ou plusieurs rôles IAM associés au cluster, utilisez la `aws redshift modify-cluster-iam-roles` AWS CLI commande.

La AWS CLI commande suivante supprime `myrole3` et `myrole4` retire du cluster.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --remove-iam-roles 'arn:aws:iam::012345678910:role/myrole3'
 'arn:aws:iam::012345678910:role/myrole4'
```

L’extrait suivant représente un exemple de réponse.

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
```

```
        "NodeType": "dc2.large",
        "MasterUsername": "adminuser",
        "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
        "IamRoles": [
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
                "ApplyStatus": "in-sync"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
                "ApplyStatus": "in-sync"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole3",
                "ApplyStatus": "removing"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole4",
                "ApplyStatus": "removing"
            }
        ],
        ...
    }
}
```

Pour définir un rôle IAM associé comme rôle par défaut pour le cluster

Pour définir un rôle IAM associé comme rôle par défaut pour le cluster, utilisez la `aws redshift modify-cluster-iam-roles` AWS CLI commande.

La AWS CLI commande suivante est définie `myrole2` comme valeur par défaut pour le cluster.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole2'
```

L'extrait suivant représente un exemple de réponse.

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
        "NodeType": "dc2.large",
        "MasterUsername": "adminuser",
```

```
        "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
        "IamRoles": [
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
                "ApplyStatus": "in-sync"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
                "ApplyStatus": "in-sync"
            }
        ],
        ...
    }
}
```

Pour définir un rôle IAM non associé comme rôle par défaut pour le cluster

Pour définir un rôle IAM non associé comme rôle par défaut pour le cluster, utilisez la `aws redshift modify-cluster-iam-roles` AWS CLI commande.

La AWS CLI commande suivante ajoute `myrole2` au cluster Amazon Redshift et la définit comme valeur par défaut pour le cluster.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --add-iam-roles 'arn:aws:iam::012345678910:role/myrole3' \
    --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole3'
```

L’extrait suivant représente un exemple de réponse.

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
        "NodeType": "dc2.large",
        "MasterUsername": "adminuser",
        "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole3",
        "IamRoles": [
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
                "ApplyStatus": "in-sync"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
```

```
                "ApplyStatus": "in-sync"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole3",
                "ApplyStatus": "adding"
            }
        ],
        ...
    }
}
```

Pour restaurer un cluster à partir d'un instantané et lui définir un rôle IAM comme rôle par défaut

Lorsque vous restaurez votre cluster à partir d'un instantané, vous pouvez associer un rôle IAM existant ou en créer un et le définir comme rôle par défaut pour le cluster.

Pour restaurer un cluster Amazon Redshift à partir d'un instantané et définir un rôle IAM comme rôle par défaut du cluster, utilisez la `aws redshift restore-from-cluster-snapshot` AWS CLI commande.

La AWS CLI commande suivante restaure le cluster à partir d'un instantané et la définit `myrole2` comme valeur par défaut pour le cluster.

```
aws redshift restore-from-cluster-snapshot \
    --cluster-identifier mycluster-clone \
    --snapshot-identifier my-snapshot-id
    --iam-roles 'arn:aws:iam::012345678910:role/myrole1'
 'arn:aws:iam::012345678910:role/myrole2' \
    --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole1'
```

L’extrait suivant représente un exemple de réponse.

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster-clone",
        "NodeType": "dc2.large",
        "MasterUsername": "adminuser",
        "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
        "IamRoles": [
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
                "ApplyStatus": "adding"
```

```
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
                "ApplyStatus": "adding"
            }
        ],
        ...
    }
}
```

Utilisation d'une identité fédérée pour gérer l'accès d'Amazon Redshift aux ressources locales et aux tables externes Amazon Redshift Spectrum

L'utilisation de la fédération d'identités AWS avec les informations d'identification fournies `GetDatabaseCredentials` peut simplifier l'autorisation et l'accès aux données locales et aux données externes. Dans ce didacticiel, nous vous montrons comment fournir un accès aux ressources grâce à la fédération AWS d'identités, au lieu d'utiliser un rôle IAM spécifique.

Actuellement, pour permettre aux utilisateurs d'accéder aux données externes qui se trouvent dans Amazon S3, vous créez un rôle IAM avec des autorisations définies dans une politique d'autorisations. Les utilisateurs auxquels le rôle est associé peuvent ensuite accéder aux données externes. Cela fonctionne, mais si vous souhaitez fournir des règles détaillées, par exemple rendre certaines colonnes indisponibles pour un utilisateur en particulier, vous devrez peut-être effectuer une configuration supplémentaire sur le schéma externe.

La fédération d'identités, avec les informations d'identification fournies par`GetDatabaseCredentials`, peut fournir un accès aux ressources Redshift Spectrum AWS Glue et fournir des règles IAM granulaires plus faciles à spécifier et à modifier. Cela facilite l'application d'un accès conforme à vos règles commerciales.

Les avantages de l'utilisation d'informations d'identification fédérées sont les suivants :

- Vous ne devez pas gérer les rôles IAM attachés à un cluster pour Redshift Spectrum.
- Les administrateurs de clusters peuvent créer un schéma externe accessible aux utilisateurs dans différents contextes IAM. Cela est utile, par exemple, pour effectuer un filtrage de colonnes sur une table, où différents consommateurs interrogent le même schéma externe et obtiennent des champs différents dans les enregistrements renvoyés.
- Vous pouvez interroger Amazon Redshift à l'aide d'un utilisateur disposant d'autorisations IAM, plutôt que d'un seul rôle.

Préparation d'une identité pour se connecter avec une identité fédérée

Avant de vous connecter avec une identité fédérée, vous devez effectuer plusieurs étapes préliminaires. Ces instructions supposent que vous disposez d'un schéma externe Redshift Spectrum existant qui fait référence à un fichier de données stocké dans un compartiment Amazon S3, et que le compartiment se trouve sur le même compte que votre cluster Amazon Redshift ou votre entrepôt des données Amazon Redshift Serverless.

1. Créez une identité IAM. Il peut s'agir d'un utilisateur ou d'un rôle IAM. Utilisez n'importe quel nom pris en charge par IAM.
2. Attachez des stratégies d'autorisation à une identité. Spécifiez chacune des valeurs suivantes :

   - `redshift:GetClusterCredentialsWithIAM` (pour un cluster provisionné Amazon Redshift)
   - `redshift-serverless:GetCredentials` (pour Amazon Redshift Serverless)

   Vous pouvez ajouter des autorisations avec l'éditeur de stratégies à l'aide de la console IAM.

   L'identité IAM nécessite également des autorisations pour accéder aux données externes. Accordez l'accès à Amazon S3 en ajoutant directement les politiques AWS gérées suivantes :

   - `AmazonS3ReadOnlyAccess`
   - `AWSGlueConsoleFullAccess`

   La dernière stratégie gérée est requise si vous utilisez AWS Glue pour préparer vos données externes. Pour plus d'informations sur les étapes à suivre pour accorder l'accès à Amazon Redshift Spectrum, consultez Créer un rôle IAM pour Amazon Redshift, qui fait partie du guide de démarrage pour Amazon Redshift et Redshift Spectrum. Il montre les étapes à suivre pour ajouter des politiques IAM afin d'accéder à Redshift Spectrum.
3. Configurez votre client SQL pour une connexion à Amazon Redshift. Utilisez le pilote JDBC Amazon Redshift et ajoutez les informations d'identification de votre utilisateur aux propriétés des informations d'identification de l'outil. Un client tel que SQL Workbench/J fonctionne bien pour cela. Définissez les propriétés étendues de connexion client suivantes :

   - AccessKeyID : identifiant de votre clé d'accès.
   - SecretAccessKey— Votre clé d'accès secrète. (Notez le risque de sécurité lié à la transmission de la clé secrète si vous n'utilisez pas le chiffrement.)

- SessionToken— Un ensemble d'informations d'identification temporaires pour un rôle IAM.
- GroupFederation – Définissez sur `true` si vous configurez une identité fédérée pour un cluster provisionné. Ne définissez pas ce paramètre si vous utilisez Amazon Redshift Serverless.
- LogLevel— Valeur entière au niveau du journal. Ce nom est facultatif.

4. Définissez l'URL du point de terminaison JDBC trouvé dans la console Amazon Redshift ou Amazon Redshift Serverless. Remplacez votre schéma d'URL par jdbc:redshift:iam: et utilisez cette mise en forme :

   - Format d'un cluster provisionné Amazon Redshift : `jdbc:redshift:iam://<cluster_id>.<unique_suffix>.<region>.redshift.amazonaws.com:<port>/<database_name>`

     Exemple : `jdbc:redshift:iam://test1.12345abcdefg.us-east-1.redshift.amazonaws.com:5439/dev`
   - Pour Amazon Redshift sans serveur : `jdbc:redshift:iam://<workgroup-name>.<account-number>.<aws-region>.redshift-serverless.amazonaws.com:5439:<port>/<database_name>`

     Exemple : `jdbc:redshift:iam://default.123456789012.us-east-1.redshift-serverless.amazonaws.com:5439/dev`

   Une fois que vous vous êtes connecté à la base de données pour la première fois à l'aide d'une identité IAM, Amazon Redshift crée automatiquement une identité Amazon Redshift portant le même nom, préfixée par `IAM:` pour un utilisateur ou par `IAMR:` pour un rôle IAM. Les étapes restantes de cette rubrique présentent des exemples pour un utilisateur.

   Si un utilisateur Redshift n'est pas créé automatiquement, vous pouvez en créer un en exécutant une instruction `CREATE USER`, en utilisant un compte administrateur, en spécifiant le nom d'utilisateur au format `IAM:<user name>`.

5. En tant qu'administrateur de votre cluster Amazon Redshift, accordez à l'utilisateur Redshift les autorisations requises pour accéder au schéma externe.

   ```
   GRANT ALL ON SCHEMA my_schema to "IAM:my_user";
   ```

   Pour permettre à votre utilisateur Redshift de créer des tables dans le schéma externe, il doit être propriétaire du schéma. Par exemple :

```
ALTER SCHEMA my_schema owner to "IAM:my_user";
```

6. Pour vérifier la configuration, exécutez une requête en tant qu'utilisateur, à l'aide du client SQL, une fois les autorisations accordées. Cet exemple de requête extrait des données d'une table externe.

```
SELECT * FROM my_schema.my_table;
```

Commencer à propager les identités et les autorisations vers Redshift Spectrum

Pour transmettre une identité fédérée à des tables externes d'interrogation, vous devez définir `SESSION` comme valeur pour le paramètre de requête `IAM_ROLE` de `CREATE EXTERNAL SCHEMA`. Les étapes suivantes montrent comment configurer et utiliser `SESSION` pour autoriser des requêtes sur le schéma externe.

1. Créez des tables locales et des tables externes. Tables externes cataloguées avec une tâche AWS Glue à cet effet.
2. Connectez-vous à Amazon Redshift à l'aide de votre identité IAM. Comme indiqué dans la section précédente, lorsque l'identité se connecte à Amazon Redshift, un utilisateur de base de données Redshift est créé. L'utilisateur est créé s'il n'existait pas auparavant. Si l'utilisateur est nouveau, l'administrateur doit lui accorder les autorisations nécessaires pour effectuer des tâches dans Amazon Redshift, telles que l'interrogation et la création de tables.
3. Connectez-vous à Redshift à l'aide de votre compte administrateur. Exécutez la commande pour créer un schéma externe à l'aide de la valeur `SESSION`.

```
create external schema spectrum_schema from data catalog
database '<my_external_database>'
region '<my_region>'
iam_role 'SESSION'
catalog_id '<my_catalog_id>';
```

Notez que `catalog_id` est défini dans ce cas. Il s'agit d'un nouveau paramètre ajouté à la fonctionnalité, car `SESSION` remplace un rôle spécifique.

Dans cet exemple, les valeurs de la requête imitent l'apparence des valeurs réelles.

```
create external schema spectrum_schema from data catalog
```

```
database 'spectrum_db'
region 'us-east-1'
iam_role 'SESSION'
catalog_id '123456789012'
```

La `catalog_id` valeur dans ce cas est votre identifiant de AWS compte.

4. Exécutez des requêtes pour accéder à vos données externes, en utilisant l'identité IAM à laquelle vous vous êtes connecté à l'étape 2. Par exemple :

```
select * from spectrum_schema.table1;
```

Dans ce cas, il `table1` peut s'agir, par exemple, de JSON-formatted données dans un fichier, dans un compartiment Amazon S3.

5. Si vous disposez déjà d'un schéma externe qui utilise un rôle IAM attaché à un cluster, pointant vers votre base de données ou votre schéma externe, vous pouvez soit remplacer le schéma existant et utiliser une identité fédérée comme indiqué dans ces étapes, soit en créer un nouveau.

`SESSION` indique que les informations d'identification fédérées sont utilisées pour interroger le schéma externe. Lorsque vous utilisez le paramètre de requête `SESSION`, assurez-vous de définir le `catalog_id`. Elle est obligatoire car elle pointe vers le catalogue de données utilisé pour le schéma. Précédemment, `catalog_id` a été extrait de la valeur attribuée à `iam_role`. Lorsque vous configurez la propagation des identités et des autorisations de cette manière, par exemple vers Redshift Spectrum, en utilisant des informations d'identification fédérées pour interroger un schéma externe, aucune autorisation au moyen d'un rôle IAM n'est requise.

Notes d’utilisation

Voici une erreur de connexion courante : Erreur IAM lors de la récupération des informations d'identification temporaires : impossible d'annuler la réponse d'exception à l'aide des filtres de déconnexion fournis. Cette erreur est due à l'existence d'un ancien pilote JDBC. La version minimale du pilote requise pour l'identité fédérée est 2.1.0.9. Vous pouvez obtenir le pilote JDBC en cliquant sur Télécharger le pilote JDBC Amazon Redshift, version 2.x.

Ressources supplémentaires

Ces liens fournissent des informations supplémentaires pour gérer l'accès aux données externes.

- Vous pouvez toujours accéder aux données Redshift Spectrum à l'aide d'un rôle IAM. Pour plus d'informations, consultez Autorisation d'accès à Amazon Redshift AWS services en votre nom.
- Lorsque vous gérez l'accès à des tables externes avec AWS Lake Formation, vous pouvez les interroger à l'aide de Redshift Spectrum avec des identités IAM fédérées. Vous ne devez plus gérer les rôles IAM attachés à un cluster pour que Redshift Spectrum interroge les données enregistrées avec AWS Lake Formation. Pour en savoir plus, consultez Utilisation d' AWS Lake Formation avec Amazon Redshift Spectrum.

Gestion des mots de passe d'administration Amazon Redshift à l'aide de AWS Secrets Manager

Amazon Redshift peut s'intégrer AWS Secrets Manager pour générer et gérer vos informations d'identification d'administrateur dans un secret crypté. Avec AWS Secrets Manager, vous pouvez remplacer vos mots de passe d'administrateur par un appel d'API pour récupérer le secret par programmation lorsque cela est nécessaire. L'utilisation de secrets à la place d'informations d'identification codées en dur réduit le risque de divulgation ou de compromission de ces informations d'identification. Pour plus d'informations AWS Secrets Manager, consultez le guide de AWS Secrets Manager l'utilisateur.

Vous pouvez spécifier qu'Amazon Redshift gère votre mot de passe d'administrateur AWS Secrets Manager lorsque vous effectuez l'une des opérations suivantes :

- Créer un cluster alloué ou d'un espace de noms sans serveur
- Modifier ou mettre à jour les informations d'identification d'administrateur d'un cluster alloué ou d'un espace de noms sans serveur
- Restaurer un cluster ou d'un espace de noms sans serveur à partir d'un instantané

Lorsque vous spécifiez qu'Amazon Redshift gère le mot de passe administrateur dans AWS Secrets Manager, Amazon Redshift génère le mot de passe et le stocke dans Secrets Manager. Vous pouvez accéder au secret directement AWS Secrets Manager pour récupérer les informations d'identification de l'utilisateur administrateur. Vous pouvez éventuellement spécifier une clé gérée par le client pour chiffrer le secret si vous devez accéder au secret depuis un autre AWS compte. Vous pouvez également utiliser la clé KMS qui AWS Secrets Manager fournit.

Amazon Redshift gère les paramètres du secret et effectue la rotation du secret tous les 30 jours, par défaut. Vous pouvez effectuer la rotation du secret manuellement à tout moment. Si vous

supprimez un cluster provisionné ou un espace de noms sans serveur qui gère un secret dans AWS Secrets Manager, le secret et les métadonnées associées sont également supprimés.

Pour vous connecter à un cluster ou à un espace de noms sans serveur avec des informations d'identification gérées par secret, vous pouvez récupérer le secret à l'aide de la console AWS Secrets Manager Secrets Manager ou de l'appel d'API `GetSecretValue` Secrets Manager. Pour plus d'informations, voir Extraire des secrets depuis une base de données SQL AWS Secrets Manager et Se connecter à une base de données SQL avec des informations d'identification inscrites dans un AWS Secrets Manager secret dans le Guide de AWS Secrets Manager l'utilisateur.

Autorisations requises pour AWS Secrets Manager intégration

Les utilisateurs doivent disposer des autorisations requises pour effectuer des opérations liées à l'intégration d' AWS Secrets Manager . Créez des politiques IAM qui accordent des autorisations pour effectuer des opérations d'API spécifiques sur les ressources spécifiées dont elles ont besoin. Attachez ensuite ces politiques aux jeux d'autorisations ou rôles IAM qui requièrent ces autorisations. Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Redshift.

L'utilisateur qui indique qu'Amazon Redshift gère le mot de passe administrateur AWS Secrets Manager doit être autorisé à effectuer les opérations suivantes :

- `secretsmanager:CreateSecret`
- `secretsmanager:RotateSecret`
- `secretsmanager:DescribeSecret`
- `secretsmanager:UpdateSecret`
- `secretsmanager:DeleteSecret`
- `secretsmanager:GetRandomPassword`
- `secretsmanager:TagResource`

Si l'utilisateur souhaite transmettre une clé KMS dans le paramètre `MasterPasswordSecretKmsKeyId` pour les clusters provisionnés, ou dans le paramètre `AdminPasswordSecretKmsKeyId` pour les espaces de noms sans serveur, il a besoin des autorisations suivantes en plus des autorisations répertoriées ci-dessus.

- `kms:Decrypt`

- `kms:GenerateDataKey`
- `kms:CreateGrant`
- `kms:RetireGrant`

Rotation secrète des mots de passe administrateur

Par défaut, Amazon Redshift effectue la rotation automatique de votre secret tous les 30 jours afin de garantir que vos informations d'identification ne restent pas les mêmes pendant de longues périodes. Lorsqu'Amazon Redshift change le secret d'un mot de passe administrateur, AWS Secrets Manager met à jour le secret existant pour qu'il contienne un nouveau mot de passe administrateur. Amazon Redshift modifie le mot de passe d'administrateur du cluster afin qu'il corresponde au mot de passe indiqué dans le secret mis à jour.

Vous pouvez effectuer immédiatement la rotation d'un secret au lieu d'attendre une rotation planifiée en utilisant AWS Secrets Manager. Pour plus d'informations sur la rotation des secrets, consultez Rotation des secrets AWS Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager .

Considérations concernant l'utilisation AWS Secrets Manager avec Amazon Redshift

Lorsque vous l'utilisez AWS Secrets Manager pour gérer les informations d'administration de votre cluster provisionné ou de votre espace de noms sans serveur, tenez compte des points suivants :

- Lorsque vous suspendez un cluster dont les informations d'identification d'administrateur sont gérées par AWS Secrets Manager, le secret de votre cluster n'est pas supprimé et vous continuez à être facturé pour le secret. Les secrets ne sont supprimés que lorsque vous supprimez le cluster.
- Si votre cluster est suspendu quand Amazon Redshift tente d'effectuer la rotation du secret qui lui est attaché, la rotation échoue. Dans ce cas, Amazon Redshift arrête la rotation automatique et n'essaiera plus d'effectuer la rotation, même après la reprise du cluster. Vous devez redémarrer la planification de la rotation automatique à l'aide de l'appel d'API `secretsmanager:RotateSecret` pour qu' AWS Secrets Manager continue à effectuer la rotation automatique de votre secret.
- Si aucun groupe de travail n'est associé à votre espace de noms sans serveur quand Amazon Redshift tente d'effectuer la rotation du secret qui lui est attaché, la rotation échoue et ne sera plus tentée, même une fois qu'un groupe de travail est attaché. Vous devez redémarrer la planification

de la rotation automatique à l'aide de l'appel d'API `secretsmanager:RotateSecret` pour qu' AWS Secrets Manager continue à effectuer la rotation automatique de votre secret.

Récupération de l'Amazon Resource Name (ARN) du secret dans Amazon Redshift

Vous pouvez consulter l'Amazon Resource Name (ARN) de tous les secrets gérés par AWS Secrets Manager à l'aide de la console Amazon Redshift. Une fois que vous avez l'ARN du secret, vous pouvez consulter les détails de votre secret et les données cryptées qu'il contient à l'aide de AWS Secrets Manager. Pour plus d'informations sur la récupération des secrets à l'aide de l'ARN, consultez Récupération des secrets dans le Guide de l'utilisateur AWS Secrets Manager .

Affichage des détails d'un secret pour un cluster provisionné Amazon Redshift

Consultez l'Amazon Resource Name (ARN) du secret de votre cluster à l'aide de la console Amazon Redshift en exécutant la procédure suivante :

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la.
2. Dans le volet Présentation des clusters, choisissez le cluster dont vous souhaitez afficher le secret.
3. Choisissez l'onglet Propriétés.
4. Consultez l'ARN du secret sous ARN des informations d'identification d'administration. Cet ARN est l'identifiant du secret, que vous pouvez utiliser AWS Secrets Manager pour afficher les détails du secret.

Affichage des détails d'un secret pour un espace de noms Amazon Redshift sans serveur

Consultez l'Amazon Resource Name (ARN) du secret de votre espace de noms sans serveur à l'aide de la console Amazon Redshift en exécutant la procédure suivante :

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la.
2. Dans le tableau de bord Clusters provisionnés, choisissez Passer au sans serveur en haut à droite de la page.
3. Dans Tableau de bord sans serveur, faites défiler la page jusqu'au volet Espaces de noms / Groupes de travail et choisissez l'espace de noms dont vous souhaitez consulter le secret.
4. Dans le volet Informations générales, consultez l'ARN du secret sous ARN des informations d'identification d'administration. Cet ARN est l'identifiant du secret, que vous pouvez utiliser AWS Secrets Manager pour afficher les détails du secret.

Création d’un secret pour les informations d’identification de connexion à une base de données

Vous pouvez créer un secret Secrets Manager pour stocker les informations d’identification utilisées pour vous connecter à un cluster alloué Amazon Redshift ou à un espace de noms et à un groupe de travail sans serveur Redshift. Vous pouvez également utiliser ce secret lors de la planification d’une requête dans Amazon Redshift Query Editor V2.

Pour créer un secret pour une base de données dans un cluster alloué Amazon Redshift à l’aide de la console Secrets Manager

1. Ouvrez la console Secrets Manager (https://console.aws.amazon.com/secretsmanager/).
2. Accédez à la liste des Secrets et choisissez Enregistrer un nouveau secret.
3. Choisissez informations d’identification pour un entrepôt de données Amazon Redshift. Entrez vos informations dans les étapes suivantes pour créer un secret :

   - Dans Informations d’identification pour le Nom d’utilisateur, entrez le nom de l’utilisateur administratif de l’entrepôt de données.
   - Dans Informations d’identification pour le Mot de passe, entrez le mot de passe du Nom d’utilisateur.
   - Pour Clé de chiffrement, choisissez votre clé de chiffrement.
   - Pour Entrepôt de données, choisissez le cluster alloué Amazon Redshift qui contient vos données.
   - Pour Nom du secret, saisissez le nom du secret.
   - Pour Description, saisissez une description du secret.
   - Pour Balises, entrez une Clé de balise avec le mot **`Redshift`**. Cette clé de balise est nécessaire pour répertorier les secrets lorsque vous tentez de vous connecter à votre entrepôt de données à l’aide de Amazon Redshift Query Editor V2. Le secret doit comporter une clé de balise commençant par la chaîne **`Redshift`** sous laquelle le secret doit être répertorié sous AWS Secrets Manager sur la console de gestion.
4. Continuez à saisir les informations relatives à votre secret en plusieurs étapes jusqu’à ce que vous enregistriez vos modifications à l’étape Révision.

   Les valeurs spécifiques de vos informations d’identification, de votre moteur, de votre hôte, de votre port et de votre identifiant de cluster sont stockées dans le secret. De plus, le secret est marqué avec la clé de balise `Redshift`.

Pour créer un secret pour une base de données dans un espace de noms sans serveur Redshift à l'aide de la console Redshift sans serveur

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Choisissez Redshift sans serveur et accédez à Configuration de l'espace de noms.
3. Choisissez un espace de noms pour lequel vous souhaitez créer des informations d'identification secrètes.
4. Ouvrez Actions, Modifier les informations d'identification de l'administrateur.
5. Pour Mot de passe administrateur, choisissez Gérer les informations d'identification de l'administrateur dans AWS Secrets Manager.
6. Choisissez Enregistrer les Modifications pour enregistrer vos Modifications.

Confirmez l'affichage d'un message indiquant que le mot de passe a bien été modifié. Vous pouvez également consulter le secret dans la console Secrets Manager. Vous pouvez utiliser ce secret pour vous connecter à une base de données d'un groupe de travail dans la console Redshift Serverless et dans l'éditeur de requêtes Amazon Redshift v2, en utilisant la méthode de connexion. AWS Secrets Manager Le secret doit disposer d'une clé de balise commençant par la chaîne « Redshift » pour que le secret soit répertorié dans l'application web de l'éditeur de requêtes v2. Le secret doit comporter une clé de balise qui commence par la chaîne **`Redshift`** sous laquelle le secret doit être répertorié AWS Secrets Manager sur la console de gestion.

Pour créer un secret pour une base de données dans un espace de noms sans serveur Redshift à l'aide de la console Secrets Manager

1. Ouvrez la console Secrets Manager (https://console.aws.amazon.com/secretsmanager/).
2. Accédez à la liste des Secrets et choisissez Enregistrer un nouveau secret.
3. Choisissez informations d'identification pour un entrepôt de données Amazon Redshift. Entrez vos informations dans les étapes suivantes pour créer un secret :
   - Dans Informations d'identification pour le Nom d'utilisateur, entrez le nom de l'utilisateur administratif de l'entrepôt de données.
   - Dans Informations d'identification pour le Mot de passe, entrez le mot de passe du Nom d'utilisateur.
   - Pour Clé de chiffrement, choisissez votre clé de chiffrement.

- Pour Entrepôt de données, choisissez l’espace de noms Redshift sans serveur qui contient vos données.
- Pour Nom du secret, saisissez le nom du secret.
- Pour Description, saisissez une description du secret.
- Pour Balises, entrez une Clé de balise avec le mot **`Redshift`**. Cette clé de balise est nécessaire pour répertorier les secrets lorsque vous tentez de vous connecter à votre entrepôt de données à l’aide de Amazon Redshift Query Editor V2. Le secret doit comporter une clé de balise commençant par la chaîne **`Redshift`** sous laquelle le secret doit être répertorié sous AWS Secrets Manager sur la console de gestion.

4. Continuez à saisir les informations relatives à votre secret en plusieurs étapes jusqu’à ce que vous enregistriez vos modifications à l’étape Révision.

   Les valeurs spécifiques de vos informations d’identification, du nom de la base de données, de l’hôte, du port, de l’espace de noms et du moteur sont stockées dans le secret. De plus, le secret est marqué avec la clé de balise `Redshift`.

Pour créer un secret pour une base de données dans un espace de noms Redshift Serverless à l'aide du AWS CLI

Vous pouvez utiliser le AWS CLI pour créer un secret. L'une des méthodes consiste AWS CloudShell à exécuter la AWS CLI commande Secrets Manager comme suit. Vous devez disposer des autorisations appropriées pour exécuter les commandes de l’ AWS CLI indiquée dans la procédure suivante.

1. Sur la AWS console, ouvrez l'invite de AWS CloudShell commande. Pour plus d'informations AWS CloudShell, voir Contenu du guide AWS CloudShell de l'AWS CloudShell utilisateur.
2. Par exemple, pour le secret `MyTestSecret`, entrez une commande Secrets Manager pour stocker le secret utilisé pour se connecter à une base de données ou planifier une requête de Amazon Redshift Query Editor V2. Remplacez les valeurs suivantes dans la commande par les valeurs pour votre environnement.

   - *`admin`*est le nom d'utilisateur de l'administrateur de l'entrepôt de données.
   - *`passw0rd`*est le mot de passe de l'administrateur.
   - *`dev`*est le nom initial de la base de données dans l'entrepôt de données.
   - *`region`*est celui Région AWS qui contient l'entrepôt de données. Par exemple `us-east-1`.
   - *`123456789012`*est le Compte AWS.

- *namespace-id*est l'identifiant de l'espace de noms similaire à. c3928f0e-c889-4d2b-97a5-5738324d5d3e Vous trouverez cet identifiant sur la page des détails de la console Amazon Redshift pour l'espace de noms sans serveur.

```
aws secretsmanager create-secret \
--name MyTestSecret \
--description "My test secret created with the CLI." \
--secret-string "{\"username\":\"admin\",\"password\":\"passw0rd\",\"dbname\":
\"dev\",\"engine\":\"redshift\"}" \
--tags "[{\"Key\":\"redshift-serverless:namespaceArn\",\"Value\":
\"arn:aws:redshift-serverless:region:123456789012:namespace/namespace-id\"}]"
```

Journalisation et surveillance dans Amazon Redshift

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon Redshift et de vos AWS solutions. Vous pouvez collecter des données de surveillance à partir de toutes les parties de votre AWS solution afin de pouvoir déboguer plus facilement une panne multipoint le cas échéant. AWS fournit plusieurs outils pour surveiller vos ressources Amazon Redshift et répondre aux incidents potentiels :

CloudWatch Alarmes Amazon

À l'aide CloudWatch des alarmes Amazon, vous observez une seule métrique sur une période que vous spécifiez. Si la métrique dépasse un seuil donné, une notification est envoyée à une rubrique ou à une AWS Auto Scaling politique Amazon SNS. CloudWatch les alarmes n'invoquent aucune action car elles se trouvent dans un état particulier. L'état doit avoir changé et avoir été conservé pendant un nombre de périodes spécifié. Pour plus d'informations, consultez Création d'une alarme. Pour connaître la liste des métriques, consultez Données de performances dans Amazon Redshift.

AWS CloudTrail Journaux

CloudTrail fournit un enregistrement des opérations d'API effectuées par un utilisateur, un rôle IAM ou un AWS service dans Amazon Redshift. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Amazon Redshift, l'adresse IP à partir de laquelle la demande a été faite, qui a effectué la demande, quand elle a été faite et des

informations supplémentaires. Pour de plus amples informations, veuillez consulter Se connecter avec CloudTrail.

Journalisation des audits de base de données

Amazon Redshift consigne dans un journal les informations sur les connexions et les activités de l'utilisateur dans votre base de données. Ces journaux vous permettent de contrôler la base de données à des fins de sécurité et de résolution des problèmes, ce qui est un processus souvent appelé audit de la base de données. Les journaux peuvent être stockés dans :

- Compartiments Amazon S3 : ils fournissent un accès pratique aux fonctions de sécurité des données pour les utilisateurs qui sont responsables de la surveillance des activités de la base de données.
- Amazon CloudWatch - Vous pouvez consulter les données d'enregistrement des audits à l'aide des fonctionnalités intégrées CloudWatch, telles que les fonctionnalités de visualisation et les actions de configuration.

> **Note**
>
> SYS_CONNECTION_LOG collecte les données de journal de connexion pour Amazon Redshift sans serveur. Notez que lorsque vous collectez des données de journalisation d'audit pour Amazon Redshift Serverless, elles ne peuvent pas être envoyées vers des fichiers journaux, mais uniquement vers. CloudWatch

Rubriques

- Journaux Amazon Redshift
- Journaux d'audit et Amazon CloudWatch
- Activation de la journalisation des audits
- Journalisation sécurisée

Journaux Amazon Redshift

Amazon Redshift enregistre les informations dans les fichiers journaux suivants :

- Journal de connexion : consigne les tentatives d'authentification, les connexions et les déconnexions.
- Journal de l'utilisateur : consigne les informations sur les modifications apportées aux définitions d'utilisateur de base de données.
- Journal d'activité utilisateur : consigne chaque requête avant qu'elle soit exécutée sur la base de données.

Les journaux de connexion et utilisateur sont utiles principalement à des fins de sécurité. Vous pouvez utiliser le journal de connexion pour contrôler les informations sur les utilisateurs qui se connectent à la base de données ainsi que les informations de connexion associées. Il peut s'agir de leur adresse IP, du moment où la demande a été effectuée, du type d'authentification utilisé, etc. Vous pouvez utiliser le journal utilisateur pour surveiller les modifications apportées aux définitions des utilisateurs de base de données.

Le journal d'activité utilisateur est utile principalement à des fins de résolution de problèmes. Il effectue le suivi d'informations sur les types de requêtes exécutées par les utilisateurs et le système dans la base de données.

Les journaux de connexion et utilisateur correspondent aux informations stockées dans les tables système de votre base de données. Vous pouvez utiliser les tables système pour obtenir les mêmes informations, mais les fichiers journaux constituent un mécanisme de récupération et de vérification plus simple. Les fichiers journaux s'appuient sur les autorisations Amazon S3 plutôt que sur les autorisations de base de données pour exécuter des requêtes sur les tables de base de données. En outre, le fait d'afficher les informations dans des fichiers journaux plutôt que d'interroger les tables système vous permet de limiter l'impact de l'interaction avec la base de données.

> **Note**
>
> Les fichiers journaux ne sont pas aussi courants que les tables des journaux système que sont STL_USERLOG et STL_CONNECTION_LOG. Les enregistrements qui sont plus anciens que les derniers enregistrements, mais ne les incluent pas, sont copiés dans les fichiers journaux.

> **Note**
>
> Pour Amazon Redshift sans serveur, SYS_CONNECTION_LOG collecte les données de journal de connexion. Lorsque vous collectez des données de journalisation d'audit pour Amazon Redshift Serverless, elles ne peuvent pas être envoyées vers des fichiers journaux, mais uniquement vers. CloudWatch

Journal de connexion

Enregistre les tentatives d'authentification, ainsi que les connexions et déconnexions. Le tableau suivant décrit les informations contenues dans le journal de connexion. Pour plus d'informations sur ces champs, veuillez consulter STL_CONNECTION_LOG dans le Guide du développeur de base de données Amazon Redshift. Pour en savoir plus sur les données de journal de connexion collectées pour Amazon Redshift sans serveur, consultez SYS_CONNECTION_LOG.

Nom de la colonne	Description
event	Connexion ou événement d'authentification.
recordtime	Heure de l'événement.
remotehost	Nom ou adresse IP de l'hôte distant.
remoteport	Numéro de port de l'hôte distant.
pid	ID de processus associé à l’instruction.
dbname	Nom de la base de données.
nom d’utilisateur	Nom d'utilisateur.
authmethod	Méthode d'authentification.
duration	Durée de connexion en microsecondes.
sslversion	Version du protocole SSL (Secure Sockets Layer).

Nom de la colonne	Description
sslcipher	Chiffrement SSL.
mtu	Unité de transmission maximale (MTU).
sslcompression	Type de compression SSL.
sslexpansion	Type d'extension SSL.
iamauthguid	L'ID d'authentification Gestion des identités et des accès AWS (IAM) pour la AWS CloudTrail demande. Il s'agit de l'identifiant de l'appel d'GetClusterCredentialsAPI destiné à créer les informations d'identification utilisées pour une connexion donnée.
application_name	Nom initial ou mis à jour de l’application pour une séance.
os_version	La version du système d’exploitation de la machine cliente qui se connecte à votre cluster Amazon Redshift.
driver_version	Version du pilote ODBC ou JDBC qui se connecte à votre cluster Amazon Redshift à partir de vos outils clients SQL tiers.
plugin_name	Le nom du plugin utilisé pour se connecter à votre cluster Amazon Redshift.
protocol_version	La version du protocole interne que le pilote Amazon Redshift utilise pour établir sa connexion avec le serveur.
sessionid	Identifiant unique au niveau mondial pour la session en cours.
compression	Algorithme de compression utilisé pour la connexion.

Journal utilisateur

Enregistre les détails des modifications suivantes apportées à un utilisateur de base de données :

- Créer un utilisateur
- Supprimer un utilisateur

- Modifier un utilisateur (renommer)
- Modifier un utilisateur (modifier les propriétés)

Nom de la colonne	Description
userid	ID de l'utilisateur affecté par la modification.
nom d’utilisateur	Nom d'utilisateur de l'utilisateur affecté par la modification.
oldusername	Pour une action d’attribution d’un nouveau nom, le nom original de l’utilisateur. Pour toute autre action, ce champ est vide.
action	Action qui s’est produite. Valeurs valides : • Alter • Créer • Drop • Rename
usecreatedb	Si true (1), indique que l'utilisateur a créé des autorisations de base de données.
usesuper	Si true (1), indique que l'utilisateur est un super-utilisateur.
usecatupd	Si true (1), indique que l'utilisateur peut mettre à jour les catalogues système.
valuntil	Date d'expiration du mot de passe.
pid	ID du processus.
xid	ID de transaction.
recordtime	Heure au format UTC du début de la requête.

Interrogez la vue système SYS_USERLOG pour trouver des informations supplémentaires sur les modifications apportées aux utilisateurs. Cette vue comprend les données de journal d'Amazon Redshift sans serveur.

Journal d'activité utilisateur

Consigne chaque requête avant qu'elle soit exécutée sur la base de données.

Nom de la colonne	Description
recordtime	Heure de l'événement.
db	Nom de la base de données.
user	Nom d'utilisateur.
pid	ID de processus associé à l’instruction.
userid	ID de l'utilisateur.
xid	ID de transaction.
query	Préfixe LOG: suivi du texte de la requête incluant les sauts de ligne.

Journaux d'audit et Amazon CloudWatch

La journalisation des audits n'est pas activée par défaut dans Amazon Redshift. Lorsque vous activez la journalisation sur votre cluster, Amazon Redshift exporte les journaux vers Amazon CloudWatch, ou crée et télécharge des journaux vers Amazon S3, qui capturent les données depuis le moment où la journalisation des audits est activée jusqu'à aujourd'hui. Chaque mise à jour de journalisation constitue la suite des journaux précédents.

La journalisation des audits vers CloudWatch ou vers Amazon S3 est un processus facultatif. La journalisation dans les tables système n'est pas facultative et se fait automatiquement. Pour plus d'informations sur la journalisation dans les tables système, veuillez consulter la rubrique Référence des tables système dans le Guide du développeur de la base de données Amazon Redshift.

Le journal de connexion, le journal utilisateur et le journal d'activité utilisateur sont activés ensemble à l' Console de gestion AWS aide de la référence d'API Amazon Redshift ou du AWS Command

Line Interface ()AWS CLI. Pour le journal d'activité utilisateur, vous devez également activer le paramètre de base de données `enable_user_activity_logging`. Si vous activez uniquement la fonction de journalisation des audits, mais pas le paramètre associé, les journaux d'audit de base de données enregistrent des informations uniquement pour les journaux de connexion et utilisateur, mais pas pour le journal d'activité utilisateur. Le paramètre `enable_user_activity_logging` n'est pas activé (`false`) par défaut. Vous pouvez le définir sur `true` pour activer le journal d'activité de l'utilisateur. Pour de plus amples informations, veuillez consulter Groupes de paramètres Amazon Redshift.

Lorsque vous activez la connexion à CloudWatch, Amazon Redshift exporte les données de connexion au cluster, d'utilisateur et d'activité des utilisateurs vers un groupe de CloudWatch journaux Amazon Logs. Les données du journal ne changent pas, en termes de schéma. CloudWatch est conçu pour surveiller les applications, et vous pouvez l'utiliser pour effectuer des analyses en temps réel ou le configurer pour qu'il prenne des mesures. Vous pouvez également utiliser Amazon CloudWatch Logs pour stocker vos enregistrements de journal dans un espace de stockage durable.

L'utilisation CloudWatch pour afficher les journaux est une alternative recommandée au stockage des fichiers journaux dans Amazon S3. Cela ne nécessite pas beaucoup de configuration et peut répondre à vos exigences de surveillance, surtout si vous l'utilisez déjà pour surveiller d'autres services et d’autres applications.

Groupes de journaux et événements de journalisation sur Amazon CloudWatch

Après avoir sélectionné les journaux Amazon Redshift à exporter, vous pouvez surveiller les événements des journaux dans Amazon CloudWatch Logs. Un nouveau groupe de journaux est automatiquement créé pour Amazon Redshift Serverless sous le préfixe suivant, dans lequel `log_type` représente le type de journal.

```
/aws/redshift/cluster/<cluster_name>/<log_type>
```

Par exemple, si vous choisissez d'exporter le journal des connexions, les données du journal sont stockées dans le groupe de journaux suivant.

```
/aws/redshift/cluster/cluster1/connectionlog
```

Les événements de journal sont exportés vers un groupe de journaux à l'aide du flux de journaux. Pour rechercher des informations dans les événements de journal de votre point de terminaison sans

serveur, utilisez la console Amazon CloudWatch Logs AWS CLI, ou l'API Amazon CloudWatch Logs. Pour de plus amples informations sur la recherche et le filtrage des données de journaux, veuillez consulter Création de métriques à partir d'événements du journal à l'aide de filtres.

Dans CloudWatch, vous pouvez rechercher les données de votre journal à l'aide d'une syntaxe de requête garantissant granularité et flexibilité. Pour plus d'informations, consultez la section Syntaxe de requête CloudWatch Logs Insights.

Migration vers la journalisation des CloudWatch audits Amazon

Dans tous les cas où vous envoyez des journaux à Amazon S3 et que vous modifiez la configuration, par exemple pour envoyer des journaux à CloudWatch, les journaux qui restent dans Amazon S3 ne sont pas affectés. Vous pouvez toujours interroger les données de journaux dans les compartiments Simple Storage Service (Amazon S3) où elles se trouvent.

Fichiers journaux dans Amazon S3

Le nombre et la taille des fichiers journaux Amazon Redshift dans Amazon S3 dépendent fortement de l'activité de votre cluster. Si vous avez un cluster actif qui génère un grand nombre de journaux, Amazon Redshift peut générer des fichiers journaux plus fréquemment. Vous pouvez disposer d'une série de fichiers journaux pour le même type d'activité, par exemple plusieurs journaux de connexion au cours de la même heure.

Lorsqu'Amazon Redshift utilise Amazon S3 pour stocker les journaux, vous devez payer des frais pour le stockage que vous utilisez dans Amazon S3. Avant de configurer la journalisation dans Amazon S3, vous devez avoir planifié la durée de stockage des fichiers journaux. Dans le cadre de ce plan, déterminez quand les fichiers journaux peuvent être supprimés ou archivés en fonction de vos besoins en audit. Le plan que vous créez dépend fortement du type de données que vous stockez, telles que les données soumises à des exigences réglementaires ou de conformité. Pour de plus amples informations sur la tarification d'Amazon S3, veuillez consulter la tarification Amazon Simple Storage Service (S3).

Limites lorsque vous activez la journalisation sur Amazon S3

La journalisation d'audit présente les contraintes suivantes :

- Vous ne pouvez utiliser que le chiffrement (SSE-S3) des S3-managed clés Amazon (AES-256).
- Les compartiments Amazon S3 doivent avoir la fonction Verrouillage des objets S3 désactivée.

Autorisations du compartiment pour la journalisation des audits Amazon Redshift

Lorsque vous activez la journalisation dans Amazon S3, Amazon Redshift collecte des informations de journalisation et les charge dans les fichiers journaux stockés dans Amazon S3. Vous ou utiliser un compartiment existant ou créer un compartiment. Amazon Redshift requiert les autorisations IAM suivantes pour le compartiment :

- `s3:GetBucketAcl` Le service nécessite des autorisations de lecture pour le compartiment Amazon S3 afin de pouvoir identifier le propriétaire du compartiment.
- `s3:PutObject` Le service nécessite des autorisations de placement d'objet pour charger les journaux. De plus, l'utilisateur ou le rôle IAM qui permet la journalisation doit avoir les autorisations `s3:PutObject` pour le compartiment Amazon S3. Chaque fois que les journaux sont chargés, le service détermine si le propriétaire actuel du compartiment correspond au propriétaire du compartiment au moment de l'activation de la journalisation. Si ces propriétaires ne correspondent pas, vous recevez une erreur.

Si, lorsque vous activez la journalisation d'audit, vous sélectionnez l'option permettant de créer un compartiment, les autorisations correctes sont appliquées à celui-ci. Toutefois, si vous créez votre propre compartiment dans Amazon S3 ou que vous utilisez un compartiment existant, veillez à ajouter une politique de compartiment incluant le nom du compartiment. Les journaux sont fournis à l'aide des informations d'identification du principal du service. Dans la plupart des Régions AWS cas, vous ajoutez le nom principal du service Redshift,. *`redshift.amazonaws.com`*

La politique du bucket utilise le format suivant. *`ServiceName`*et *`BucketName`* sont des espaces réservés à vos propres valeurs. Spécifiez également les actions et les ressources associées dans la politique de compartiment.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Put bucket policy needed for audit logging",
            "Effect": "Allow",
            "Principal": {
                "Service": "ServiceName"
            },
            "Action": [
```

```
                "s3:PutObject",
                "s3:GetBucketAcl"
            ],
            "Resource": [
                "arn:aws:s3:::BucketName",
                "arn:aws:s3:::BucketName/*"
            ]
        }
    ]
}
```

L'exemple suivant présente une politique de compartiment pour la région USA Est (Virginie du Nord) et le compartiment nommé `AuditLogs`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Put bucket policy needed for audit logging",
            "Effect": "Allow",
            "Principal": {
                "Service": "redshift.amazonaws.com"
            },
            "Action": [
                "s3:PutObject",
                "s3:GetBucketAcl"
            ],
            "Resource": [
                "arn:aws:s3:::AuditLogs",
                "arn:aws:s3:::AuditLogs/*"
            ]
        }
    ]
}
```

Les régions qui ne sont pas activées par défaut, également appelées régions « optionnelles », nécessitent un nom principal Region-specific de service. Pour cela, le nom du principal du service inclut la région, au format `redshift.`*`region`*`.amazonaws.com`. Par exemple, *`redshift.ap-`*

east-1.amazonaws.com pour la région Asie-Pacifique (Hong Kong). Pour obtenir une liste des régions qui ne sont pas activées par défaut, consultez la section Gestion des Régions AWS dans Références générales AWS.

> **Note**
>
> Le nom Region-specific principal du service correspond à la région dans laquelle se trouve le cluster.

Bonnes pratiques relatives aux fichiers journaux

Lorsque Redshift charge des fichiers journaux sur Amazon S3, les fichiers volumineux peuvent être téléchargés en plusieurs parties. Si un chargement partitionné ne réussit pas, il est possible que certaines parties d'un fichier restent dans le compartiment Amazon S3. Cela peut entraîner des coûts de stockage supplémentaires. Il est donc important de comprendre ce qui se produit lorsqu'un chargement partitionné échoue. Pour obtenir des explications détaillées sur le chargement partitionné pour les journaux d'audit, veuillez consulter Chargement et copie d'objets à l'aide d'un chargement partitionné et Interruption d'un chargement partitionné.

Pour plus d'informations sur la création de compartiments Amazon S3 et l'ajout de stratégies de compartiment, consultez Création d'un compartiment à usage général et Stratégies de compartiment pour Amazon S3 dans le Guide de l'utilisateur Amazon Simple Storage Service.

Structure du compartiment pour la journalisation d'audit Amazon Redshift

Par défaut, Amazon Redshift organise les fichiers journaux dans le compartiment Amazon S3 en utilisant la structure de compartiment et d'objet suivante :

`AWSLogs/AccountID/ServiceName/Region/Year/Month/Day/AccountID_ServiceName_Region`

Voici un exemple : `AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz`.

Si vous fournissez un préfixe de clé Amazon S3, placez-le au début de la clé.

Par exemple, si vous spécifiez un préfixe « myprefix » : `myprefix/AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz`

Le préfixe de clé Amazon S3 ne doit pas dépasser 512 caractères. Il ne peut pas contenir d'espaces ( ), de guillemets doubles ("), d'apostrophes (') et de barre oblique inverse (\). Un certain nombre de caractères spéciaux et de caractères de contrôle ne sont pas autorisés non plus. Les codes hexadécimaux de ces caractères sont les suivants :

- x00 à x20
- x22
- x27
- x5c
- x7f ou plus

Considérations relatives à la journalisation des audits Amazon S3

La journalisation d'audit Amazon Redshift peut être interrompue pour les raisons suivantes :

- Amazon Redshift n'a pas l'autorisation de télécharger les journaux vers le compartiment Amazon S3. Vérifiez que le compartiment est configuré avec la bonne stratégie IAM. Pour plus d'informations, consultez Autorisations du compartiment pour la journalisation des audits Amazon Redshift.
- Le propriétaire du compartiment a changé. Quand Amazon Redshift charge les journaux, il vérifie que le propriétaire du compartiment est le même que lors de l'activation de la journalisation. Si le propriétaire du compartiment a changé, Amazon Redshift ne peut pas charger les journaux tant que vous ne configurez pas d'autre compartiment à utiliser pour la journalisation d'audit.
- Impossible de trouver le compartiment. Si le compartiment est supprimé dans Amazon S3, Amazon Redshift ne peut pas télécharger les journaux. Vous devez recréer le compartiment ou configurer Amazon Redshift pour charger les journaux dans un autre compartiment.

Appels d'API avec AWS CloudTrail

Amazon Redshift est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions effectuées par un utilisateur, un rôle ou un AWS service dans Amazon Redshift. CloudTrail capture tous les appels d'API pour Amazon Redshift sous forme d'événements. Pour plus d'informations sur l'intégration d'Amazon Redshift avec AWS CloudTrail, consultez Logging with. CloudTrail

Vous pouvez utiliser la journalisation des audits de base de données Amazon Redshift CloudTrail indépendamment ou en complément de celle-ci.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Activation de la journalisation des audits

Configurez Amazon Redshift de manière à exporter les données de journaux d’audit. Les journaux peuvent être exportés vers CloudWatch ou sous forme de fichiers vers des compartiments Amazon S3.

Activation de la journalisation d'audit grâce à la console

Étapes de la console

Pour activer la journalisation d'audit pour un cluster

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters, puis choisissez le cluster que vous souhaitez mettre à jour.
3. Choisissez l’onglet Propriétés. Dans le volet Database configurations (Configurations de base), choisissez Edit (Modifier), puis Edit audit logging (Modifier la journalisation d'audit).
4. Sur la page Modifier la journalisation des audits, choisissez Activer et sélectionnez le compartiment S3 ou CloudWatch. Nous vous recommandons de l'utiliser CloudWatch car l'administration est simple et elle comporte des fonctionnalités utiles pour la visualisation des données.
5. Choisissez les journaux à exporter.
6. Pour enregistrer vos choix, sélectionnez Save changes (Enregistrer les modifications).

Journalisation sécurisée

Lorsqu'Amazon Redshift enregistre une requête qui fait référence à une ou plusieurs AWS Glue Data Catalog vues, Amazon Redshift masque automatiquement les champs de certaines tables système et colonnes de vue lors de l'enregistrement des métadonnées relatives à cette requête.

Le masquage sécurisé des journaux s’applique à toutes les entrées de table et de vue système générées par Amazon Redshift lors de l’exécution d’une requête répondant aux conditions de masquage. La table suivante répertorie les vues et les colonnes du système auxquelles une journalisation sécurisée est appliquée, masquant le texte avec `******` et les chiffres avec `-1`. Le nombre d’astérisques utilisés pour masquer le texte correspond au nombre de caractères du texte

d'origine, jusqu'à 6 caractères. Les chaînes de plus de 6 caractères apparaissent toujours sous la forme de 6 astérisques.

Table système	Colonnes sensibles
SYS_EXTERNAL_QUERY_DETAIL	Colonnes : source_type, total_partitions, qualified_partitions, scanned_files, returned_rows, returned_bytes, file_format, file_location, external_query_text, warning_message.
ERREUR SYS_EXTERNAL_QUERY_ERROR	Colonnes : file_location, rowid, column_name, original_value, modified_value, trigger, action, action_value, error_code.
SYS_QUERY_DETAIL	Colonnes : step_id, step_name, table_id, table_name, input_bytes, input_rows, output_bytes, output_rows, blocks_read, blocks_write, local_read_IO, remote_read_IO, spilled_block_local_disk, spilled_block_remote_disk, step_attribute.
SYS_QUERY_HISTORY	Colonnes : returned_rows, returned_bytes.
STL_AGGR	Colonnes : rows, bytes, tbl, type.
STL_BCAST	Colonnes : rows, bytes, packets.
STL_DDLTEXT	Colonnes : label, text.
STL_SUPPRIMER	Colonnes : rows, tbl.
STL_DIST	Colonnes : rows, bytes, packets.
ERREUR STL	Colonnes : file, linenum, context, error.
STL_EXPLAIN	Colonnes : plannode, info.
STL_FILE_SCAN	Colonnes : name, line, bytes.
STL HASH	Colonnes : rows, bytes, tbl, est_rows.
STL_HASHJOIN	Colonnes : rows, tbl, num_parts, join_type.
STL_INSERT	Colonnes : rows, tbl.

Table système	Colonnes sensibles
STL_LIMIT	Colonnes : rows.
STL_MERGE	Colonnes : rows.
STL_MERGEJOIN	Colonnes : rows, tbl.
STL NESTLOOP	Colonnes : rows, tbl.
STL_PARSE	Colonnes : rows.
INFORMATIONS SUR LE PLAN STL	Colonnes : startupcost, totalcost, rows, bytes.
PROJET STL	Colonnes : rows, tbl.
REQUÊTE STL	Colonnes : querytxt.
STL_QUERY_METRICS	Colonnes : max_rows, rows, max_blocks_read, blocks_read, max_blocks_to_disk, blocks_to_disk, max_query_scan_size, query_scan_size.
TEXTE DE REQUÊTE STL	Colonnes : text.
STL_RETURN	Colonnes : rows, bytes.
CLIENT STL_S3	Colonnes : bucket, key, transfer_size, data_size.
STL_S3CLIENT_ERROR	Colonnes : bucket, key, error, transfer_size.
STL_SAVE	Colonnes : rows, bytes, tbl.
STL_SCAN	Colonnes : rows, bytes, fetches, type, tbl, rows_pre_filter, rows_pre_user_filter, perm_table_name, scanned_mega_value.
STL_SORT	Colonnes : rows, bytes, tbl.

Table système	Colonnes sensibles
ERREUR STL_SSHCLIENT_ERROR	Colonnes : ssh_username, endpoint, command, error.
STL_TR_CONFLICT	Colonnes : table_id.
STL_UNDONE	Colonnes : table_id.
STL UNIQUE	Colonnes : rows, type, bytes.
STL_UTILITYTEXT	Colonnes : label, text.
FENÊTRE STL	Colonnes : rows.
STV_BLOCKLIST	Colonnes : col, tbl, num_values, minvalue, maxvalue.
STV_EXEC_STATE	Colonnes : rows, bytes, label.
STV_INFLIGHT	Colonnes : label, text.
STV LOCKS	Colonnes : table_id.
STV_QUERY_METRICS	Colonnes : rows, max_rows, blocks_read, max_blocks_read, max_blocks_to_disk, blocks_to_disk, max_query_scan_size, query_scan_size.
STV_STARTUP_RECOVERY_STATE	Colonnes : table_id, table_name.
STV_TBL_PERM	Colonnes : id, name, rows, sorted_rows, temp, block_count, query_scan_size.
STV_TBL_TRANS	Colonnes : id, rows, size.
SVCS_EXPLAIN	Colonnes : plannode, info.
INFORMATIONS SUR LE PLAN SVCS	Colonnes : rows, bytes.

Table système	Colonnes sensibles
RÉSUMÉ DE LA REQUÊTE SVCS	Colonnes : step, rows, bytes, rate_row, rate_byte, label, rows_pre_filter.
LISTE SVCS_S3	Colonnes : bucket, prefix, retrieved_files, max_file_size, avg_file_size.
SVCS_S3LOG	Colonnes : message.
SVCS_S3PARTITION_SUMMARY	Colonnes : total_partitions, qualified_partitions, min_assigned_partitions, max_assigned_partitions, avg_assigned_partitions.
SVCS_S3QUERY_SUMMARY	Colonnes : external_table_name, file_format, s3_scanned_rows, s3_scanned_bytes, s3query_returned_rows, s3query_returned_bytes.
SVL_QUERY_METRICS	Colonnes : step_label, scan_row_count, join_row_count, nested_loop_join_row_count, return_row_count, spectrum_scan_row_count, spectrum_scan_size_mb.
SVL_QUERY_METRICS_SUMMARY	Colonnes : step_label, scan_row_count, join_row_count, nested_loop_join_row_count, return_row_count, spectrum_scan_row_count, spectrum_scan_size_mb.
SVL_QUERY_REPORT	Colonnes : rows, bytes, label, rows_pre_filter.
RÉSUMÉ DE LA REQUÊTE SVL	Colonnes : rows, bytes, rows_pre_filter.
LISTE SVL_S3	Colonnes : bucket, prefix, retrieved_files, max_file_size, avg_file_size.
SVL_S3LOG	Colonnes : message.
PARTITION SVL_S3	Colonnes : rows, bytes, label, rows_pre_filter.
RÉSUMÉ DE LA PARTITION SVL_S3	Colonnes : total_partitions, qualified_partitions, min_assigned_partitions, max_assigned_partitions, avg_assigned_partitions.
REQUÊTE SVL_S3	Colonnes : external_table_name, file_format, s3_scanned_rows, s3_scanned_bytes, s3query_returned_rows, s3query_returned_bytes, files.

Table système	Colonnes sensibles
RÉSUMÉ DE LA REQUÊTE SVL_S3	Colonnes : external_table_name, file_format, s3_scanned_rows, s3_scanned_bytes, s3query_returned_rows, s3query_returned_bytes.
SVL_S3 RÉESSAIE	Colonnes : file_size, location, message.
SVL_SPECTRUM_SCAN_ERROR	Colonnes : location, rowid, colname, original_value, modified_value, trigger, action, action_value, error_code.
SVL_STATEMENTTEXT	Colonnes : type, text.
SVL_STORED_PROC_CALL	Colonnes : querytxt.
SVL_STORED_PROC_MESSAGES	Colonnes : message, linenum, querytext.
SVL_UDF_LOG	Colonnes : message, funcname.
UTILISATION DU DISQUE SVV	Colonnes : name, col, tbl, blocknum, num_values, minvalue, maxvalue.
SVV_QUERY_STATE	Colonnes : rows, bytes, label.
SVV_TABLE_INFO	Colonnes : table_id, table.
SVV_TRANSACTIONS	Colonnes : relation.

Pour plus d'informations sur les vues et les tables système dans, consultez Informations de référence sur les tables et les vues système dans le Guide du développeur de base de données Amazon Redshift. Pour plus d'informations sur la capacité d'Amazon Redshift à masquer dynamiquement les résultats des requêtes, consultez la section Masquage dynamique des données dans le Guide du développeur de base de données Amazon Redshift Pour plus d'informations sur la création de vues dans le cadre de AWS Glue Data Catalog l'utilisation d'Amazon Redshift, consultez les AWS Glue Data Catalog vues dans le manuel Amazon Redshift Database Developer Guide.

Se connecter avec CloudTrail

Amazon Redshift, le partage de données, Amazon Redshift Serverless, l'API de données Amazon Redshift et l'éditeur de requêtes v2 sont tous intégrés à. AWS CloudTrail CloudTrail est un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Amazon Redshift. CloudTrail capture tous les appels d'API pour Amazon Redshift sous forme d'événements. Les appels capturés incluent les appels de la console Redshift et les appels de code aux opérations Redshift.

Si vous créez un suivi CloudTrail , vous pouvez bénéficier d'une diffusion continue des CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Redshift. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer certaines choses. Il s’agit notamment de la requête qui a été envoyée à Redshift, de l’adresse IP à partir de laquelle la demande a été effectuée, de l’auteur et de la date de la requête, ainsi que d’autres détails.

Vous pouvez utiliser la journalisation des audits de base de données Amazon Redshift CloudTrail indépendamment ou en complément de celle-ci.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations dans CloudTrail

CloudTrail est activé dans votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour Redshift, créez un journal. CloudTrail utilise des traces pour envoyer des fichiers journaux dans un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s’applique à toutes les régions AWS . Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d’informations, consultez les rubriques suivantes dans le Guide de l’utilisateur AWS CloudTrail :

- Présentation de la création d'un journal d'activité
- CloudTrail Services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions Amazon Redshift, Amazon Redshift Serverless, Data API, partage de données et éditeur de requêtes v2 sont enregistrées par. CloudTrail Par exemple, les appels aux `CreateConnection` actions `AuthorizeDatashareCreateNamespace`,`ExecuteStatement`, et génèrent des entrées dans les fichiers CloudTrail journaux.

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 les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou .
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez la section CloudTrail UserIdentity Element dans le guide de l'AWS CloudTrail utilisateur.

Entrées de fichier journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Exemple de partage de données Amazon Redshift

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`AuthorizeDataShare`opération.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
                "arn": "arn:aws:sts::111122223333:user/janedoe",
                "accountId": "111122223333",
                "userName": "janedoe"
            },
            "attributes": {
                "creationDate": "2021-08-02T23:40:45Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2021-08-02T23:40:58Z",
    "eventSource": "redshift.amazonaws.com",
    "eventName": "AuthorizeDataShare",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "3.227.36.75",
    "userAgent":"aws-cli/1.18.118 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.41",
    "requestParameters": {
        "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
        "consumerIdentifier": "555555555555"
    },
    "responseElements": {
        "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
        "producerNamespaceArn": "arn:aws:redshift:us-
east-1:123456789012:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
        "producerArn": "arn:aws:redshift:us-
east-1:111122223333:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
        "allowPubliclyAccessibleConsumers": true,
        "dataShareAssociations": [
```

```
            {
                "consumerIdentifier": "555555555555",
                "status": "AUTHORIZED",
                "createdDate": "Aug 2, 2021 11:40:56 PM",
                "statusChangeDate": "Aug 2, 2021 11:40:57 PM"
            }
        ]
    },
    "requestID": "87ee1c99-9e41-42be-a5c4-00495f928422",
    "eventID": "03a3d818-37c8-46a6-aad5-0151803bdb09",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Exemple Amazon Redshift sans serveur

Amazon Redshift Serverless est intégré AWS CloudTrail pour fournir un enregistrement des actions effectuées dans Amazon Redshift Serverless. CloudTrail capture tous les appels d'API pour Amazon Redshift Serverless sous forme d'événements. Pour de plus amples informations sur les fonctionnalités Amazon Redshift sans serveur, consultez Présentation des fonctionnalités Amazon Redshift sans serveur.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateNamespace`action.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAKEOFPINEXAMPLE:admin",
        "arn": "arn:aws:sts::111111111111:assumed-role/admin/admin",
        "accountId": "111111111111",
        "accessKeyId": "AAKEOFPINEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAKEOFPINEXAMPLE",
                "arn": "arn:aws:iam::111111111111:role/admin",
                "accountId": "111111111111",
                "userName": "admin"
            },
```

```
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-21T20:51:58Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-21T23:15:40Z",
    "eventSource": "redshift-serverless.amazonaws.com",
    "eventName": "CreateNamespace",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "56.23.155.33",
    "userAgent": "aws-cli/2.4.14 Python/3.8.8 Linux/5.4.181-109.354.amzn2int.x86_64
 exe/x86_64.amzn.2 prompt/off command/redshift-serverless.create-namespace",
    "requestParameters": {
        "adminUserPassword": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "adminUsername": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "dbName": "dev",
        "namespaceName": "testnamespace"
    },
    "responseElements": {
        "namespace": {
            "adminUsername": "HIDDEN_DUE_TO_SECURITY_REASONS",
            "creationDate": "Mar 21, 2022 11:15:40 PM",
            "defaultIamRoleArn": "",
            "iamRoles": [],
            "logExports": [],
            "namespaceArn": "arn:aws:redshift-serverless:us-
east-1:111111111111:namespace/befa5123-16c2-4449-afca-1d27cb40fc99",
            "namespaceId": "8b726a0c-16ca-4799-acca-1d27cb403599",
            "namespaceName": "testnamespace",
            "status": "AVAILABLE"
        }
    },
    "requestID": "ed4bb777-8127-4dae-aea3-bac009999163",
    "eventID": "1dbee944-f889-4beb-b228-7ad0f312464",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management",
}
```

Exemples d’API de données Amazon Redshift

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`ExecuteStatement`action.


```
{
    "eventVersion":"1.05",
    "userIdentity":{
        "type":"IAMUser",
        "principalId":"AKIAIOSFODNN7EXAMPLE:janedoe",
        "arn":"arn:aws:sts::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAI44QH8DHBEXAMPLE",
        "userName": "janedoe"
    },
    "eventTime":"2020-08-19T17:55:59Z",
    "eventSource":"redshift-data.amazonaws.com",
    "eventName":"ExecuteStatement",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"192.0.2.0",
    "userAgent":"aws-cli/1.18.118 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.41",
    "requestParameters":{
        "clusterIdentifier":"example-cluster-identifier",
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "sql":"***OMITTED***"
    },
    "responseElements":{
        "clusterIdentifier":"example-cluster-identifier",
        "createdAt":"Aug 19, 2020 5:55:58 PM",
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "id":"5c52b37b-9e07-40c1-98de-12ccd1419be7"
    },
    "requestID":"00c924d3-652e-4939-8a7a-cd0612eeb8ac",
    "eventID":"c1fb7076-102f-43e5-9ec9-40820bcc1175",
    "readOnly":false,
    "eventType":"AwsApiCall",
    "recipientAccountId":"123456789012"
}
```


L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`ExecuteStatement`action indiquant le type `clientToken` utilisé pour l'idempuissance.

```
{
    "eventVersion":"1.05",
    "userIdentity":{
        "type":"IAMUser",
        "principalId":"AKIAIOSFODNN7EXAMPLE:janedoe",
        "arn":"arn:aws:sts::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAI44QH8DHBEXAMPLE",
        "userName": "janedoe"
    },
    "eventTime":"2020-08-19T17:55:59Z",
    "eventSource":"redshift-data.amazonaws.com",
    "eventName":"ExecuteStatement",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"192.0.2.0",
    "userAgent":"aws-cli/1.18.118 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.41",
    "requestParameters":{
        "clusterIdentifier":"example-cluster-identifier",
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "sql":"***OMITTED***",
        "clientToken":"32db2e10-69ac-4534-b3fc-a191052616ce"
    },
    "responseElements":{
        "clusterIdentifier":"example-cluster-identifier",
        "createdAt":"Aug 19, 2020 5:55:58 PM",
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "id":"5c52b37b-9e07-40c1-98de-12ccd1419be7"
    },
    "requestID":"00c924d3-652e-4939-8a7a-cd0612eeb8ac",
    "eventID":"c1fb7076-102f-43e5-9ec9-40820bcc1175",
    "readOnly":false,
    "eventType":"AwsApiCall",
    "recipientAccountId":"123456789012"
}
```


Exemple de Amazon Redshift Query Editor V2.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateConnection`action.


```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAKEOFPINEXAMPLE:session",
        "arn": "arn:aws:sts::123456789012:assumed-role/MyRole/session",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAKEOFPINEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/MyRole",
                "accountId": "123456789012",
                "userName": "MyRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-09-21T17:19:02Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-09-21T22:22:05Z",
    "eventSource": "sqlworkbench.amazonaws.com",
    "eventName": "CreateConnection",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "192.2.0.2",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0)
 Gecko/20100101 Firefox/102.0",
    "requestParameters": {
        "password": "***",
        "databaseName": "***",
        "isServerless": false,
        "name": "***",
        "host": "redshift-cluster-2.c8robpbxvbf9.ca-central-1.redshift.amazonaws.com",
        "authenticationType": "***",
        "clusterId": "redshift-cluster-2",
        "username": "***",
        "tags": {
            "sqlworkbench-resource-owner": "AAKEOFPINEXAMPLE:session"
        }
    },
    "responseElements": {
        "result": true,
```

```
        "code": "",
        "data": {
            "id": "arn:aws:sqlworkbench:ca-central-1:123456789012:connection/ce56b1be-
dd65-4bfb-8b17-12345123456",
            "name": "***",
            "authenticationType": "***",
            "databaseName": "***",
            "secretArn": "arn:aws:secretsmanager:ca-
central-1:123456789012:secret:sqlworkbench!7da333b4-9a07-4917-b1dc-12345123456-qTCoFm",
            "clusterId": "redshift-cluster-2",
            "dbUser": "***",
            "userSettings": "***",
            "recordDate": "2022-09-21 22:22:05",
            "updatedDate": "2022-09-21 22:22:05",
            "accountId": "123456789012",
            "tags": {
                "sqlworkbench-resource-owner": "AAKEOFPINEXAMPLE:session"
            },
            "isServerless": false
        }
    },
    "requestID": "9b82f483-9c03-4cdd-bb49-a7009e7da714",
    "eventID": "a7cdd442-e92f-46a2-bc82-2325588d41c3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


Identifiants de compte Amazon Redshift dans AWS CloudTrail journaux

Lorsqu'Amazon Redshift appelle un autre AWS service pour vous, l'appel est enregistré avec un identifiant de compte appartenant à Amazon Redshift. Il n’est pas consigné avec votre ID de compte. Supposons par exemple qu'Amazon Redshift appelle AWS Key Management Service (AWS KMS) des opérations telles que`CreateGrant`, `DecryptEncrypt`, et `RetireGrant` pour gérer le chiffrement sur votre cluster. Dans ce cas, les appels sont enregistrés à AWS CloudTrail l'aide d'un identifiant de compte Amazon Redshift.

Amazon Redshift utilise les ID de compte du tableau suivant lorsqu’il appelle d’autres services AWS .

Région	Région	ID de compte
Région USA Est (Virginie du Nord)	us-east-1	368064434614
Région USA Est (Ohio)	us-east-2	790247189693
Région US West (N. California)	us-west-1	703715109447
Région USA Ouest (Oregon)	us-west-2	473191095985
Région Afrique (Le Cap)	af-south-1	420376844563
Région Asie-Pacifique (Hong Kong)	ap-east-1	651179539253
Région Asie-Pacifique (Hyderabad)	ap-south-2	297058826802
Région Asie-Pacifique (Jakarta)	ap-southeast-3	623197973179
Région Asie-Pacifique (Malaisie)	ap-southeast-5	590184011157
Région Asie-Pacifique (Melbourne)	ap-southeast-4	945512339897
Région Asie-Pacifique (Mumbai)	ap-south-1	408097707231
Asie-Pacifique (Nouvelle Zélande)	ap-southeast-6	730335362089
Région Asie-Pacifique (Osaka)	ap-northeast-3	398671365691
Région Asie-Pacifique (Séoul)	ap-northeast-2	713597048934
Région Asie-Pacifique (Singapour)	ap-southeast-1	960118270566
Région Asie-Pacifique (Sydney)	ap-southeast-2	485979073181
Asie-Pacifique (Taipei)	ap-east-2	211125526206

Région	Région	ID de compte
Région Asie-Pacifique (Thaïlande)	ap-southeast-7	767397930036
Région Asie-Pacifique (Tokyo)	ap-northeast-1	615915377779
Région Canada (Centre)	ca-central-1	764870610256
Région Canada Ouest (Calgary)	ca-west-1	830903446466
Région Europe (Francfort)	eu-central-1	434091160558
Région Europe (Irlande)	eu-west-1	246478207311
Région Europe (Londres)	eu-west-2	885798887673
Europe (Milan) Region	eu-south-1	041313461515
Région Europe (Paris)	eu-west-3	694668203235
Région Europe (Espagne)	eu-south-2	028811157404
Région Europe (Stockholm)	eu-north-1	553461782468
Région Europe (Zurich)	eu-central-2	668912161003
Région Israël (Tel Aviv)	il-central-1	901883065212
Région Mexique (Centre)	mx-central-1	058264411980
Middle East (Bahrain) Region	me-south-1	051362938876
Région Moyen-Orient (EAU)	me-central-1	595013617770
Région Amérique du Sud (São Paulo)	sa-east-1	392442076723

L'exemple suivant montre une entrée de CloudTrail journal pour l'opération AWS KMS Decrypt appelée par Amazon Redshift.

```
{

    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAI5QPCMKLTL4VHFCYY:i-0f53e22dbe5df8a89",
        "arn": "arn:aws:sts::790247189693:assumed-role/prod-23264-role-wp/
i-0f53e22dbe5df8a89",
        "accountId": "790247189693",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2017-03-03T16:24:54Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAI5QPCMKLTL4VHFCYY",
                "arn": "arn:aws:iam::790247189693:role/prod-23264-role-wp",
                "accountId": "790247189693",
                "userName": "prod-23264-role-wp"
            }
        }
    },
    "eventTime": "2017-03-03T17:16:51Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "52.14.143.61",
    "userAgent": "aws-internal/3",
    "requestParameters": {
        "encryptionContext": {
            "aws:redshift:createtime": "20170303T1710Z",
            "aws:redshift:arn": "arn:aws:redshift:us-east-2:123456789012:cluster:my-dw-
instance-2"
        }
    },
    "responseElements": null,
    "requestID": "30d2fe51-0035-11e7-ab67-17595a8411c8",
    "eventID": "619bad54-1764-4de4-a786-8898b0a7f40c",
    "readOnly": true,
    "resources": [
        {
```

```
            "ARN": "arn:aws:kms:us-east-2:123456789012:key/f8f4f94f-e588-4254-
b7e8-078b99270be7",
            "accountId": "123456789012",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012",
    "sharedEventID": "c1daefea-a5c2-4fab-b6f4-d8eaa1e522dc"

}
```


Intégration des tables système avec les tables S3

Utilisez l'intégration des tables système à Amazon S3 Tables pour conserver les données de vos tables système Amazon Redshift au-delà de la période de conservation de 7 jours dans le cluster. Cela vous permet de répondre aux exigences de conformité, d'audit et d'observabilité. Lorsque vous activez cette fonctionnalité, Redshift écrit les journaux des tables système dans les tables S3 au Apache Iceberg format et gère le partitionnement, le compactage et la maintenance des instantanés. Vous pouvez conserver ces données aussi longtemps que nécessaire à des fins d'analyse et d'audit. Les données étant stockées au format ouvert Iceberg, vous pouvez les interroger avec Redshift, Amazon Athena ou tout autre moteur. Iceberg-compatible Vous pouvez également utiliser les compétences des agents IA pour les requêtes en langage naturel (voir Compétences des tables système pour AWS Agent Toolkit sur le GitHub site Web).

Lorsque vous activez cette fonctionnalité via la console, l'interface de ligne de commande Redshift ou le SDK, Redshift commence à écrire de nouvelles lignes à partir des tables système que vous sélectionnez dans les tables S3 peu de temps après, à une fréquence fixe. Vous choisissez les tables système à publier ; S3 Tables applique la durée de conservation que vous configurez.

Cela prend en charge les cas d'utilisation suivants :

- Répondez aux exigences de conformité et d'audit. Conservez l'historique des requêtes, des connexions et des modifications pendant des mois, voire des années.
- Surveillez votre flotte depuis un seul endroit. Consolidez les données de surveillance provenant de plusieurs entrepôts de données de votre compte et de votre région et analysez l'activité de votre flotte.

- Supprimez le besoin de pipelines d'extraction, de transformation et de chargement (ETL) personnalisés. Arrêtez de créer et de gérer des tâches qui exportent les données des tables système vers S3 pour une conservation plus longue.
- Enquêtez sur les incidents passés. Interrogez les données historiques au-delà de la fenêtre intégrée au cluster de 7 jours pour analyser les causes premières, effectuer un examen post-incident et suivre l'évolution de la charge de travail et les tendances des performances au fil du temps.

Cette fonctionnalité est disponible pour les instances RA3 et RG provisionnées par Amazon Redshift et pour Amazon Redshift Serverless dans toutes les régions AWS commerciales où les tables Redshift et S3 sont prises en charge. Dans cette rubrique, l'entrepôt de données fait référence à un cluster provisionné ou à un groupe de travail Redshift Serverless.

Rubriques

- Comment ça marche
- Activation de l'intégration des tables système avec les tables S3
- Tables système prises en charge
- Colonnes de métadonnées ajoutées à chaque tableau
- Configuration de la rétention
- Gouvernance des données
- Comportement de livraison et de cycle de
- Bonnes pratiques
- Facturation
- Considérations et restrictions

Comment ça marche

Après avoir activé la fonctionnalité et sélectionné une ou plusieurs tables système prises en charge, Redshift écrit les enregistrements récemment complétés à partir de ces tables système dans les tables S3. Les données sont fournies par lots à une fréquence fixe.

Les tables système se trouvent dans votre AWS compte mais sont gérées par un service : AWS possède et gère la distribution des données et la gestion des tables, y compris les suivantes :

- Création du compartiment de tables S3, de l'espace de noms et des tables S3 dans votre compte.

- Définition et évolution des schémas de tables.
- Écrire des données au Apache Iceberg format dans des tables S3.
- Compactage des données et gestion des instantanés (gérés automatiquement par S3 Tables).

Il n'y a aucune infrastructure à créer ou à entretenir et aucun impact sur vos charges de travail.

Vous configurez la durée de conservation des données jusqu'à l'expiration des enregistrements S3 Tables. Pour de plus amples informations, veuillez consulter the section called “Configuration de la rétention”.

Comme les tables sont gérées par AWS, vous ne pouvez ni modifier ni supprimer les lignes fournies par Redshift. Les données fournies sont immuables. Vous contrôlez uniquement l'accès en lecture aux tables. Pour de plus amples informations, veuillez consulter the section called “Gouvernance des données”.

Seule l'activité terminée est transmise à S3 Tables. Les tables système de votre entrepôt de données peuvent indiquer l'activité en vol, mais seuls les enregistrements ayant atteint leur état final sont copiés. Par exemple, une requête terminée, abandonnée ou annulée est envoyée, mais une requête toujours en cours d'exécution n'est pas remise tant qu'elle n'a pas atteint son état final.

Activation de l'intégration des tables système avec les tables S3

Pour activer l'intégration des tables système avec les tables S3, utilisez les API Redshift existantes avec un nouveau type de destination de `s3table` journal, à savoir. Lorsque cette option est activée, Redshift crée un compartiment de tables S3 nommé `aws-redshift` dans votre compte. Vous gérez la fonctionnalité avec les mêmes opérations que vous utilisez pour les autres destinations de journaux : pour les clusters provisionnés, `enable-loggingdisable-logging`, et `describe-logging-status` ; pour Redshift Serverless, et. `update-namespace` `get-namespace`

Permissions

Le principal qui active, modifie ou désactive la fonctionnalité doit disposer des autorisations suivantes :

- `redshift:EnableLogging`(pour les clusters provisionnés) ou `redshift-serverless:UpdateNamespace` (pour Redshift Serverless).
- Autorisation de créer et de configurer le compartiment de tables S3. Le principal d'activation a besoin des autorisations S3 Tables suivantes :

- `s3tables:CreateTableBucket`
- `s3tables:PutTableBucketEncryption`
- `s3tables:PutTableBucketPolicy`

Lorsque vous activez la fonctionnalité, Redshift crée et configure le bucket de tables S3 en utilisant l'identité du principal qui déclenche l'opération.

Une fois le compartiment créé, Redshift crée des espaces de noms et des tables dans celui-ci en utilisant une relation de confiance de service entre Redshift et S3 Tables. Le principal d'activation n'a pas besoin d'autorisations pour créer des espaces de noms ou des tables.

Options de déploiement

Vous pouvez configurer la diffusion selon l'un des deux modèles suivants. Un entrepôt de données donné utilise un modèle à la fois.

Option de déploiement	Description
Per-warehouse	Redshift écrit les données des tables système de chaque entrepôt de données dans son propre ensemble de tables S3. Chaque ligne d'un tableau provient d'un seul entrepôt de données. Utilisez-le pour l'isolation physique entre les entrepôts.
Consolidé	Redshift écrit les données des tables système provenant de plusieurs entrepôts de données au sein du même compte et de la même région dans un ensemble partagé de tables S3. Les lignes provenant de différents entrepôts sont distinguées par les `warehouse_name` colonnes `warehouse_namespace_arn` et. Utilisez-le pour une analyse centralisée entre entrepôts.

Le modèle de déploiement détermine la manière dont les données sont organisées dans les tables S3. Dans le modèle par entrepôt, le nom de l'espace de noms S3 Tables contient un identifiant unique pour l'entrepôt de données, de sorte que les données de chaque entrepôt sont physiquement séparées dans son propre espace de noms. Dans le modèle consolidé, le nom de l'espace de noms S3 Tables contient le numéro de AWS compte, et les données de tous les entrepôts de ce compte et de cette région sont stockées ensemble dans le même espace de noms et les mêmes tables.

Les deux options sont prises en charge au sein d'un seul AWS compte et d'une seule AWS région. Pour analyser les données entre les régions ou les comptes, combinez les résultats des tables de chaque région ou compte au moment de la requête. Pour accéder à plusieurs comptes, vous pouvez utiliser le partage du catalogue de AWS Glue données. Pour plus d'informations, consultez la section Octroi d'un accès multicompte dans le Guide du AWS Glue développeur.

> **Note**
>
> Si vous faites passer un entrepôt de données d'un modèle de déploiement à un autre, les données fournies précédemment restent dans leur table existante et sont conservées conformément à leur rétention configurée. Redshift commence à fournir de nouvelles données à la nouvelle cible et ne remplace pas les données historiques.

Utilisation de la console

Pour configurer l'intégration des tables système avec S3 Tables

1. Ouvrez la console Redshift et dans le volet de navigation, sous Amazon Redshift ou Amazon Redshift Serverless, choisissez System table integrations. Vous pouvez également effectuer la configuration à partir de la page détaillée du cluster ou de l'espace de noms en choisissant l'onglet Intégrations ou en choisissant Actions, Intégrations , Configurer l'intégration de la table système.
2. Choisissez Créer une intégration de tables système.
3. Sélectionnez votre cluster provisionné ou votre groupe de travail Redshift Serverless.
4. Choisissez les tables système à publier. Sélectionnez des SYS_* vues individuelles ou choisissez Sélectionner toutes les tables système prises en charge pour publier toutes les vues prises en charge actuelles et futures. Si vous sélectionnez tout, les nouvelles vues ajoutées ultérieurement sont automatiquement incluses sans qu'il soit nécessaire de modifier la configuration.
5. Sélectionnez le modèle de déploiement :
   - Table S3 individuelle par table système et par entrepôt de données pour conserver les données de cet entrepôt dans son propre ensemble de tables.
   - Table S3 partagée par table système entre les entrepôts de données pour consolider les données provenant de plusieurs entrepôts du compte dans un ensemble partagé de tables.

6. Vous pouvez éventuellement choisir une clé de chiffrement. Par défaut, les données sont cryptées avec des S3-managed clés Amazon (SSE-S3). Pour utiliser votre propre AWS KMS clé, sélectionnez-la ici. Si vous utilisez votre propre AWS KMS clé, la politique de clé doit autoriser Redshift et S3 Tables à accéder à la clé. Pour de plus amples informations, veuillez consulter the section called “Configuration du chiffrement”.
7. Enregistrez vos modifications. Redshift commence à publier les tables système sélectionnées dans S3 Tables et continue d'ajouter de nouveaux enregistrements de manière récurrente.

Pour arrêter de publier une table système, revenez aux paramètres et supprimez-la. Les données déjà publiées sont conservées jusqu'à ce que vous configuriez l'expiration via S3 Tables.

Vous pouvez consulter l'état de l'intégration sur la page détaillée du cluster ou de l'espace de nommage. Développez Afficher le mappage des tables S3 pour voir le mappage entre chaque table système et le nom et l'espace de noms de la table S3 correspondants. Vous pouvez également consulter les données publiées depuis la console S3 Tables.

Utilisation de AWS CLI

Les paramètres suivants configurent la publication de tables S3 :

Paramètre	S’applique à	Description
`--log-destination-type`	les deux	Réglez sur `s3table` pour publier sur S3 Tables. Les autres valeurs sont `s3` et`cloudwatch` .
`--log-exports`	Alloué	Les tables système à publier, sous forme de liste de noms de `SYS_*` vues, ou`all`.
`--s3-table-names`	sans serveur	Les tables système à publier, sous forme de liste de noms de `SYS_*` vues, ou`all`.
`--s3-table-action`	sans serveur	`Enable`ou la publication de tables `Disable` S3.
`--s3-table-granularity`	les deux	Portée de la table. Provisionné : `cluster` (par défaut) ou`account`. Serverless : `namespace` (par défaut) ou`account`.

Paramètre	S'applique à	Description
`--s3-table-kms-key-id`	les deux	AWS KMS Clé ARN ou ID en option pour le chiffrement. La valeur par défaut est Amazon S3-managed keys (SSE-S3).

Clusters alloués

Activez la livraison. `--log-exports`accepte `all` ou une liste séparée par des espaces des tables système prises en charge, et `--s3-table-granularity` accepte `cluster` (par entrepôt) ou `account` (consolidé).

```
aws redshift enable-logging \
    --cluster-identifier my-redshift-cluster \
    --log-destination-type s3table \
    --log-exports all \
    --s3-table-granularity account
```

Pour activer la diffusion de tables système spécifiques uniquement, procédez comme suit :

```
aws redshift enable-logging \
    --cluster-identifier my-redshift-cluster \
    --log-destination-type s3table \
    --log-exports sys_query_history sys_query_text sys_userlog \
    --s3-table-granularity cluster
```

Vérifiez l'état de la livraison.

```
aws redshift describe-logging-status \
    --cluster-identifier my-redshift-cluster
```

Désactivez la diffusion pour toutes les tables du système ou pour des tables spécifiques avec `--log-exports` :

```
aws redshift disable-logging \
    --cluster-identifier my-redshift-cluster \
    --log-destination-type s3table \
```

```
    --log-exports sys_stream_scan_states
```

Redshift sans serveur

Dans Redshift Serverless, vous configurez la fonctionnalité par espace de noms avec. `update-namespace` Les noms des tables système sont transmis `--s3-table-names` (non`--log-exports`).

Activez la livraison.

```
aws redshift-serverless update-namespace \
    --namespace-name my-namespace \
    --log-destination-type s3table \
    --s3-table-action Enable \
    --s3-table-names all \
    --s3-table-granularity namespace
```

Désactivez la diffusion pour des tables système spécifiques (ou`all`) :

```
aws redshift-serverless update-namespace \
    --namespace-name my-namespace \
    --log-destination-type s3table \
    --s3-table-action Disable \
    --s3-table-names sys_stream_scan_states
```

Vérifiez l'état de la livraison.

```
aws redshift-serverless get-namespace \
    --namespace-name my-namespace
```

Pour reprendre la livraison après la suppression du compartiment de tables S3 ou d'une table, exécutez à nouveau la commande enable.

S'inscrire auprès de AWS Glue Data Catalog

Avant de pouvoir interroger les données conservées avec Redshift, Athena ou d'autres services d'analyse, le compartiment de tables S3 géré par le service doit être intégré à. AWS Glue Data Catalog Il s'agit d'une étape unique par compte et par région. Si vous avez déjà intégré S3 Tables à AWS Glue Data Catalog, aucune action supplémentaire n'est requise.

Pour obtenir des instructions d'intégration, consultez la section Intégrer les tables Amazon S3 AWS Glue Data Catalog dans le Guide du AWS Glue développeur.

Configuration du chiffrement

Par défaut, les données transmises à S3 Tables sont chiffrées avec des S3-managed clés Amazon (SSE-S3). Pour utiliser une clé gérée par le AWS KMS client à la place, spécifiez son ARN avec `--s3-table-kms-key-id` lorsque vous activez la livraison :

```
aws redshift enable-logging \
    --cluster-identifier my-redshift-cluster \
    --log-destination-type s3table \
    --log-exports all \
    --s3-table-granularity account \
    --s3-table-kms-key-id arn:aws:kms:us-west-2:111122223333:key/key-id
```

Si vous utilisez une clé gérée par le client, sa politique de clé doit permettre au principal du service d'intégration des tables système Redshift de générer des clés de données lorsqu'il écrit vos tables système, et au principal du service de maintenance des tables S3 d'utiliser la clé lors de la maintenance des tables (comme le compactage). Ajoutez les déclarations suivantes à la politique clé, en les remplaçant par *REGIONACCOUNT*, et *KEY_ID* par vos propres valeurs.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnableRedshiftSystemTableKeyUsage",
      "Effect": "Allow",
      "Principal": {
        "Service": "systemtables.redshift.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:REGION:ACCOUNT:key/KEY_ID",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "ACCOUNT"
        }
      }
```

```
    },
    {
      "Sid": "EnableS3TableMaintenanceKeyUsage",
      "Effect": "Allow",
      "Principal": {
        "Service": "maintenance.s3tables.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:REGION:ACCOUNT:key/KEY_ID",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3tables:REGION:ACCOUNT:bucket/
aws-redshift/*"
        }
      }
    }
  ]
}
```

Si la politique clé n'accorde pas ces autorisations, Redshift ne peut pas écrire dans les tables S3 chiffrées et la livraison échoue.

Tables système prises en charge

Vous pouvez sélectionner l'une des vues de SYS_* surveillance suivantes à intégrer à S3 Tables. Pour obtenir une description des colonnes de chaque vue, choisissez le nom de la vue.

- SYS_ANALYZE_COMPRESSION_HISTORY
- SYS_ANALYZE_HISTORY
- OPTIMISATION AUTOMATIQUE DU SYSTÈME
- OPTIMISATION DE SYS_AUTO_TABLE
- SYS_CHILD_QUERY_TEXT
- SYS_CONNECTION_LOG
- SYS_COPY_JOB_INFO
- SYS_COPY_REPLACEMENTS
- SYS_DATASHARE_CHANGE_LOG

- SYS_DATASHARE_USAGE_CONSUMER
- SYS_DATASHARE_USAGE_PRODUCER
- SYS_DATASHARE_WRITE_HISTORY
- ERREUR SYS_EXTERNAL_QUERY_ERROR
- ACTIVITÉ_D'INTÉGRATION_SYSTÈME
- SYS_MV_STATE
- MESSAGES DE PROCÉDURE SYSTÈME
- SYS_QUERY_DETAIL
- SYS_QUERY_EXPLAIN
- SYS_QUERY_HISTORY
- SYS_QUERY_TEXT
- VIOLATIONS DES QUOTAS DU SCHÉMA SYSTÈME
- SYS_SESSION_HISTORY
- SYS_SPATIAL_SIMPLIFY
- ERREURS SYS_STREAM_SCAN
- SYS_STREAM_SCAN_STATES
- SYS_UNLOAD_DETAIL
- SYS_USERLOG
- SYS_VACUUM_HISTORY

> **Note**
>
> Les vues suivantes nécessitent le correctif P203 ou une version ultérieure : SYS_CHILD_QUERY_TEXT, SYS_COPY_REPLACEMENTS, SYS_EXTERNAL_QUERY_ERROR, SYS_PROCEDURE_MESSAGES, SYS_QUERY_DETAIL, SYS_QUERY_EXPLAIN, SYS_SPATIAL_SIMPLIFY et SYS_UNLOAD_DETAIL. Si vous activez ces vues sur un entrepôt de données exécutant un correctif antérieur à P203, les tables sont créées avec le schéma correct mais ne contiennent aucune donnée tant que l'entrepôt de données n'est pas mis à jour vers la version P203 ou ultérieure.

Colonnes de métadonnées ajoutées à chaque tableau

Chaque table S3 contient toutes les colonnes de la SYS_* vue source, ainsi que les cinq colonnes de métadonnées suivantes que Redshift ajoute pour identifier la source de chaque ligne et la date de livraison.

Colonne	Type	Description
warehouse_account_id	chaîne	Le AWS compte propriétaire de l'entrepôt de données source.
warehouse_region_name	chaîne	AWS Région dans laquelle fonctionne l'entrepôt de données source.
warehouse_namespace_arn	chaîne	L'ARN de l'espace de noms de l'entrepôt de données source. Il s'agit d'un identifiant unique et stable qui est immuable lors des renommages et des loisirs.
warehouse_name	chaîne	Le nom lisible par l'homme de l'entrepôt de données source (nom du cluster ou nom du groupe de travail).
s3_tables_ingestion_time	horodatage (6), UTC	Heure à laquelle Redshift a validé la ligne dans S3 Tables. Il s'agit du délai de livraison, et non de l'heure à laquelle l'événement sous-jacent s'est produit.

Configuration de la rétention

Redshift ne définit pas de politique de rétention pour les données qu'il fournit aux tables S3. Vous configurez la durée de conservation des données en définissant une politique d'expiration des enregistrements via S3 Tables. Vous spécifiez le nombre de jours (par exemple, 5 jours, 100 jours ou 365 jours) et S3 Tables supprime automatiquement les données qui dépassent la durée configurée.

Si vous ne configurez pas de politique d'expiration, les données sont conservées indéfiniment.

Lorsque vous désactivez l'intégration ou supprimez une table système, Redshift arrête d'écrire de nouvelles données, mais les données précédemment fournies restent dans les tables S3 et continuent d'être soumises à la politique d'expiration que vous avez configurée.

Pour plus d'informations, consultez la section Configuration de l'expiration des enregistrements pour les compartiments de tables S3 dans le guide de l'utilisateur Amazon S3.

Gouvernance des données

Vous régissez l'accès aux données des tables système conservées ; Redshift n'applique pas d'autorisations de lecture en votre nom et ne masque pas les données.

- Contrôle d'accès. Après avoir intégré le bucket de tables S3 à AWS Glue Data Catalog, vous pouvez gérer l'accès en lecture à l'aide de Gestion des identités et des accès AWS (IAM) ou AWS Lake Formation. Dans un déploiement consolidé, vous pouvez définir l'accès en lecture par entrepôt.
- Catalogage et découverte. L' AWS Glue Data Catalog intégration fournit un emplacement central pour découvrir les tables conservées et appliquer des autorisations précises (par exemple, accès au niveau des tables, des colonnes ou des lignes avec Lake Formation).

Comportement de livraison et de cycle de

- Fréquence de livraison. Les données sont fournies par lots à une fréquence fixe.
- Exactly-once livraison. Chaque enregistrement est livré une seule fois ; le fait de réactiver ou de rajouter une table système ne crée pas de doublons.
- Activez, désactivez, réactivez. Lorsque la fonctionnalité (ou une table système spécifique) est désactivée, aucune donnée n'est capturée pendant cette période. La désactivation arrête les écritures mais ne supprime pas les tables S3 ni les données fournies précédemment. Re-enabling reprend la livraison à l'avenir et ne comble pas l'écart.
- Suppression d'une table système de votre sélection. Redshift cesse de fournir de nouvelles données pour cette table système. Les données fournies précédemment restent dans les tables S3 et sont soumises à toute politique d'expiration des enregistrements que vous avez configurée. Re-adding la table système reprend la livraison sans dupliquer les données.
- Suppression de l'entrepôt de données contenant des données en vol. Si vous supprimez un entrepôt de données alors que la livraison est en cours et que la clé de chiffrement de l'entrepôt de données diffère de celle utilisée pour les tables S3, Redshift peut continuer à utiliser l' AWS

KMS autorisation associée à la clé de l'entrepôt de données pendant une courte période après la suppression afin de terminer la livraison des données restantes.

Vérification de l'état de livraison

Vous pouvez consulter la configuration actuelle et le délai de livraison le plus récent par tableau système à tout moment :

- Clusters provisionnés. `describe-logging-status`(ou`describe-cluster`) renvoie les tables système actives, l'espace de noms S3 Tables, la granularité et l'heure de dernière ingestion pour chaque table système.
- Redshift sans serveur. `get-namespace`renvoie les mêmes informations dans l'état de publication des tables S3 de l'espace de noms.

Redshift sans serveur

La livraison n'empêche pas un groupe de travail de rester éveillé et ne consomme pas votre ordinateur. Avant que le groupe de travail ne fasse une pause, Redshift s'assure que tout lot en attente est livré.

Bonnes pratiques

1. Évaluez la sensibilité de vos données. Déterminez quel type de données est stocké dans votre entrepôt de données et si les tables système contiennent des informations sensibles. Certaines tables système (telles que SYS_QUERY_TEXT et SYS_PROCEDURE_MESSAGES) peuvent capturer des valeurs littérales à partir de vos requêtes et de vos procédures stockées.
2. Choisissez un modèle de déploiement. Si votre entrepôt de données stocke des informations sensibles, envisagez d'utiliser le modèle de déploiement par entrepôt pour isoler physiquement les données de la table système de chaque entrepôt de données. Si vos données ne sont pas sensibles et que vous souhaitez exécuter des requêtes entre entrepôts sans combiner les résultats de plusieurs tables, utilisez le modèle de déploiement consolidé.
3. Sélectionnez les tables système dont vous avez besoin. Consultez la liste des tables système prises en charge et choisissez celles qui correspondent à vos exigences de conformité, d'audit ou d'observabilité. Il n'est pas nécessaire d'activer toutes les tables système.
4. Configurez le chiffrement avant d'activer la fonctionnalité. Si vous souhaitez utiliser une AWS KMS clé gérée par le client, spécifiez-la lors de la première activation de la fonctionnalité. Vous ne pouvez pas modifier la clé une fois que les tables S3 ont été créées. Pour modifier la clé,

désactivez la fonctionnalité, supprimez les tables S3 à l'aide de l'API S3 Tables (cela supprime définitivement les données conservées), puis réactivez la fonctionnalité avec la nouvelle clé.

5. Définissez la rétention en fonction des besoins de l'entreprise. Configurez la politique d'expiration des enregistrements directement dans S3 Tables au niveau de la table, en fonction de vos besoins de conformité, d'audit ou opérationnels. Les différentes tables peuvent avoir des durées de conservation différentes. Si vous ne configurez pas de politique d'expiration, les données sont conservées indéfiniment. Pour surveiller l'utilisation du stockage pour les tables de votre système, consultez les CloudWatch statistiques d'Amazon S3 Tables dans le guide de l'utilisateur Amazon S3.

Facturation

L'écriture des données des tables système dans S3 Tables est gratuite. Le stockage et la maintenance standard des tables S3 pour les données conservées, ainsi que le moteur de requête que vous utilisez pour lire les données, vous sont facturés conformément à la tarification de ce moteur. Pour plus d'informations, consultez la rubrique Tarification d'Amazon S3 Tables.

Considérations et restrictions

- Pris en charge au sein d'un seul AWS compte et d'une seule AWS région. Pour analyser les données de différents comptes ou régions, combinez les résultats au moment de la requête.
- Un entrepôt de données utilise un modèle de déploiement (par entrepôt ou consolidé) à la fois.
- Le fait de changer de modèle de déploiement, de désactiver et de réactiver, ou de supprimer et de rajouter une table système ne permet pas de remplir les données historiques.
- Les données fournies sont immuables. Vous ne pouvez pas modifier ou supprimer des lignes individuelles via Redshift.
- Vous pouvez supprimer les tables S3 créées par cette fonctionnalité, mais cela supprime définitivement toutes les données conservées dans ces tables et arrête la livraison. Redshift ne recrée pas automatiquement les tables supprimées. Pour reprendre la diffusion, vous devez réactiver la fonctionnalité, qui crée de nouvelles tables et commence à fournir de nouvelles données à l'avenir. Les données fournies précédemment ne sont pas restaurées. Pour plus d'informations, consultez la section Supprimer des tables S3 dans le guide de l'utilisateur Amazon S3.
- La livraison se fait par lots (les données sont écrites à une fréquence fixe).
- Les requêtes depuis Redshift nécessitent l'intégration du bucket de tables S3. AWS Glue Data Catalog

Validation de la conformité pour Amazon Redshift

Third-party les auditeurs évaluent la sécurité et la conformité d'Amazon Redshift dans le cadre de plusieurs programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d'autres.

Pour une liste des AWS services concernés par des programmes de conformité spécifiques, voir AWS Services concernés par programme de conformité. Pour obtenir des informations générales, veuillez consulter Programmes de conformité d'AWS.

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, consultez la section Téléchargement de rapports dans AWS Artifact.

Votre responsabilité de conformité lors de l'utilisation d'Amazon Redshift est déterminée par la sensibilité de vos données, les objectifs de conformité de votre organisation, ainsi que par la législation et la réglementation applicables. Si votre utilisation d'Amazon Redshift est soumise à la conformité à des normes telles que HIPAA, PCI ou FedRAMP, fournit des ressources pour vous aider à : AWS

- Guides de démarrage rapide sur la sécurité et la conformité qui abordent les considérations architecturales et les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur AWS.
- Livre blanc sur l'architecture pour la sécurité et la conformité HIPAA, qui décrit comment les entreprises peuvent créer des applications. AWS HIPAA-compliant
- AWS des ressources, des classeurs et des guides de conformité susceptibles de s'appliquer à votre secteur d'activité et à votre région.
- AWS Config, un AWS service, peut évaluer dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub CSPM, un AWS service, fournit une vue complète de votre état de sécurité AWS qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub CSPM utilise des contrôles de sécurité pour évaluer les configurations des ressources et les normes de sécurité afin de vous aider à vous conformer aux différents cadres de conformité. Pour plus d'informations sur l'utilisation de Security Hub CSPM pour évaluer les ressources Amazon Redshift, consultez les contrôles Amazon Redshift dans le guide de l'utilisateur.AWS Security Hub

Les documents de conformité et de sécurité suivants concernent Amazon Redshift et sont disponibles sur demande auprès de. AWS Artifact Pour de plus amples informations, veuillez consulter AWS Artifact.

- Cloud Computing Compliance Controls Catalogue (C5)
- ISO 27001 : Déclaration d'applicabilité 2013 (DdA)
- ISO 27001 : Certification 2013
- ISO 27017 : Déclaration d'applicabilité 2015 (DdA)
- ISO 27017 : Certification 2015
- ISO 27018 : Déclaration d'applicabilité 2015 (DdA)
- ISO 27018 : Certification 2014
- ISO 9001: Certification 2015
- Attestation de conformité (AOC) et récapitulatif des responsabilités PCI DSS
- Rapport SOC 1 (Service Organization Controls)
- Rapport SOC 2 (Service Organization Controls)
- Rapport SOC 2 (Service Organization Controls) relatif à la confidentialité

Résilience d'Amazon Redshift

L'infrastructure AWS mondiale est construite autour AWS des régions et des zones de disponibilité (AZ). AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées qui sont 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 de disponibilité à l’autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Presque toutes les AWS régions disposent de plusieurs zones de disponibilité et centres de données. Vous pouvez déployer vos applications dans plusieurs zones de disponibilité au sein d’une même Région pour bénéficier d’une tolérance aux pannes et d’une faible latence.

Pour déplacer un cluster vers une autre zone de disponibilité sans aucune perte de données ou modification de vos applications, vous pouvez relocaliser votre cluster. Avec la relocalisation, vous pouvez continuer les opérations en cas d’interruption de service sur votre cluster avec un impact minimal. Lorsque la relocalisation des clusters est activée, Amazon Redshift peut relocaliser les

clusters dans certaines situations. Pour plus d'informations sur la relocalisation dans Amazon Redshift, consultez Relocalisation d’un cluster.

Dans les scénarios de défaillance où un événement inattendu se produit dans une zone de disponibilité, vous pouvez configurer un déploiement de plusieurs zones de disponibilité (Multi-AZ) pour garantir que votre entrepôt de données Amazon Redshift puisse continuer à fonctionner. Amazon Redshift déploie des ressources de calcul égales dans deux zones de disponibilité accessibles via un seul point de terminaison. En cas de panne de l'ensemble d'une zone de disponibilité, les ressources de calcul restantes dans la seconde zone de disponibilité seront disponibles pour poursuivre le traitement des charges de travail. Pour plus d'informations sur les Multi-AZ déploiements, consultezMulti-AZ déploiement.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale. Pour plus d’informations sur l’utilisation d’Amazon Redshift pour la reprise après sinistre, consultez Implémenter la reprise après sinistre avec Amazon Redshift.

.

Sécurité de l'infrastructure dans Amazon Redshift

En tant que service géré, Amazon Redshift est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Amazon Redshift via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Des suites de chiffrement dotées d'un secret de transmission parfait (PFS), telles que DHE (Ephemeral) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

Isolement de réseau

Un cloud privé virtuel (VPC) basé sur le service Amazon VPC est votre réseau privé et logiquement isolé dans le cloud. AWS Vous pouvez déployer un cluster Amazon Redshift ou un groupe de travail sans serveur Redshift dans un VPC en procédant comme suit :

- Créez un VPC dans une AWS région. Pour de plus amples informations, veuillez consulter Qu'est-ce qu'Amazon VPC ? dans le Guide de l'utilisateur Amazon VPC.
- Créez au moins deux sous-réseaux VPC privés. Pour plus d'informations, consultez VPC et sous-réseaux dans le Guide de l'utilisateur Amazon VPC.
- Déployez un cluster Amazon Redshift ou un groupe de travail Redshift sans serveur. Pour plus d'informations, consultez Sous-réseaux pour les ressources Redshift ou Groupe de travail et espace de noms.

Par défaut, un cluster Amazon Redshift est verrouillé lors du provisionnement. Pour autoriser le trafic réseau entrant en provenance des clients Amazon Redshift, associez un groupe de sécurité de VPC à un cluster Amazon Redshift. Pour plus d'informations, consultez Sous-réseaux pour les ressources Redshift.

Pour autoriser le trafic uniquement vers ou en provenance de plages d'adresses IP spécifiques, mettez à jour les groupes de sécurité avec votre VPC. Par exemple, vous pouvez autoriser le trafic uniquement depuis ou vers votre réseau d'entrreprise.

Lorsque vous configurez les listes de contrôle d'accès réseau associées au (x) sous-réseau (s) associé (s) à votre cluster Amazon Redshift, assurez-vous que les plages d'adresses CIDR S3 de la région AWS concernée sont ajoutées à la liste d'autorisation pour les règles d'entrée et de sortie. Cela vous permet d'exécuter S3-based des opérations telles que Redshift Spectrum, COPY et UNLOAD sans aucune interruption.

L'exemple de commande suivant analyse la réponse JSON pour toutes les adresses IPv4 utilisées dans Amazon S3 dans la région us-east-1.

```
curl https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] |
 select(.region=="us-east-1") | select(.service=="S3") | .ip_prefix'

54.231.0.0/17

52.92.16.0/20
```

```
52.216.0.0/15
```

Pour savoir comment obtenir des plages d'adresses IP S3 pour une région donnée, consultez Plages d'adresses IP AWS.

Amazon Redshift prend en charge le déploiement des clusters dans des VPC de location dédiée. Pour de plus amples informations, veuillez consulter Instances dédiées dans le Guide de l'utilisateur Amazon EC2.

Groupes de sécurité Amazon Redshift

Lorsque vous allouez un cluster Amazon Redshift, il est verrouillé par défaut afin que personne n'y ait accès. Pour autoriser d'autres utilisateurs à accéder à un cluster Amazon Redshift, associez le cluster à un groupe de sécurité. Si vous utilisez la EC2-VPC plateforme, vous pouvez soit utiliser un groupe de sécurité Amazon VPC existant, soit en définir un nouveau, puis l'associer à un cluster. Pour plus d'informations sur la gestion d'un cluster sur la EC2-VPC plateforme, consultezRessources Redshift dans un VPC.

Points de terminaison de VPC d'Interface

Vous pouvez vous connecter directement à l'API Amazon Redshift et Amazon Redshift sans serveur à l'aide d'un point de terminaison de VPC d'interface (AWS PrivateLink) dans votre Virtual Private Cloud (VPC) au lieu de vous connecter via Internet. Pour plus d'informations sur les actions d'API Amazon Redshift, consultez Actions dans la Référence d'API Amazon Redshift. Pour plus d'informations sur les actions d'API Redshift sans serveur, consultez Actions dans la Référence d'API Amazon Redshift sans serveur. Pour de plus amples informations sur AWS PrivateLink, veuillez consulter Points de terminaison d'un VPC d'interface (AWS PrivateLink) dans le Guide de l'utilisateur Amazon VPC. Notez que la JDBC/ODBC connexion au cluster ou à l'espace de travail ne fait pas partie du service d'API Amazon Redshift.

Lorsque vous utilisez un point de terminaison VPC d'interface, la communication entre votre VPC et Amazon Redshift ou Redshift Serverless s'effectue entièrement au sein du réseau, ce qui peut renforcer la sécurité. AWS Chaque point de terminaison d'un VPC est représenté par une ou plusieurs interfaces réseau Elastic avec des adresses IP privées dans vos sous-réseaux VPC. Pour plus d'informations sur les interfaces réseau Elastic, veuillez consulter Interfaces réseau Elastic dans le Guide de l'utilisateur Amazon EC2.

Un point de terminaison de VPC d'interface connecte votre VPC directement à Amazon Redshift. Il n'utilise pas de passerelle Internet, de périphérique de traduction d'adresses réseau (NAT), de

connexion à un réseau privé virtuel (VPN) ou de Direct Connect connexion. Les instances de votre VPC ne nécessitent pas d'adresses IP publiques pour communiquer avec l'API Amazon Redshift.

Pour utiliser Amazon Redshift ou Redshift sans serveur via votre VPC, vous avez deux options. L'une consiste à vous connecter à partir d'une instance qui se trouve à l'intérieur de votre VPC. L'autre consiste à connecter votre réseau privé à votre VPC à l'aide d'une Site-to-Site VPN option ou. Direct Connect Pour plus d'informations sur Site-to-Site VPN les options, consultez la section Connexions VPN dans le guide de l'utilisateur Amazon VPC. Pour obtenir des informations sur Direct Connect, consultez Création d'une connexion dans le Guide de l'utilisateur Direct Connect .

Vous pouvez créer un point de terminaison VPC d'interface pour vous connecter à Amazon Redshift à Console de gestion AWS l'aide des commandes AWS Command Line Interface or AWS CLI(). Pour plus d'informations, consultez Création d'un point de terminaison d'interface.

Une fois que vous avez créé un point de terminaison de VPC d'interface, vous pouvez activer les noms d'hôte DNS privés pour le point de terminaison. Dans ce cas, le point de terminaison par défaut est le suivant :

- Amazon Redshift alloué : `https://redshift.Region.amazonaws.com`
- Amazon Redshift sans serveur : `https://redshift-serverless.Region.amazonaws.com`

Si vous n'activez pas les noms d'hôte DNS privés, Amazon VPC fournit un nom de point de terminaison DNS que vous pouvez utiliser au format suivant.

- Amazon Redshift alloué : `VPC_endpoint_ID.redshift.Region.vpce.amazonaws.com`
- Amazon Redshift sans serveur : `VPC_endpoint_ID.redshift-serverless.Region.vpce.amazonaws.com`

Pour de plus amples informations, consultez Points de terminaison VPC (AWS PrivateLink) dans le Guide de l'utilisateur Amazon VPC.

Amazon Redshift et Redshift sans serveur permettent d'appeler toutes les opérations d'API Amazon Redshift et les opérations d'API Redshift sans serveur au sein de votre VPC.

Vous pouvez attacher des politiques de point de terminaison de VPC à un point de terminaison VPC pour contrôler l'accès des entités Gestion des identités et des accès AWS (IAM). Vous pouvez également associer des groupes de sécurité à un point de terminaison de VPC pour contrôler l'accès entrant et sortant en fonction de l'origine et de la destination du trafic réseau. Un exemple est une

plage d'adresses IP. Pour plus d'informations, consultez Contrôle de l'accès aux services avec des points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Politiques de point de terminaison d'un VPC pour Amazon Redshift

Vous pouvez créer une politique pour les points de terminaison de VPC pour les instances de bloc-notes Amazon Redshift afin de spécifier les éléments suivants :

- Principal qui peut ou ne peut pas effectuer des actions
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Vous trouverez ci-dessous des exemples de politiques de point de terminaison de VPC.

Exemples de politiques de point de terminaison Amazon Redshift alloué

Vous trouverez ci-dessous des exemples de politiques de point de terminaison d'un VPC pour Amazon Redshift alloué.

Exemple : politique de point de terminaison VPC visant à refuser tout accès à partir d'un point spécifié AWS compte

La politique de point de terminaison VPC suivante refuse au AWS compte *123456789012* tout accès aux ressources utilisant ce point de terminaison.

```
{
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "*",
            "Effect": "Deny",
```

```
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Exemple : politique de point de terminaison d'un VPC pour autoriser l'accès VPC uniquement à un rôle IAM spécifié

La politique de point de terminaison VPC suivante autorise un accès complet uniquement au rôle IAM dans *redshiftrole* le compte. AWS *123456789012* Toutes les autres entités IAM se voient refuser l’accès à l’aide du point de terminaison.

```
   {
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::123456789012:role/redshiftrole"
                ]
            }
        }]
}
```

Il s'agit uniquement d'un exemple. Dans la plupart des cas d'utilisation, nous recommandons d'associer des autorisations à des actions spécifiques afin de réduire la portée des autorisations.

Exemple : politique de point de terminaison de VPC pour autoriser l'accès VPC uniquement à un principal IAM spécifié (utilisateur)

La politique de point de terminaison VPC suivante autorise un accès complet uniquement à l'utilisateur *redshiftadmin* IAM inscrit dans le compte. AWS *123456789012* Toutes les autres entités IAM se voient refuser l’accès à l’aide du point de terminaison.

```
   {
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::123456789012:user/redshiftadmin"
                ]
            }
        }]
}
```

Il s'agit uniquement d'un exemple. Dans la plupart des cas d'utilisation, nous recommandons d'associer des autorisations à un rôle avant de les attribuer à un utilisateur. En outre, nous vous recommandons d'utiliser des actions spécifiques pour réduire la portée des autorisations.

Exemple : politique de point de terminaison VPC pour autoriser les opérations Amazon Redshift en lecture seule

La politique de point de terminaison VPC suivante autorise uniquement le AWS compte *123456789012* à effectuer les actions Amazon Redshift spécifiées.

Les actions spécifiées fournissent l'équivalent d'un accès en lecture seule pour Amazon Redshift. Toutes les autres actions sur le VPC sont refusées pour le compte spécifié. En outre, tous les autres comptes se voient refuser tout accès. Pour afficher la liste des actions Amazon Redshift, veuillez consulter Actions, ressources et clés de condition pour Amazon Redshift dans le Guide de l'utilisateur IAM.

```
  {
    "Statement": [
        {
            "Action": [
                "redshift:DescribeAccountAttributes",
                "redshift:DescribeClusterParameterGroups",
                "redshift:DescribeClusterParameters",
                "redshift:DescribeClusterSecurityGroups",
                "redshift:DescribeClusterSnapshots",
```

```
                "redshift:DescribeClusterSubnetGroups",
                "redshift:DescribeClusterVersions",
                "redshift:DescribeDefaultClusterParameters",
                "redshift:DescribeEventCategories",
                "redshift:DescribeEventSubscriptions",
                "redshift:DescribeHsmClientCertificates",
                "redshift:DescribeHsmConfigurations",
                "redshift:DescribeLoggingStatus",
                "redshift:DescribeOrderableClusterOptions",
                "redshift:DescribeQuery",
                "redshift:DescribeReservedNodeOfferings",
                "redshift:DescribeReservedNodes",
                "redshift:DescribeResize",
                "redshift:DescribeSavedQueries",
                "redshift:DescribeScheduledActions",
                "redshift:DescribeSnapshotCopyGrants",
                "redshift:DescribeSnapshotSchedules",
                "redshift:DescribeStorage",
                "redshift:DescribeTable",
                "redshift:DescribeTableRestoreStatus",
                "redshift:DescribeTags",
                "redshift:FetchResults",
                "redshift:GetReservedNodeExchangeOfferings"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Exemple : politique de point de terminaison de VPC refusant l'accès à un cluster spécifié

La politique de point de terminaison de VPC suivante permet un accès complet à tous les comptes et entités. Dans le même temps, il refuse tout accès au AWS compte *123456789012* aux actions effectuées sur le cluster Amazon Redshift avec un identifiant de cluster. *my-redshift-cluster* D'autres actions Amazon Redshift qui ne prennent pas en charge les autorisations au niveau des ressources pour les clusters sont toujours autorisées. Pour obtenir une liste des actions

Amazon Redshift et de leur type de ressource correspondant, veuillez consulter la rubrique Actions, ressources et clés de condition pour Amazon Redshift dans le Guide de l'utilisateur IAM.

```
 {
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "*",
            "Effect": "Deny",
            "Resource": "arn:aws:redshift:us-east-1:123456789012:cluster:my-redshift-
cluster",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Exemples de politique de point de terminaison Amazon Redshift sans serveur

Vous trouverez ci-dessous des exemples de politiques de point de terminaison d'un VPC pour Redshift sans serveur.

Exemple : politique de point de terminaison VPC pour autoriser les opérations Redshift sans serveur en lecture seule

La politique de point de terminaison VPC suivante autorise uniquement le AWS compte *123456789012* à effectuer les actions Redshift Serverless spécifiées.

Les actions spécifiées fournissent l'équivalent d'un accès en lecture seule pour Redshift sans serveur. Toutes les autres actions sur le VPC sont refusées pour le compte spécifié. En outre, tous les autres comptes se voient refuser tout accès. Pour afficher la liste des actions Redshift sans

serveur, consultez Actions, ressources et clés de condition pour Redshift sans serveur dans le Guide de l'utilisateur IAM.

```
{
  "Statement": [
      {
          "Action": [
              "redshift-serverless:DescribeOneTimeCredit",
              "redshift-serverless:GetCustomDomainAssociation",
              "redshift-serverless:GetEndpointAccess",
              "redshift-serverless:GetNamespace",
              "redshift-serverless:GetRecoveryPoint",
              "redshift-serverless:GetResourcePolicy",
              "redshift-serverless:GetScheduledAction",
              "redshift-serverless:GetSnapshot",
              "redshift-serverless:GetTableRestoreStatus",
              "redshift-serverless:GetUsageLimit",
              "redshift-serverless:GetWorkgroup"
          ],
          "Effect": "Allow",
          "Resource": "*",
          "Principal": {
              "AWS": [
                  "123456789012"
              ]
          }
      }
  ]
}
```

Exemple : politique de point de terminaison de VPC refusant l'accès à un groupe de travail spécifié

La politique de point de terminaison de VPC suivante permet un accès complet à tous les comptes et entités. Dans le même temps, il refuse tout accès au AWS compte *123456789012* aux actions effectuées sur le groupe de travail Amazon Redshift avec un identifiant de groupe de travail. *my-redshift-workgroup* D'autres actions Amazon Redshift qui ne prennent pas en charge les autorisations au niveau des ressources pour les groupes de travail sont toujours autorisées. Pour obtenir une liste des actions Redshift sans serveur et de leur type de ressource correspondant, consultez la rubrique Actions, ressources et clés de condition pour Redshift sans serveur dans le Guide de l'utilisateur IAM.

```
 {
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "*",
            "Effect": "Deny",
            "Resource": "arn:aws:redshift-serverless:us-
east-1:123456789012:workgroup:my-redshift-workgroup",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Configuration et analyse des vulnérabilités dans Amazon Redshift

AWS gère les tâches de sécurité de base telles que l'application de correctifs au système d'exploitation client (OS) et aux bases de données, la configuration du pare-feu et la reprise après sinistre (DR). Ces procédures ont été vérifiées et certifiées par les tiers appropriés. Pour de plus amples informations, veuillez consulter Validation de la conformité pour Amazon Redshift, le Modèle de responsabilité partagée et les Bonnes pratiques en matière de sécurité, d'identité et de conformité.

Amazon Redshift applique automatiquement les mises à jour et les correctifs à votre entrepôt de données afin que vous puissiez rester concentré sur votre application, et non sur son administration. Les correctifs et les mises à niveau sont appliqués au cours d'une fenêtre de maintenance configurable. Pour de plus amples informations, veuillez consulter Fenêtres de maintenance.

L'éditeur de requêtes Amazon Redshift v2 est une application gérée AWS. Tous les correctifs et mises à jour sont appliqués AWS selon les besoins.

Connectez-vous à Redshift grâce aux sessions de Identity-enhanced rôles IAM

Vous pouvez utiliser IAM Identity Center pour fournir un accès fédéré à vos clusters Amazon Redshift et à vos groupes de travail sans serveur. Cette approche permet aux utilisateurs de s'authentifier à l'aide de leurs informations d'identification Identity Center.

Amazon Redshift fournit des opérations `GetIdentityCenterAuthToken` d'API pour générer un jeton autorisé contenant des informations d'identité utilisateur. Ces API sont disponibles à la fois pour les clusters provisionnés et pour les groupes de travail sans serveur. Les jetons permettent un accès simplifié par authentification unique aux bases de données Amazon Redshift à l'aide de votre configuration Identity Center existante.

Conditions préalables

Avant d'utiliser l'authentification Identity Center avec Amazon Redshift, assurez-vous de disposer des éléments suivants :

- Configuration du centre d'identité : IAM Identity Center doit être configuré sur votre compte avec les identités des utilisateurs et les attributions d'applications appropriées. Pour obtenir des instructions de configuration, consultez la section Configuration d'IAM Identity Center.

  > **Important**
  >
  > Si vous souhaitez vous connecter à Redshift, vous devez utiliser redshift:connect scope.

- Identity-enhanced informations d'identification : votre application doit utiliser des informations d'identification améliorées contenant des informations d'identité utilisateur intégrées. Pour plus d'informations, consultez la section Utilisation de sessions de rôles IAM à identité améliorée.
- Autorisations IAM : votre rôle ou utilisateur IAM doit disposer des autorisations nécessaires pour appeler l'`GetIdentityCenterAuthToken`API et accéder aux clusters ou groupes de travail spécifiés. Autorisations requises :
  - Pour les clusters provisionnés : `redshift:GetIdentityCenterAuthToken` sur les ARN des clusters (format :) `arn:aws:redshift:region:account:cluster:cluster-name`

  - Pour les groupes de travail sans serveur : `redshift-serverless:GetIdentityCenterAuthToken` sur les ARN des groupes de travail (format :) `arn:aws:redshift-serverless:region:account:workgroup/workgroup-name`
- Pilotes compatibles : utilisez des pilotes JDBC ou ODBC Amazon Redshift qui prennent en charge les jetons autorisés par Identity Center :
  - Pilotes JDBC : voir Installation et configuration du pilote JDBC Amazon Redshift version 2.x
  - Pilotes ODBC : voir Installation et configuration du pilote ODBC Amazon Redshift version 2.0
- Configuration réseau pour un routage VPC amélioré : si le routage VPC amélioré est activé, votre VPC doit être en mesure d'accéder aux services Identity Center. Les points de terminaison Interface VPC constituent la méthode recommandée pour fournir cette connectivité. Configurez cette connectivité avant que les utilisateurs ne se connectent. Pour plus d'informations sur les exigences de routage VPC améliorées pour Identity Center, consultezUtilisation AWS Authentification IAM Identity Center avec routage VPC amélioré.

Comment fonctionne l'authentification Identity Center

L'authentification Identity Center pour Amazon Redshift utilise le flux de travail suivant :

1. Votre application appelle l'`GetIdentityCenterAuthToken`API à l'aide d'informations d'identification améliorées qui contiennent des informations d'identité utilisateur intégrées.
2. Amazon Redshift valide l'identité de l'Identity Center et génère un jeton autorisé chiffré limité à des clusters ou à des groupes de travail spécifiques. Consultez des exemples de politiques IAM.
3. Votre application utilise ce jeton pour se connecter au cluster ou au groupe de travail Amazon Redshift spécifié.
4. Le plan de données Amazon Redshift valide le jeton et accorde l'accès en fonction des autorisations de l'utilisateur Identity Center dans l'application Identity Center.

> **Important**
>
> Cette API nécessite des informations d'identification améliorées. Pour plus d'informations, consultez la section Utilisation de sessions de rôles IAM à identité améliorée.
> Si vous appelez l'API sans informations d'identification améliorées, vous recevrez un `UnsupportedOperationFault` message d'erreur.

GetIdentityCenterAuthToken Opérations d'API

Amazon Redshift propose deux opérations d'`GetIdentityCenterAuthToken`API distinctes : l'une pour les clusters provisionnés et l'autre pour les groupes de travail sans serveur. Les deux opérations portent le même nom mais acceptent des paramètres différents selon le type de ressource cible.

GetIdentityCenterAuthToken pour les clusters provisionnés

Pour les clusters Amazon Redshift provisionnés, utilisez l'`GetIdentityCenterAuthToken`API du service Amazon Redshift pour générer un jeton autorisé.

Syntaxe de demande

```
{
   "ClusterIds": [ "string" ]
}
```

Paramètres de demande

ClusterIds

Liste des identifiants de cluster Amazon Redshift auxquels le jeton sera autorisé à accéder. Le jeton ne peut être utilisé que pour s'authentifier auprès des clusters spécifiés dans cette liste.

Type : tableau de chaînes

Contraintes de longueur : minimum d'un article. Maximum de 20 articles.

Obligatoire : oui

Exemples de commandes CLI

Exemple : obtenir un jeton autorisé pour un seul cluster

```
aws redshift get-identity-center-auth-token \
    --cluster-ids my-redshift-cluster
```

Exemple : obtenir un jeton autorisé pour plusieurs clusters

```
aws redshift get-identity-center-auth-token \
    --cluster-ids my-cluster-1 my-cluster-2
```

GetIdentityCenterAuthToken pour les groupes de travail sans serveur

Pour les groupes de travail Amazon Redshift Serverless, utilisez l'`GetIdentityCenterAuthToken`API du service Amazon Redshift Serverless pour générer un jeton autorisé.

Syntaxe de demande

```
{
   "WorkgroupNames": [ "string" ]
}
```

Paramètres de demande

WorkgroupNames

Liste des noms de groupes de travail Amazon Redshift Serverless auxquels le jeton sera autorisé à accéder. Le jeton ne peut être utilisé que pour s'authentifier auprès des groupes de travail spécifiés dans cette liste.

Type : tableau de chaînes

Contraintes de longueur : minimum d'un article. Maximum de 20 articles.

Obligatoire : oui

Exemples de commandes CLI

Exemple : obtenir un jeton autorisé pour un seul groupe de travail

```
aws redshift-serverless get-identity-center-auth-token \
    --workgroup-names my-workgroup
```

Exemple : obtenir un jeton autorisé pour plusieurs groupes de travail

```
aws redshift-serverless get-identity-center-auth-token \
    --workgroup-names workgroup-1 workgroup-2
```

Syntaxe de réponse

Les deux API renvoient la même structure de réponse :

```
{
   "AuthorizedToken": "string",
   "ExpirationTime": "timestamp"
}
```

Paramètres de réponse

AuthorizedToken

Un jeton autorisé chiffré qui contient les informations d'identité de l'utilisateur et la liste des clusters ou groupes de travail autorisés. Ce jeton doit être traité comme une donnée sensible.

Type : Chaîne

ExpirationTime

Date et heure d'expiration du jeton, en UTC. Les jetons sont valables pendant 1 heure à compter de leur génération.

Type : Timestamp

Exemple de réponse

```
{
    "AuthorizedToken":
 "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ1c2VyQGV4YW1wbGUuY29tIiwiaWF0IjoxNjQwOTk1MjAw
    "ExpirationTime": "2024-01-01T12:00:00Z"
}
```

Intégration des pilotes

Les pilotes Amazon Redshift prennent en charge l'authentification Identity Center via l'utilisation directe de jetons :

Utilisation directe des jetons

Après avoir appelé l'`GetIdentityCenterAuthToken`API pour obtenir un jeton, utilisez le type `IdpTokenAuthPlugin` with the `SUBJECT_TOKEN` token.

Configuration de la connexion :

```
plugin_name = com.amazon.redshift.plugin.IdpTokenAuthPlugin
token_type = SUBJECT_TOKEN
token = {encrypted_token_from_api_response}
```

Pour des informations détaillées sur les plug-ins d'authentification Identity Center et la configuration des pilotes, consultez la section Connexion à un cluster Amazon Redshift.

Exemple de code Java

Exemple de code Java pour se connecter à l'aide de l'authentification Identity Center :

```
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.SQLException;
import java.util.Properties;

// Get token from GetIdentityCenterAuthToken API
String token = "your_encrypted_token_from_api_response";

// Configure connection properties
Properties props = new Properties();
props.setProperty("user", "your_username");
props.setProperty("plugin_name", "com.amazon.redshift.plugin.IdpTokenAuthPlugin");
props.setProperty("token_type", "SUBJECT_TOKEN");
props.setProperty("token", token);

// Connect to Redshift
```

```
String url = "jdbc:redshift://your-cluster.region.redshift.amazonaws.com:5439/
your_database";
try (Connection conn = DriverManager.getConnection(url, props)) {
    // Use connection
    System.out.println("Connected successfully!");
} catch (SQLException e) {
    e.printStackTrace();
}
```

Exigences de la politique IAM

Pour utiliser l'authentification Identity Center avec Amazon Redshift, des autorisations IAM spécifiques sont requises au-delà des autorisations standard requises pour la connexion aux clusters et groupes de travail Amazon Redshift.

Autorisations d'API

Pour les clusters provisionnés, votre session de rôle IAM améliorée doit disposer des éléments suivants :

- `redshift:GetIdentityCenterAuthToken`sur les ARN des clusters (format :`arn:aws:redshift:region:account:cluster:cluster-name`)

Pour les groupes de travail sans serveur, votre session de rôle IAM améliorée doit comporter les éléments suivants :

- `redshift-serverless:GetIdentityCenterAuthToken`sur les ARN des groupes de travail (format :) `arn:aws:redshift-serverless:region:account:workgroup/workgroup-name`

Exemple de politiques IAM

Exemple de politique pour les clusters provisionnés :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "redshift:GetIdentityCenterAuthToken"
            ],
            "Resource": [
                "arn:aws:redshift:us-east-1:123456789012:cluster:my-cluster"
            ]
        }
    ]
}
```

Exemple de politique pour les groupes de travail sans serveur :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "redshift-serverless:GetIdentityCenterAuthToken"
            ],
            "Resource": [
                "arn:aws:redshift-serverless:us-east-1:123456789012:workgroup/my-
workgroup"
            ]
        }
    ]
}
```

Exemple de politique pour plusieurs ressources :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "redshift:GetIdentityCenterAuthToken"
            ],
            "Resource": [
                "arn:aws:redshift:*:123456789012:cluster/*"
            ]
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "redshift-serverless:GetIdentityCenterAuthToken"
            ],
            "Resource": [
                "arn:aws:redshift-serverless:*:123456789012:workgroup/*"
            ]
        }
    ]
}
```

Disponibilité par région

L'authentification Identity Center est disponible dans les AWS régions suivantes :

- Régions commerciales : toutes les régions Amazon Redshift prises en charge
- AWS GovCloud: Disponible dans us-gov-east-1 et us-gov-west-1
- Régions de Chine : Disponible en cn-north-1 et cn-northwest-1

> **Note**
>
> La disponibilité des fonctionnalités peut varier lors du déploiement initial.

Résolution des problèmes d'authentification Identity Center

Consultez les sections suivantes pour vous aider à résoudre les problèmes que vous rencontrez avec l'authentification Identity Center.

Rubriques

- erreurs d’API
- Erreurs de connexion

erreurs d’API

L'`GetIdentityCenterAuthToken`API peut renvoyer les erreurs suivantes :

- UnsupportedOperationFault— La demande a été faite sans informations d'identification améliorées ou la propagation de l'identité Identity Center n'est pas prise en charge dans la configuration actuelle.
- ClusterNotFoundFault (redshift :GetIdentityCenterAuthToken) — Un ou plusieurs des identifiants de cluster spécifiés n'existent pas ou vous n'êtes pas autorisé à y accéder.
- WorkgroupNotFoundFault (redshift-serverless :GetIdentityCenterAuthToken) — Un ou plusieurs des noms de groupes de travail spécifiés n'existent pas ou vous n'êtes pas autorisé à y accéder.
- InvalidParameterValueException— Les paramètres de demande ne sont pas valides, tels qu'une liste vide de clusters ou de groupes de travail ou plus de 20 éléments dans la liste.

Erreurs de connexion

Lorsque vous vous connectez à Amazon Redshift à l'aide de jetons Identity Center, vous pouvez rencontrer les erreurs suivantes :

- Les informations d'identification du jeton ont expiré ou ne sont pas valides : générez un nouveau jeton à l'aide de l'`GetIdentityCenterAuthToken`API et mettez à jour la configuration de votre connexion.
- jeton non valide : vérifiez le format du jeton et assurez-vous qu'il a été généré pour le cluster ou le groupe de travail approprié.
- TYPE_INVALID_TOKEN — Assurez-vous d'utiliser `token_type = SUBJECT_TOKEN` dans vos paramètres de connexion.
- le type de fournisseur d'identité « awsidc » n'est pas pris en charge. Vérifiez que votre cluster ou groupe de travail Amazon Redshift prend en charge l'authentification Identity Center et passez à une version compatible.
- AWS Le fournisseur d'identité iDC n'existe pas. Configurez l'intégration d'Identity Center pour votre ressource Amazon Redshift via la AWS console.
- Étendue non valide. Les informations d'identification de l'utilisateur ne sont pas autorisées à se connecter à Amazon Redshift. Vérifiez que l'utilisateur dispose des autorisations appropriées dans Identity Center et que le jeton a été généré pour les ressources appropriées.
- Échecs de connexion avec routage VPC amélioré — Lorsque le routage VPC amélioré est activé, Amazon Redshift accède aux services Identity Center via votre VPC. Vérifiez que votre VPC possède des points de terminaison VPC d'interface pour ces services. Vérifiez que les noms DNS privés sont activés pour chaque point de terminaison. Vérifiez que les groupes de sécurité des terminaux autorisent le trafic entrant sur le port TCP 443. Pour plus d'informations

sur les exigences de routage VPC améliorées pour Identity Center, consultezUtilisation AWS Authentification IAM Identity Center avec routage VPC amélioré.

Tâches de mise en réseau

Vous pouvez effectuer des tâches de mise en réseau, telles que la personnalisation de votre connexion à une base de données Redshift. Vous pouvez le faire pour contrôler le trafic à des fins de sécurité ou pour d'autres raisons. Vous pouvez également effectuer des DNS-related tâches, telles que la configuration d'un nom de domaine personnalisé pour vos ressources Redshift. Ces tâches de configuration sont disponibles si vous disposez d'un cluster alloué Amazon Redshift ou d'un groupe de travail Amazon Redshift sans serveur.

Rubriques

- Noms de domaine personnalisé pour les connexions client
- Redshift-managed Points de terminaison VPC
- Ressources Redshift dans un VPC
- Contrôle du trafic réseau avec le routage VPC amélioré Redshift

Noms de domaine personnalisé pour les connexions client

Vous pouvez créer un nom de domaine personnalisé, également appelé URL personnalisée, pour votre cluster Amazon Redshift et votre groupe de travail Amazon Redshift sans serveur. Il s'agit d'un enregistrement DNS facile à lire qui achemine les connexions client SQL vers votre point de terminaison. Vous pouvez le configurer à tout moment pour un cluster ou un groupe de travail existant. Il offre plusieurs avantages :

- Le nom de domaine personnalisé est une chaîne plus simple que l'URL par défaut, qui inclut généralement le nom du cluster ou du groupe de travail et la région. Il est plus facile à mémoriser et à utiliser.
- Vous pouvez acheminer rapidement le trafic vers un nouveau cluster ou groupe de travail, par exemple en cas de basculement. Ainsi, les clients n'ont pas à modifier la configuration lorsqu'ils se reconnectent. Les connexions peuvent être réacheminées de manière centralisée, avec un minimum de perturbations.
- Vous pouvez éviter de partager des informations privées comme le nom d'un serveur dans une URL de connexion. Vous pouvez le masquer dans une URL personnalisée.

Lorsque vous configurez un nom de domaine personnalisé à l'aide d'un CNAME, Amazon Redshift ne facture aucun frais supplémentaire. Votre fournisseur DNS peut vous facturer un nom de domaine si vous en créez un nouveau, mais ce coût est généralement faible.

Enregistrement d'un nom de domaine

La configuration du nom de domaine personnalisé comprend plusieurs tâches, parmi lesquelles l'enregistrement du nom de domaine personnalisé auprès de votre fournisseur DNS et la création d'un certificat. Après avoir effectué ces tâches, vous configurez le nom de domaine personnalisé dans la console Amazon Redshift ou dans la console Amazon Redshift Serverless, ou vous le configurez à l'aide de commandes. AWS CLI

Vous devez disposer d'un nom de domaine Internet enregistré pour configurer un nom de domaine personnalisé dans Amazon Redshift. Vous pouvez enregistrer un domaine Internet à l'aide de Route 53, ou utiliser un bureau d'enregistrement de domaine tiers. Vous effectuez ces tâches en dehors de la console Amazon Redshift. Un domaine enregistré est un prérequis pour terminer les procédures restantes visant à créer un domaine personnalisé.

> **Note**
>
> Si vous utilisez un cluster provisionné, la relocalisation doit être activée sur le celui-ci avant d'effectuer les étapes de configuration du nom de domaine personnalisé. Pour plus d'informations, consultez Relocalisation d'un cluster. Cette étape n'est pas obligatoire pour Amazon Redshift sans serveur.

Le nom de domaine personnalisé inclut généralement le domaine racine et un sous-domaine, comme `mycluster.example.com`. Pour le configurer, effectuez les opérations suivantes :

Création d'une entrée DNS CNAME pour votre nom de domaine personnalisé

1. Enregistrez un domaine racine, par exemple `example.com`. Vous pouvez éventuellement utiliser un domaine existant. Votre nom personnalisé peut être soumis à des restrictions relatives à des caractères particuliers ou à la validation de dénomination. Pour plus d'informations sur l'enregistrement d'un domaine avec Route 53, consultez Registering a new domain.
2. Ajoutez un enregistrement CNAME DNS qui pointe votre nom de domaine personnalisé vers le point de terminaison Redshift pour votre cluster ou groupe de travail. Vous pouvez trouver le point de terminaison dans les propriétés du cluster ou du groupe de travail, dans la console

Redshift ou Amazon Redshift sans serveur. Copiez l'URL JDBC disponible sous Informations générales dans les propriétés du cluster ou du groupe de travail. Les URL se présentent comme suit :

- Pour un cluster Amazon Redshift : `redshift-cluster-sample.abc123456.us-east-1.redshift.amazonaws.com`
- Pour un groupe de travail Amazon Redshift sans serveur : `endpoint-name.012345678901.us-east-1-dev.redshift-serverless-dev.amazonaws.com`

Si l'URL comporte un préfixe JDBC, supprimez-le.

> **Note**
>
> Les enregistrements DNS sont soumis à disponibilité, car chaque nom doit être unique et utilisable au sein de votre organisation.

Limites

Il existe quelques restrictions concernant la création d'enregistrements CNAME pour un domaine personnalisé :

- La création de plusieurs noms de domaine personnalisés pour le même cluster provisionné ou le même groupe de travail Amazon Redshift sans serveur n'est pas prise en charge. Vous ne pouvez associer qu'un seul enregistrement CNAME.
- L'association d'un enregistrement CNAME à plusieurs clusters ou groupes de travail n'est pas prise en charge. Le CNAME de chaque ressource Redshift doit être unique.

Après avoir enregistré votre domaine et créé l'enregistrement CNAME, vous sélectionnez un certificat nouveau ou existant. Vous effectuez cette étape en utilisant AWS Certificate Manager :

Nous vous recommandons de créer un certificat validé par le DNS répondant aux critères d'éligibilité au renouvellement géré, disponible avec AWS Certificate Manager. Le renouvellement géré implique qu'ACM renouvelle automatiquement vos certificats, ou vous envoie des notifications par e-mail quand la date d'expiration approche. Pour plus d'informations sur le renouvellement de certificats gérés, consultez Renouvellement géré des certificats ACM.

Demande de certificat pour un nom de domaine

Amazon Redshift ou Amazon Redshift sans serveur exigent un certificat SSL (Secure Sockets Layer) validé pour un point de terminaison personnalisé afin de sécuriser les communications et de vérifier la propriété du nom de domaine. Vous pouvez utiliser votre AWS Certificate Manager compte avec et AWS KMS key pour une gestion sécurisée des certificats. La validation de sécurité inclut la vérification complète du nom d'hôte (sslmode=verify-full).

Les renouvellements de certificats sont gérés par Amazon Redshift uniquement lorsque vous choisissez la validation DNS plutôt que la validation par e-mail. Si vous utilisez la validation par e-mail, vous pouvez utiliser le certificat, mais vous devez le renouveler vous-même avant son expiration. Nous vous recommandons de choisir la validation DNS pour votre certificat. Vous pouvez surveiller les dates d'expiration des certificats importés dans AWS Certificate Manager.

Demande de certificat auprès d'ACM pour un nom de domaine

1. Connectez-vous à la console ACM Console de gestion AWS et ouvrez-la à https://console.aws.amazon.com/acm/l'adresse.
2. Choisissez Request a certificate (Demander un certificat).
3. Saisissez votre nom de votre domaine personnalisé dans le champ Nom de domaine.

   > **Note**
   >
   > Vous pouvez spécifier de nombreux préfixes, en plus du domaine du certificat, afin d'utiliser un seul certificat pour plusieurs enregistrements de domaines personnalisés. À titre d'exemple, vous pouvez utiliser des enregistrements supplémentaires tels que `one.example.com` et `two.example.com`, ou un enregistrement DNS générique comme `*.example.com` avec le même certificat.

4. Choisissez Review and request.
5. Choisissez Confirm and request.
6. Pour que la demande soit valide et quACM puisse émettre le certificat, le propriétaire inscrit du domaine Internet doit préalablement approuver cette demande. Une fois les étapes terminées, assurez-vous que le statut apparaît comme Émis dans la console ACM.

Configuration d’un domaine personnalisé

Vous pouvez utiliser la console Amazon Redshift ou Amazon Redshift sans serveur pour créer l’URL de votre domaine personnalisé. Si vous ne l’avez pas configurée, la propriété Nom de domaine personnalisé apparaît sous la forme d’un tiret (–) sous Informations générales. Après avoir créé votre enregistrement CNAME et le certificat, vous associez le nom de domaine personnalisé au cluster ou groupe de travail.

Pour créer une association de domaine personnalisé, les autorisations IAM suivantes sont requises :

- `redshift:CreateCustomDomainAssociation` : vous pouvez restreindre l’autorisation à un cluster spécifique en ajoutant son ARN.
- `redshiftServerless:CreateCustomDomainAssociation` : vous pouvez restreindre l’autorisation à un groupe de travail spécifique en ajoutant son ARN.
- `acm:DescribeCertificate`

Il est recommandé d’associer des politiques d’autorisation à un rôle IAM, puis de l’attribuer à des utilisateurs et à des groupes, le cas échéant. Pour plus d’informations, consultez Identity and Access Management dans Amazon Redshift.

Vous attribuez le nom de domaine personnalisé en procédant comme suit.

1. Choisissez le cluster dans la console Redshift, ou le groupe de travail dans la console Amazon Redshift sans serveur, puis choisissez Créer un nom de domaine personnalisé dans le menu Action. Une boîte de dialogue s’affiche.
2. Entrez le nom du domaine personnalisé.
3. Sélectionnez l'ARN AWS Certificate Manager du certificat ACM. Confirmez vos modifications. Conformément aux instructions fournies dans les étapes que vous avez suivies pour créer le certificat, nous vous recommandons de choisir un certificat validé par le DNS éligible au renouvellement géré via AWS Certificate Manager.
4. Vérifiez dans les propriétés du cluster que le Nom de domaine personnalisé et l’ARN du certificat de domaine personnalisé sont renseignés avec les informations que vous avez saisies. La Date d’expiration du certificat de domaine personnalisé est également répertoriée.

Une fois le domaine personnalisé configuré, vous ne pouvez utiliser `sslmode=verify-full` que pour le nouveau domaine personnalisé. Vous ne pouvez pas l’utiliser pour le point de terminaison

par défaut. Mais vous pouvez toujours vous connecter au point de terminaison par défaut en utilisant d'autres modes SSL, tels que `sslmode=verify-ca`.

> **Note**
>
> Pour rappel, la relocalisation du cluster n'est pas une condition préalable à la configuration de fonctionnalités de mise en réseau Redshift supplémentaires. Il n'est pas nécessaire de l'activer pour activer les fonctionnalités suivantes :
>
> - Connexion à Redshift depuis un VPC entre comptes ou entre régions : vous pouvez vous connecter d'un cloud privé AWS virtuel (VPC) à un autre qui contient une base de données Redshift. Cela facilite par exemple la gestion de l'accès client à partir de comptes ou de VPC disparates, sans avoir à fournir un accès VPC local aux identités se connectant à la base de données. Pour plus d'informations, consultez Connexion à Amazon Redshift sans serveur à partir d'un point de terminaison de VPC Redshift dans un autre compte ou une autre région.
> - Configuration d'un nom de domaine personnalisé : vous pouvez créer un nom de domaine personnalisé, comme décrit dans cette rubrique, pour rendre le nom du point de terminaison plus pertinent et plus simple.

Connexion à votre cluster alloué Amazon Redshift ou à un groupe de travail Amazon Redshift sans serveur

Pour vous connecter à un nom de domaine personnalisé, les autorisations IAM suivantes sont requises pour un cluster alloué : `redshift:DescribeCustomDomainAssociations`. Pour Amazon Redshift sans serveur, vous n'avez pas besoin d'ajouter d'autorisations.

Il est recommandé d'associer des politiques d'autorisation à un rôle IAM, puis de l'attribuer à des utilisateurs et à des groupes, le cas échéant. Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift.

Après avoir terminé les étapes pour créer votre CNAME et l'attribuer à votre cluster ou groupe de travail dans la console, vous pouvez fournir l'URL personnalisée dans les propriétés de connexion de votre client SQL. Notez que la propagation du DNS peut prendre du temps juste après la création d'un enregistrement CNAME.

1. Ouvrez un client SQL. Par exemple, vous pouvez utiliser SQL/Workbench J. Ouvrez les propriétés d'une connexion et ajoutez le nom de domaine personnalisé pour la chaîne de connexion. Par exemple, `jdbc:redshift://mycluster.example.com:5439/dev?sslmode=verify-full`. Dans cet exemple, `dev` spécifie la base de données par défaut.
2. Ajoutez le nom d'utilisateur et le mot de passe de l'utilisateur de base de données.
3. Testez la connexion. Votre capacité à interroger les ressources de base de données telles que des tables spécifiques peut varier en fonction des autorisations accordées à l'utilisateur de base de données ou aux rôles de base de données Amazon Redshift attribués.

   Notez que s'il se trouve dans un VPC, vous devrez peut-être configurer votre cluster ou groupe de travail pour qu'il soit accessible publiquement afin de vous y connecter. Vous pouvez modifier ce paramètre dans les propriétés du réseau.

> **Note**
>
> Les connexions à un nom de domaine personnalisé sont prises en charge par les pilotes JDBC, ODBC et Python.

Changement de nom d'un cluster auquel un domaine personnalisé a été attribué

> **Note**
>
> Cette série d'étapes ne s'applique pas à un groupe de travail Amazon Redshift sans serveur. Vous ne pouvez pas changer le nom du groupe de travail.

Pour renommer un cluster doté d'un nom de domaine personnalisé, l'autorisation IAM `acm:DescribeCertificate` est requise.

1. Accédez à la console Amazon Redshift et choisissez le cluster dont vous souhaitez changer le nom. Choisissez Modifier pour modifier les propriétés du cluster.
2. Modifiez l'Identifiant du cluster. Vous pouvez également modifier d'autres propriétés du cluster. Ensuite, choisissez Enregistrer les modifications.

3. Une fois le cluster renommé, vous devez mettre à jour l'enregistrement DNS pour modifier l'entrée CNAME du domaine personnalisé afin qu'elle pointe vers le point de terminaison Amazon Redshift mis à jour.

Description des associations de domaines personnalisées

Utilisez les commandes de cette section pour obtenir une liste de noms de domaine personnalisés associés à un cluster provisionné spécifique ou à un groupe de travail Amazon Redshift sans serveur.

Vous avez besoin des autorisations suivantes :

- Pour un cluster provisionné : `redshift:DescribeCustomDomainAssociations`
- Pour un groupe de travail Amazon Redshift sans serveur : `redshiftServerless:ListCnameAssociations`

Il est recommandé d'associer des politiques d'autorisation à un rôle IAM, puis de l'attribuer à des utilisateurs et à des groupes, le cas échéant. Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift.

Voici un exemple de commande permettant de répertorier les noms de domaine personnalisés pour un cluster Amazon Redshift donné :

```
aws redshift describe-custom-domain-associations --custom-domain-name customdomainname
```

Vous pouvez exécuter cette commande lorsqu'un nom de domaine personnalisé est activé pour déterminer les noms de domaine personnalisés associés au cluster. Pour plus d'informations sur la commande CLI permettant de décrire les associations de domaines personnalisés, consultez describe-custom-domain-associations.

De même, l'exemple de commande suivant permet de répertorier les noms de domaine personnalisés pour un cluster Amazon Redshift sans serveur donné. Il existe différentes manières de procéder. Vous pouvez fournir uniquement le nom de domaine personnalisé :

```
aws redshift-serverless list-custom-domain-associations --custom-domain-
name customdomainname
```

Vous pouvez également obtenir les associations en fournissant uniquement l'ARN du certificat :

```
aws redshift-serverless list-custom-domain-associations --custom-domain-certificate-
arn certificatearn
```

Vous pouvez exécuter ces commandes lorsqu'un nom de domaine personnalisé est activé pour déterminer les noms de domaine personnalisés associés au groupe de travail. Vous pouvez également exécuter une commande pour obtenir les propriétés d'une association de domaines personnalisés. Pour ce faire, vous devez fournir le nom de domaine personnalisé et le nom du groupe de travail comme paramètres. Cela renvoie l'ARN du certificat, le nom du groupe de travail et le délai d'expiration du certificat du domaine personnalisé :

```
aws redshift-serverless get-custom-domain-association --workgroup-name workgroupname --
custom-domain-name customdomainname
```

Pour plus d'informations sur les commandes de référence CLI disponibles pour Amazon Redshift sans serveur, consultez redshift-serverless.

Association d'un domaine personnalisé à un autre certificat

Pour modifier l'association de certificat d'un nom de domaine personnalisé, les autorisations IAM suivantes sont requises :

- `redshift:ModifyCustomDomainAssociation`
- `acm:DescribeCertificate`

Il est recommandé d'associer des politiques d'autorisation à un rôle IAM, puis de l'attribuer à des utilisateurs et à des groupes, le cas échéant. Pour plus d'informations, consultez Identity and Access Management dans Amazon Redshift.

Utilisez la commande suivante pour associer le domaine personnalisé à un autre certificat. Les arguments `--custom-domain-name` et `custom-domain-certificate-arn` sont obligatoires. L'ARN du nouveau certificat doit être différent de l'ARN existant.

```
aws redshift modify-custom-domain-association --cluster-id redshiftcluster --custom-
domain-name customdomainname --custom-domain-certificate-arn certificatearn
```

L'exemple suivant montre comment associer le domaine personnalisé à un certificat différent pour un groupe de travail Amazon Redshift sans serveur.

```
aws redshift-serverless modify-custom-domain-association --workgroup-
name redshiftworkgroup --custom-domain-name customdomainname --custom-domain-
certificate-arn certificatearn
```

Vous devez attendre 30 secondes maximum pour pouvoir vous connecter au cluster. Ce délai est en partie dû au fait que le cluster Amazon Redshift met à jour ses propriétés. Un délai supplémentaire se rajoute lorsque le DNS est mis à jour. Pour plus d'informations sur l'API et chaque paramètre de propriété, consultez ModifyCustomDomainAssociation.

Suppression du domaine personnalisé

Pour supprimer le nom de domaine personnalisé, l'utilisateur doit disposer des autorisations nécessaires pour effectuer les actions suivantes :

- Pour un cluster provisionné : `redshift:DeleteCustomDomainAssociation`
- Pour un groupe de travail Amazon Redshift sans serveur : `redshiftServerless:DeleteCustomDomainAssociation`

Dans la console

Vous pouvez supprimer le nom de domaine personnalisé en sélectionnant le bouton Actions, puis en choisissant Supprimer le nom de domaine personnalisé. Après cela, vous pouvez toujours vous connecter au serveur en mettant à jour vos outils pour utiliser les points de terminaison répertoriés dans la console.

Utilisation d'une commande CLI

L'exemple suivant indique comment supprimer le nom de domaine personnalisé. L'opération de suppression nécessite que vous fournissiez le nom de domaine personnalisé existant pour le cluster.

```
aws redshift delete-custom-domain-association --cluster-id redshiftcluster --custom-
domain-name customdomainname
```

L'exemple suivant montre comment supprimer le nom de domaine personnalisé pour un groupe de travail Amazon Redshift sans serveur. Le nom de domaine personnalisé est un paramètre obligatoire.

```
aws redshift-serverless delete-custom-domain-association --workgroup-name workgroupname
 --custom-domain-name customdomainname
```

Pour de plus amples informations, veuillez consulter DeleteCustomDomainAssociation.

Redshift-managed Points de terminaison VPC

Par défaut, un cluster Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur est alloué dans un cloud privé virtuel (VPC). Le VPC est accessible depuis un autre VPC ou sous-réseau lorsque vous activez l'accès public ou définissez une passerelle Internet, un appareil NAT ou une connexion AWS Direct Connect pour acheminer le trafic vers ce dernier. Vous pouvez également accéder à un cluster ou à un groupe de travail en configurant un point de terminaison Redshift-managed VPC (alimenté par AWS PrivateLink).

Vous pouvez configurer un point de terminaison Redshift-managed VPC en tant que connexion privée entre un VPC contenant un cluster ou un groupe de travail et un VPC sur lequel un outil client est exécuté. Si le cluster ou le groupe de travail se trouve sur un autre compte, le propriétaire du compte (concédant) doit accorder l'accès au compte (concessionnaire) qui souhaite établir une connexion. Avec cette approche, vous pouvez accéder à l'entrepôt des données sans utiliser d'adresse IP publique ni acheminer le trafic sur Internet.

Voici les raisons les plus courantes pour autoriser l'accès à l'aide d'un point de Redshift-managed terminaison VPC :

- AWS le compte A souhaite autoriser un VPC du AWS compte B à accéder à un cluster ou à un groupe de travail.
- AWS le compte A souhaite autoriser un VPC qui est également dans le AWS compte A à accéder à un cluster ou à un groupe de travail.
- AWS le compte A souhaite autoriser un sous-réseau différent du VPC AWS au sein du compte A à accéder à un cluster ou à un groupe de travail.

Le flux de travail permettant de configurer un point de terminaison Redshift-managed VPC pour accéder à un cluster ou à un groupe de travail dans un autre compte est le suivant :

1. Le compte propriétaire accorde l'autorisation d'accès à un autre compte et spécifie l'ID de compte AWS et l'identifiant du VPC (ou de tous les VPC) du bénéficiaire.
2. Le compte bénéficiaire est informé qu'il est autorisé à créer un point de terminaison Redshift-managed VPC.
3. Le compte bénéficiaire crée un point de terminaison Redshift-managed VPC.

4. Le compte bénéficiaire accède au cluster ou au groupe de travail du compte propriétaire via le point de terminaison Redshift-managed VPC.

Vous pouvez le faire à l'aide de la console Amazon Redshift, de ou de l' AWS CLI API Amazon Redshift.

Considérations relatives à l'utilisation de points de Redshift-managed terminaison VPC

> **Note**
>
> Pour créer ou modifier des points de terminaison Redshift-managed VPC, vous avez besoin d'une autorisation `ec2:CreateVpcEndpoint` ou d'une autorisation figurant `ec2:ModifyVpcEndpoint` dans votre politique IAM, en plus des autres autorisations spécifiées dans la politique gérée. AWS `AmazonRedshiftFullAccess`

Lorsque vous utilisez des points de terminaison Redshift-managed VPC, gardez à l'esprit les points suivants :

- Si vous utilisez un cluster provisionné, il doit avoir le type de nœud RG ou RA3. Un groupe de travail Amazon Redshift sans serveur permet également de configurer un point de terminaison d’un VPC.
- Pour les clusters provisionnés, assurez-vous que le cluster est activé pour la relocalisation du cluster ou Multi-AZ. Pour plus d’informations sur les conditions requises pour activer la relocalisation du cluster, consultez Relocalisation d’un cluster. Pour plus d'informations sur l'activation Multi-AZ, consultezConfiguration Multi-AZ lors de la création d'un nouveau cluster.
- Assurez-vous que le cluster ou groupe de travail auquel vous devez accéder via son groupe de sécurité est disponible dans les plages de ports valides 5431-5455 et 8191-8215. La valeur par défaut est 5439.
- Vous pouvez modifier les groupes de sécurité VPC associés à un point de terminaison VPC existant. Redshift-managed Pour modifier d'autres paramètres, supprimez le point de terminaison Redshift-managed VPC actuel et créez-en un nouveau.
- Le nombre de points de terminaison Redshift-managed VPC que vous pouvez créer est limité à votre quota de points de terminaison VPC.

- Les points de terminaison Redshift-managed VPC ne sont pas accessibles depuis Internet. Un point de terminaison Redshift-managed VPC est uniquement accessible au sein du VPC où le point de terminaison est provisionné ou à partir de tout VPC apparenté au VPC où le point de terminaison est provisionné conformément aux tables de routage et aux groupes de sécurité.
- Vous ne pouvez pas utiliser la console Amazon VPC pour gérer les points de terminaison VPC. Redshift-managed
- Lorsque vous créez un point de terminaison Redshift-managed VPC pour un cluster provisionné, le VPC que vous choisissez doit avoir un groupe de sous-réseaux. Pour créer un groupe de sous-réseaux, consultez Création d'un groupe de sous-réseaux de cluster..
- Si une zone de disponibilité est hors service, Amazon Redshift ne crée pas de nouvelle interface de réseau Elastic dans une autre zone de disponibilité. Dans ce cas, vous devrez peut-être créer un point de terminaison.

Pour plus d'informations sur les quotas et les contraintes de nommage, consultez Quotas et limites d'Amazon Redshift.

Pour plus d'informations sur la tarification, consultez Tarification AWS PrivateLink.

Accès accordé à un VPC

Si le VPC auquel vous souhaitez donner accès à votre cluster ou groupe de travail se trouve dans un autre compte AWS , assurez-vous de l'autoriser à partir du compte du propriétaire (concédant).

Pour autoriser un VPC dans un autre AWS compte pour avoir accès à votre cluster ou groupe de travail

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Clusters. Pour Amazon Redshift sans serveur, choisissez Tableau de bord sans serveur.
3. Affichez les détails du cluster auquel vous souhaitez autoriser l'accès en choisissant le nom du cluster. Choisissez l'onglet Properties (Propriétés) pour le cluster.

   La section Granted accounts (Comptes autorisés) affiche les comptes et les VPC correspondants ayant accès à votre cluster. Pour un groupe de travail Amazon Redshift sans serveur, choisissez le groupe de travail. Les Comptes accordés sont disponibles sous l'onglet Accès aux données.

4. Choisissez Grant access (Accorder l’accès) pour afficher un formulaire permettant de saisir les informations du bénéficiaire afin d’ajouter un compte.
5. Dans ID du compte AWS , saisissez l’ID du compte auquel vous accordez l’accès. Vous pouvez accorder l’accès à des VPC spécifiques ou à tous les VPC du compte spécifié.
6. Choisissez l’option Grant access (Accorder l’accès) pour accorder l’accès.

Création d'un point de Redshift-managed terminaison VPC

Si vous possédez un cluster ou un groupe de travail, ou si vous avez obtenu l'accès pour le gérer, vous pouvez créer un point de terminaison Redshift-managed VPC pour celui-ci.

Pour créer un point de Redshift-managed terminaison VPC

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Configurations.

   La page Configurations affiche les points de terminaison Redshift-managed VPC qui ont été créés. Pour afficher les détails d’un point de terminaison, choisissez son nom. Pour Amazon Redshift sans serveur, les points de terminaison d’un VPC se trouvent sous l’onglet Accès aux données, lorsque vous choisissez le groupe de travail.
3. Choisissez Create endpoint (Créer un point de terminaison) pour afficher un formulaire permettant de saisir des informations sur le point de terminaison à ajouter.
4. Entrez des valeurs pour le nom du point de terminaison, l’ID de compte AWS à 12 chiffres, le cloud privé virtuel (VPC) où se trouve le point de terminaison, le sous-réseau et le groupe de sécurité VPC.

   Le sous-réseau figurant dans Sous-réseau définit les sous-réseaux et les adresses IP où Amazon Redshift déploie le point de terminaison. Amazon Redshift choisit un sous-réseau dont les adresses IP sont disponibles pour l’interface réseau associée au point de terminaison.

   Le groupe de sécurité figurant dans Groupe de sécurité VPC définit les ports, les protocoles et les sources de trafic entrant que vous autorisez pour votre point de terminaison. Vous autorisez au groupe de sécurité ou à la plage CIDR où s’exécutent vos charges de travail l’accès au port sélectionné.
5. Choisissez Create endpoint (Créer un point de terminaison) pour créer le point de terminaison.

Une fois votre point de terminaison créé, vous pouvez accéder au cluster ou au groupe de travail via l'URL indiquée dans URL du point de terminaison dans les paramètres de configuration de votre point de terminaison Redshift-managed VPC.

Ressources Redshift dans un VPC

Vous pouvez lancer un cluster Amazon Redshift ou un groupe de travail Amazon Redshift Serverless dans un VPC sur la EC2-VPC plate-forme en fonction du service Amazon VPC. Pour de plus amples informations, veuillez consulter Utiliser EC2 pour créer votre cluster.

> **Note**
>
> Le lancement de clusters et de groupes de travail sans serveur dans des VPC de location dédiés n'est pas pris en charge. Pour plus d'informations, consultez Instances dédiées dans le Guide de l'utilisateur Amazon VPC pour les instances Linux.

Lorsque vous provisionnez des ressources dans un VPC, procédez comme suit :

- Fournissez des informations de VPC.

  Lorsque vous créez un cluster alloué dans votre VPC, vous devez fournir vos informations de VPC en créant d'abord un groupe de sous-réseaux de cluster. Ces informations comprennent l'ID de VPC et une liste des sous-réseaux dans votre VPC. Lorsque vous lancez un cluster, vous fournissez le groupe de sous-réseaux afin que Redshift puisse le provisionner dans l'un des sous-réseaux du VPC. Avec Amazon Redshift sans serveur, le processus est similaire. Vous attribuez des sous-réseaux directement à votre groupe de travail sans serveur. Mais dans le cas de sans serveur, vous ne créez pas de groupe de sous-réseaux. Pour plus d'informations sur la création de groupes de sous-réseaux dans Amazon Redshift, consultez Sous-réseaux pour les ressources Redshift. Pour plus d'informations sur la configuration du VPC, consultez Démarrer avec Amazon VPC dans le Guide de mise en route Amazon VPC.
- Vous pouvez configurer les options d'accessibilité (facultatif).

  Les clusters alloués et les groupes de travail sans serveur dans Amazon Redshift sont privés par défaut. Si vous configurez votre cluster alloué ou groupe de travail sans serveur pour qu'il soit accessible au public, Amazon Redshift utilise une adresse IP Elastic pour l'adresse IP externe. Une adresse IP Elastic est une adresse IP statique. Elle vous permet de modifier votre configuration sous-jacente sans affecter l'adresse IP que les clients utilisent pour se connecter. Cette approche

peut être utile pour des situations telles que la récupération après une défaillance. La création d'une adresse IP Elastic dépend de vos paramètres de relocalisation de la zone de disponibilité. Deux options s'offrent à vous :

1. Si la relocalisation de la zone de disponibilité est activée et que vous souhaitez activer l'accès public, vous ne devez pas spécifier d'adresse IP Elastic. Une adresse IP Elastic gérée par Amazon Redshift est attribuée. Elle est associée à votre compte AWS .
2. Si vous avez désactivé la relocalisation de la zone de disponibilité et que vous souhaitez activer l'accès public, vous pouvez choisir de créer une adresse IP Elastic pour le VPC dans Amazon EC2 avant de lancer votre cluster ou groupe de travail Amazon Redshift. Si vous ne créez pas d'adresse IP, Amazon Redshift fournit une adresse IP Elastic configurée à utiliser pour le VPC. Cette adresse IP élastique est gérée par Amazon Redshift et n'est pas associée à votre AWS compte.

Pour plus d'informations, consultez la rubrique Adresses IP Elastic dans le Guide de l'utilisateur Amazon EC2.

Dans certains cas, vous pouvez avoir un cluster accessible publiquement dans un VPC auquel vous souhaitez le connecter en utilisant l'adresse IP privée depuis le VPC. Le cas échéant, définissez les paramètres de VPC suivants sur `true` :

- `DNS resolution`
- `DNS hostnames`

Notez qu'avec Amazon Redshift sans serveur, vous ne pouvez pas vous connecter de cette manière.

Supposons que vous ayez un cluster alloué accessible publiquement dans un VPC, mais que vous ne définissiez pas ces paramètres sur `true` dans le VPC. Le cas échéant, les connexions effectuées depuis le VPC résolvent l'adresse IP Elastic des ressources au lieu de l'adresse IP privée. Nous vous recommandons de définir ces paramètres sur `true` et d'utiliser l'adresse IP privée pour un cluster accessible publiquement lors de la connexion depuis le VPC. Pour plus d'informations, consultez Utilisation de DNS avec votre VPC dans le Amazon VPC Guide de l'utilisateur.

> **Note**
>
> Si vous disposez d'un cluster accessible publiquement existant dans un VPC, les connexions depuis le VPC continuent d'utiliser l'adresse IP Elastic pour se connecter au

cluster jusqu'à ce qu'il soit redimensionné s'il s'agit d'un cluster alloué. Cela se produit même avec l'ensemble de paramètres précédent. Les nouveaux clusters créés suivent le nouveau comportement consistant à utiliser l'adresse IP privée lors de la connexion au cluster accessible publiquement depuis le même VPC.

L'adresse IP Elastic est une adresse IP externe qui permet d'accéder à une ressource en dehors d'un VPC. Pour un cluster alloué, elle n'est pas liée aux adresses IP publiques ni aux adresses IP privées qui sont affichées dans la console Amazon Redshift sous Adresses IP du nœud. Les adresses IP de nœud de cluster publiques et privées nœud s'affichent, que le cluster soit accessible ou non. Elles sont utilisées dans certaines circonstances pour configurer les règles d'entrée sur l'hôte distant. Ces circonstances ont lieu lorsque vous chargez des données depuis une instance Amazon EC2 ou un autre hôte distant à l'aide d'une connexion SSH (Secure Shell). Pour plus d'informations, consultez Étape 1 : Récupérer la clé publique de cluster et les adresses IP de nœud de cluster dans le Manuel du développeur de base de données Amazon Redshift.

> **Note**
>
> Les adresses IP de nœud ne s'appliquent pas à un groupe de travail Redshift sans serveur.

L'option permettant d'associer un cluster alloué à une adresse IP Elastic est disponible lorsque vous créez le cluster ou que vous restaurez le cluster à partir d'un instantané. Dans certains cas, vous pouvez avoir besoin d'associer le cluster à une adresse IP Elastic ou de modifier une adresse IP Elastic qui est associée au cluster. Pour attacher une adresse IP élastique après la création du cluster, mettez d'abord à jour le cluster afin qu'il ne soit pas accessible au public, puis rendez-le accessible au public et ajoutez une adresse IP élastique au cours de la même opération.

Pour plus d'informations sur la façon de rendre un cluster alloué ou un groupe de travail Amazon Redshift sans serveur accessible au public et d'attribuer une adresse IP Elastic, consultez Accessibilité publique avec une configuration de groupe de sécurité par défaut ou personnalisée.

- Associer un groupe de sécurité VPC.

  Vous accordez l'accès entrant à l'aide d'un groupe de sécurité VPC. Pour plus d'informations, consultez Configuration des paramètres de communication des groupes de sécurité pour les clusters Amazon Redshift, qui fournit des conseils sur la configuration des règles entrantes et sortantes entre un client et un cluster provisionné ou un groupe de travail Amazon Redshift sans

serveur. Une autre ressource qui vous aide à comprendre les groupes de sécurité est Sécurité de votre VPC dans le Guide de l'utilisateur Amazon VPC.

Restauration d'un instantané d'un cluster alloué ou d'un groupe de travail sans serveur dans un VPC

Un instantané d'un cluster ou d'un groupe de travail sans serveur dans un VPC peut être restauré uniquement dans un VPC, pas en dehors du VPC. Vous pouvez le restaurer dans le même VPC ou dans un autre VPC de votre compte. Pour plus d'informations sur les instantanés, consultez Instantanés et sauvegardes Amazon Redshift.

Création d'un cluster alloué Amazon Redshift ou d'un groupe de travail Amazon Redshift sans serveur dans un VPC

Voici les grandes étapes que vous devez suivre pour déployer un cluster ou un groupe de travail dans votre cloud privé virtuel (VPC).

Pour créer un cluster ou un groupe de travail sans serveur dans un VPC

1. Configurer un VPC : cous pouvez créer vos ressources Redshift dans le VPC par défaut pour votre compte, si votre compte en a un, ou dans un VPC que vous avez créé. Pour plus d'informations, consultez Utiliser EC2 pour créer votre cluster. Pour créer un VPC, consultez Sous-réseaux de votre VPC dans le Guide de l'utilisateur Amazon VPC. Prenez note de l'identificateur de VPC, du sous-réseau et de la zone de disponibilité du sous-réseau. Vous avez besoin de ces informations au moment du lancement de votre cluster ou groupe de travail.

   > **Note**
   >
   > Vous devez disposer d'au moins un sous-réseau défini dans votre VPC afin de l'ajouter au groupe de sous-réseaux à la prochaine étape. Pour en savoir plus sur l'ajout d'un sous-réseau à votre VPC, consultez Ajout d'un sous-réseau à votre VPC dans le Guide de l'utilisateur Amazon VPC.

2. Créez un groupe de sous-réseau de cluster Amazon Redshift pour spécifier quel sous-réseau votre cluster Amazon Redshift peut utiliser dans le VPC. Pour Redshift sans serveur, vous ne créez pas de groupe de sous-réseaux, mais vous attribuez plutôt un ensemble de sous-réseaux à votre groupe de travail lorsque vous le créez. Vous pouvez effectuer cette opération dans le Tableau de bord sans serveur lorsque vous créez un groupe de travail.

Vous pouvez créer un groupe de sous-réseaux à l'aide de la console Amazon Redshift ou par programmation. Pour plus d'informations, consultez Sous-réseaux pour les ressources Redshift.

3. Autorisez l'accès aux connexions entrantes dans un groupe de sécurité VPC que vous associez au cluster ou au groupe de travail. Vous pouvez activer un client en dehors du VPC (sur l'Internet public) pour la connexion au cluster. Pour cela, vous associez le cluster à un groupe de sécurité VPC qui octroie l'accès entrant. Pour plus d'informations, consultez Configuration des paramètres de communication des groupes de sécurité pour un cluster Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur.
4. Suivez les étapes pour créer un cluster dans la console allouée Redshift ou un groupe de travail dans la console Amazon Redshift sans serveur. Dans Réseau et sécurité, spécifiez le cloud privé virtuel (VPC), le groupe de sous-réseaux du cluster et le groupe de sécurité du VPC que vous avez configurés.

   Pour une présentation détaillée des étapes à suivre pour créer un cluster alloué d'entrepôts de donnée, consultez la section Commencer avec les entrepôts de données alloués Amazon Redshift dans le Guide de démarrage Amazon Redshift. Pour plus d'informations sur la création d'un groupe de travail Amazon Redshift sans serveur, consultez Commencer avec les entrepôts de données Amazon Redshift sans serveur dans le Guide de démarrage Amazon Redshift.

Vous pouvez suivre les étapes de mise en route pour tester le cluster ou le groupe de travail, par exemple en chargeant des exemples de données et en essayant d'exécuter des exemples de requêtes. Pour plus d'informations, consultez Commencer avec les entrepôts de données Amazon Redshift sans serveur dans le Guide de démarrage Amazon Redshift.

Groupes de sécurité VPC

Lorsque vous provisionnez un cluster Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur, l'accès est restreint par défaut afin que personne n'y ait accès. Pour autoriser l'accès entrant à d'autres utilisateurs, associez-le à un groupe de sécurité. Si vous utilisez la EC2-VPC plateforme, vous pouvez utiliser un groupe de sécurité Amazon VPC existant ou en définir un nouveau. Vous l'associez ensuite à un cluster ou un groupe de travail tel que décrit ci-après. Si vous êtes sur la EC2-Classic plateforme, vous définissez un groupe de sécurité et vous l'associez à votre cluster ou groupe de travail. Pour plus d'informations sur l'utilisation des groupes de sécurité sur la EC2-Classic plateforme, consultezGroupes de sécurité Amazon Redshift.

Un groupe de sécurité VPC se compose d'un ensemble de règles qui contrôlent l'accès à une instance du VPC, tel que votre cluster. Des règles individuelles définissent l'accès en fonction de plages d'adresses IP ou sur d'autres groupes de sécurité VPC. Lorsque vous associez un groupe de sécurité VPC à un cluster ou un groupe de travail, les règles définies dans le groupe de sécurité VPC contrôlent l'accès.

Chaque cluster que vous provisionnez sur la EC2-VPC plateforme est associé à un ou plusieurs groupes de sécurité Amazon VPC. Amazon VPC fournit un groupe de sécurité VPC appelé default, qui est créé automatiquement lorsque vous créez le VPC. Chaque cluster que vous lancez dans le VPC est automatiquement associé au groupe de sécurité VPC par défaut si vous ne spécifiez pas un autre groupe de sécurité VPC lors de la création de vos ressources Redshift. Vous pouvez associer un groupe de sécurité VPC à un cluster lorsque vous créez le cluster ou vous pouvez associer un groupe de sécurité VPC ultérieurement en modifiant le cluster.

La capture d'écran ci-après montre les règles par défaut pour le groupe de sécurité VPC par défaut.

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The security group ID (*sg-xxxxxxxx*)	All	All	Allow inbound traffic from instances assigned to the same security group
Outbound			
Destination	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	All	All	Allow all outbound traffic

Vous pouvez modifier les règles du groupe de sécurité VPC par défaut en fonction des besoins.

Si le groupe de sécurité VPC par défaut vous suffit, vous n'avez pas besoin d'en créer un autre. Cependant, vous pouvez éventuellement créer des groupes de sécurité VPC supplémentaires pour mieux gérer l'accès entrant. Par exemple, supposons que vous exécutiez un service sur un cluster Amazon Redshift ou un groupe de travail sans serveur et que vous ayez plusieurs niveaux de service distincts à fournir à vos clients. Si vous ne voulez pas fournir le même accès à tous les niveaux de service, vous pouvez créer des groupes de sécurité VPC distincts, un par niveau de service. Vous pouvez ensuite associer ces groupes de sécurité VPC à votre cluster ou vos groupes de travail.

Vous pouvez créer jusqu'à 100 groupes de sécurité VPC pour un VPC et associer un groupe de sécurité VPC à plusieurs clusters et groupes de travail. Notez toutefois que le nombre de groupes de sécurité VPC que vous pouvez associer à un cluster ou un groupe de travail est limité.

Amazon Redshift applique immédiatement les modifications à un groupe de sécurité VPC. Donc, si vous avez associé le groupe de sécurité VPC à un cluster, les règles d'accès au cluster entrant dans le groupe de sécurité VPC mis à jour s'appliquent immédiatement.

Vous pouvez créer et modifier des groupes de sécurité VPC à https://console.aws.amazon.com/vpc/ l'adresse. Vous pouvez également gérer les groupes de sécurité VPC par programmation à l'aide de l' AWS CLI interface de ligne de commande Amazon EC2 et du. AWS Tools for Windows PowerShell Pour plus d'informations sur l'utilisation des groupes de sécurité VPC, consultez Groupes de sécurité pour votre VPC dans le Guide de l'utilisateur Amazon VPC.

Configuration des paramètres de communication des groupes de sécurité pour un cluster Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur

Cette rubrique vous aide à configurer vos groupes de sécurité afin d'acheminer et de recevoir le trafic réseau de manière appropriée. Voici quelques cas d'utilisation courants :

- Vous activez l'accès public pour un cluster Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur, mais celui-ci ne reçoit pas de trafic. Pour cela, vous devez configurer une règle entrante pour autoriser le trafic à y accéder depuis Internet.
- Votre cluster ou groupe de travail n'est pas publiquement accessible, et vous utilisez le groupe de sécurité du VPC pré-configuré par défaut de Redshift pour autoriser le trafic entrant. Or, vous êtes tenu d'utiliser un groupe de sécurité différent de celui par défaut, et ce groupe de sécurité personnalisé n'autorise pas le trafic entrant. Vous devez le configurer pour autoriser la communication.

Les sections suivantes vous aident à choisir la bonne réponse pour chaque cas d'utilisation et vous montrent comment configurer le trafic réseau selon vos besoins. Vous pouvez éventuellement suivre les étapes permettant de configurer la communication à partir d'autres groupes de sécurité privés.

> **Note**
>
> Dans la plupart des cas, les paramètres de trafic réseau ne sont pas configurés automatiquement dans Amazon Redshift. Cela est dû au fait qu'ils peuvent varier à un niveau granulaire, selon que le trafic provient d'Internet ou d'un groupe de sécurité privé, et que les exigences de sécurité varient.

Accessibilité à tous avec une configuration de groupe de sécurité par défaut ou personnalisée

Si vous créez un cluster ou que vous possédez déjà un cluster ou un groupe de travail, effectuez les étapes de configuration suivantes pour le rendre accessible à tous. Vous devez suivre cette procédure, que vous optiez pour le groupe de sécurité par défaut ou pour un groupe de sécurité personnalisé :

1. Trouvez les paramètres réseau :

   - Pour un cluster Amazon Redshift provisionné, choisissez l'onglet Propriétés, puis sous Paramètres réseau et sécurité, sélectionnez le VPC pour votre cluster.
   - Pour un groupe de travail Amazon Redshift sans serveur, choisissez Configuration de groupe de travail. Choisissez le groupe de travail dans la liste. Ensuite, sous Accès aux données, dans le panneau Réseau et sécurité, choisissez Modifier.

2. Configurez la passerelle Internet et la table de routage pour votre VPC. Vous démarrez la configuration en choisissant le nom du VPC. Cela ouvre le tableau de bord du VPC. Pour se connecter à un cluster ou à un groupe de travail accessible à tous depuis Internet, une passerelle Internet doit être attachée à la table de routage. Vous pouvez le configurer en choisissant Tables de routage dans le tableau de bord du VPC. Vérifiez que la cible de la passerelle Internet est définie avec la source 0.0.0. 0/0 ou un CIDR IP public. La table de routage doit être associée au VPC où réside votre cluster. Pour plus d'informations sur la configuration de l'accès Internet pour un VPC, comme décrit ici, consultez Activer l'accès Internet dans la documentation relative à Amazon VPC. Pour en savoir plus sur la configuration d'une table de routage, consultez Configuration des tables de routage.
3. Après avoir configuré la passerelle Internet et la table de routage, revenez aux paramètres réseau pour Redshift. Ouvrez l'accès entrant en choisissant le groupe de sécurité, puis Règles entrantes. Choisissez Modifier les règles entrantes.
4. Choisissez le Protocole et le Port pour la ou les règles entrantes, selon vos besoins, afin d'autoriser le trafic depuis des clients. Pour un cluster RG ou RA3, sélectionnez un port compris dans les plages 5431 à 5455 ou 8191 à 8215. Lorsque vous avez terminé, enregistrez chaque règle.
5. Modifiez le paramètre Accessible à tous pour l'activer. Pour ce faire, vous pouvez passer par le menu Actions de votre cluster ou groupe de travail.

Lorsque vous activez le paramètre Accessible publiquement, Redshift crée une adresse IP élastique. Il s'agit d'une adresse IP statique associée à votre AWS compte. Les clients extérieurs au VPC peuvent l'utiliser pour se connecter.

Pour en savoir plus sur la configuration de votre groupe de sécurité, consultez Groupes de sécurité Amazon Redshift.

Vous pouvez tester vos règles en vous connectant à un client. Effectuez les opérations suivantes si vous vous connectez à Amazon Redshift sans serveur. Une fois la configuration réseau terminée, connectez-vous à votre outil client, tel qu'Amazon Redshift RSQL. En utilisant votre domaine Amazon Redshift sans serveur comme hôte, saisissez les informations suivantes :

```
rsql -h workgroup-name.account-id.region.amazonaws.com -U admin -d dev -p 5439
```

Accessibilité privée avec une configuration de groupe de sécurité par défaut ou personnalisée

Lorsque vous ne communiquez pas via Internet avec votre cluster ou votre groupe de travail, on parle d'accès privé. Si vous avez choisi le groupe de sécurité par défaut lors de sa création, celui-ci inclut les règles de communication par défaut suivantes :

- Règle entrante qui autorise le trafic de toutes les ressources attribuées au groupe de sécurité.
- Règle sortante qui autorise tout le trafic sortant. La destination de cette règle est 0.0.0. 0/0. En notation Routage inter-domaines sans classe (CIDR), il représente toutes les adresses IP possibles.

Vous pouvez consulter les règles dans la console en sélectionnant le groupe de sécurité pour votre cluster ou groupe de travail.

Si votre cluster ou groupe de travail et le client utilisent tous deux le groupe de sécurité par défaut, aucune configuration supplémentaire n'est nécessaire pour autoriser le trafic réseau. Mais si vous supprimez ou modifiez des règles du groupe de sécurité par défaut pour Redshift ou le client, cela ne s'applique plus. Dans ce cas, vous devez configurer des règles pour autoriser les communications entrantes et sortantes. Une configuration de groupe de sécurité courante est la suivante :

- Pour une instance Amazon EC2 cliente :
  - Règle entrante qui autorise l'adresse IP du client.

  - Règle sortante qui autorise la plage d'adresses IP (bloc d'adresse CIDR) de tous les sous-réseaux fournis pour l'utilisation de Redshift. Ou vous pouvez spécifier 0.0.0. 0/0, qui correspond à toutes les plages d'adresses IP.
- Pour votre cluster ou groupe de travail Redshift :
  - Règle entrante qui autorise le groupe de sécurité du client.
  - Règle sortante qui autorise le trafic à 0.0.0. 0/0. Généralement, la règle sortante autorise tout le trafic sortant. Vous pouvez éventuellement ajouter une règle sortante pour autoriser le trafic vers le groupe de sécurité du client. Dans ce cas facultatif, une règle sortante n'est pas toujours requise, car le trafic de réponse pour chaque demande est autorisé à atteindre l'instance. Pour plus de détails concernant le comportement des demandes et des réponses, consultez Groupes de sécurité dans le Guide de l'utilisateur Amazon VPC.

Si vous modifiez la configuration de sous-réseaux ou de groupes de sécurité spécifiés pour l'utilisation de Redshift, vous devrez peut-être modifier les règles de trafic en conséquence pour maintenir la communication ouverte. Pour plus d'informations sur la création de règles entrantes et sortantes, consultez Blocs CIDR VPC dans le Guide de l'utilisateur Amazon VPC. Pour plus d'informations sur la connexion à Amazon Redshift depuis un client, consultez Configuration des connexions dans Amazon Redshift.

Sous-réseaux pour les ressources Redshift

Vous créez un groupe de sous-réseaux si vous créez un cluster provisionné dans un cloud privé virtuel (VPC). Chaque VPC peut disposer d'un ou de plusieurs sous-réseaux, qui sont des sous-ensemble d'adresses IP au sein de votre VPC qui vous permettent de regrouper vos ressources en fonction de vos besoins en sécurité et en fonctionnement. Vous créez un groupe de sous-réseaux pour spécifier un ensemble de sous-réseaux dans votre VPC lorsque vous créez un cluster alloué. Dans le Tableau de bord des clusters alloués, vous pouvez rechercher et modifier des groupes de sous-réseaux de clusters sous Configurations. Lors de la configuration initiale d'un cluster alloué, vous spécifiez le groupe de sous-réseaux et Amazon Redshift crée le cluster dans l'un de ses sous-réseaux. Pour de plus amples informations sur le service VPC, consultez la page de détails du produit Amazon VPC.

La configuration du sous-réseau d'un groupe de travail Amazon Redshift sans serveur est similaire à celle d'un cluster alloué, mais les étapes sont légèrement différentes. Lorsque vous créez et configurez un groupe de travail sans serveur, vous spécifiez des sous-réseaux pour le groupe de travail et ils sont ajoutés à une liste. Vous pouvez afficher les sous-réseaux d'un groupe de travail

existant en sélectionnant les propriétés du groupe de travail dans le Tableau de bord sans serveur. Ils sont disponibles dans les propriétés Réseau et sécurité. Pour plus d'informations, consultez Création d'un groupe de travail avec un espace de noms.

Pour plus d'informations sur la création d'un VPC, consultez la documentation du Guide de l'utilisateur Amazon VPC.

Après avoir créé un groupe de sous-réseaux pour un cluster alloué ou choisi des sous-réseaux pour un groupe de travail sans serveur, il est possible de supprimer des sous-réseaux précédemment ajoutés ou d'en ajouter d'autres. Vous pouvez effectuer ces modifications à l'aide de la console ou des opérations d'API. Pour plus d'informations sur les opérations d'API pour un cluster provisionné, consultez ModifyClusterSubnetGroup. Pour les opérations d'API pour un groupe de travail sans serveur, consultez. UpdateWorkgroup

Vous pouvez allouer un cluster sur l'un des sous-réseaux du groupe de sous-réseaux. Un groupe de sous-réseaux de cluster vous permet de spécifier un ensemble de sous-réseaux dans votre VPC.

> **Warning**
>
> Lors des opérations de maintenance du cluster telles que le redimensionnement classique, la pause et la reprise, Multi-AZ les basculements ou d'autres événements, vos nœuds de calcul provisionnés peuvent être déplacés vers un autre sous-réseau au sein de votre groupe de sous-réseaux de clusters Amazon Redshift. Notez que tous les sous-réseaux d'un groupe de sous-réseaux doivent avoir les mêmes règles d'ACL réseau entrantes et sortantes et les mêmes chemins de table de routage. Cela garantit la connectivité vers et depuis les ressources informatiques d'Amazon Redshift, afin qu'elles puissent communiquer et fonctionner de manière optimale après de tels événements de maintenance. Évitez d'ajouter des sous-réseaux avec différentes configurations d'ACL ou de table de routage au même groupe de sous-réseaux du cluster Amazon Redshift.
> Pour plus d'informations sur la configuration des sous-réseaux, consultez Sous-réseaux pour votre VPC dans le Guide de l'utilisateur Amazon VPC. Pour plus d'informations sur les Multi-AZ déploiements de Redshift, consultez Multi-AZ déploiement le guide de gestion de Redshift. Redimensionnement d'un clusterest également traité dans le guide de gestion de Redshift.

Création d'un groupe de sous-réseaux de cluster.

La procédure suivante vous indique comment créer un groupe de sous-réseaux pour un cluster alloué. Vous devez disposer d'au moins un groupe de sous-réseaux défini pour mettre en service un cluster dans un VPC.

Pour créer un groupe de sous-réseaux de cluster pour un cluster alloué

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Configurations, puis choisissez Subnet groups (Groupes de sous-réseaux. La liste des groupes de sous-réseaux s’affiche.
3. Choisissez Create cluster subnet group (Créer un groupe de sous-réseaux de cluster) pour afficher la page de création.
4. Entrez les informations du groupe de sous-réseaux, notamment les sous-réseaux à ajouter.
5. Choisissez Create cluster subnet group (Créer un groupe de sous-réseaux de cluster) pour créer le groupe avec les sous-réseaux que vous avez choisis.

> **Note**
>
> Pour plus d’informations sur la création d’un groupe de travail Amazon Redshift sans serveur avec un ensemble de sous-réseaux, consultez Création d’un groupe de travail avec un espace de noms ou Création d’un sous-réseau dans le Guide de l’utilisateur Amazon VPC.

Modification d'un groupe de sous-réseaux de cluster

Après avoir créé un groupe de sous-réseaux, vous pouvez modifier ses informations sur la console Amazon Redshift. La procédure suivante explique comment modifier un groupe de sous-réseaux pour un cluster alloué.

Pour modifier un groupe de sous-réseaux de cluster pour un cluster alloué

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Configurations, puis choisissez Subnet groups (Groupes de sous-réseaux. La liste des groupes de sous-réseaux s’affiche.

3. Choisissez le groupe de sous-réseaux à modifier.
4. Pour Actions, choisissez Modify (Modifier) pour afficher les détails du groupe de sous-réseaux.
5. Mettez à jour les informations du groupe de sous-réseaux.
6. Choisissez Save (Enregistrer) pour modifier le groupe.

Dans certains cas, la modification ou la suppression de sous-réseaux nécessite des étapes supplémentaires. Par exemple, cet article du Centre de connaissances AWS , intitulé Comment déplacer mon cluster Amazon Redshift provisionné vers un autre sous-réseau ?, décrit un cas d'utilisation qui couvre le déplacement d'un cluster.

Suppression d’un groupe de sous-réseaux de cluster pour un cluster alloué

Lorsque vous avez terminé d’utiliser un groupe de sous-réseaux de cluster, vous devez le nettoyer en supprimant le groupe. La procédure suivante vous indique comment supprimer un groupe de sous-réseaux pour un cluster alloué.

Pour supprimer un groupe de sous-réseaux de cluster

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Configurations, puis choisissez Subnet groups (Groupes de sous-réseaux. La liste des groupes de sous-réseaux s’affiche.
3. Choisissez le groupe de sous-réseaux à supprimer, puis choisissez Delete (Supprimer).

> **Note**
>
> Vous ne pouvez pas supprimer un groupe de sous-réseaux de cluster utilisé par un cluster.

Blocage de l’accès public aux VPC et aux sous-réseaux

VPC Block Public Access (BPA) est une fonctionnalité de sécurité centralisée que vous pouvez utiliser pour empêcher les ressources des VPC et des sous-réseaux que vous possédez d'accéder à Internet ou d'être accessibles Région AWS depuis Internet via des passerelles Internet et des passerelles Internet de sortie uniquement. Si vous activez cette fonctionnalité dans un Compte AWS, elle aura, par défaut, un impact sur tout VPC ou sous-réseau utilisé par Amazon Redshift. Cela signifie qu’Amazon Redshift bloque toutes les opérations au public.

Lorsque le VPC BPA est activé et que vous souhaitez utiliser les API Amazon Redshift sur l'Internet public, vous devez ajouter une exclusion pour l'utilisation des API Amazon EC2 pour votre VPC ou votre sous-réseau. Les exclusions peuvent avoir l'un des modes suivants :

- Bidirectionnel : tout le trafic Internet à destination et en provenance des VPC et des sous-réseaux exclus est autorisé.
- Egress-only: Le trafic Internet sortant provenant des VPC et sous-réseaux exclus est autorisé. Le trafic Internet entrant vers les VPC et les sous-réseaux exclus est bloqué. Cela ne s'applique que lorsque la fonctionnalité BPA est réglée sur bidirectionnel.

Les exclusions BPA d'un VPC désignent un VPC entier ou un sous-réseau spécifique au sein d'un VPC comme étant accessible au public. Les interfaces réseau situées à l'intérieur de cette limite respectent les contrôles réseau VPC habituels, tels que les groupes de sécurité, les tables de routage et les ACL réseau, pour déterminer si cette interface dispose d'un chemin et d'un accès à l'Internet public. Pour plus d'informations sur l'ajout d'exclusions, consultez Créer et supprimer des exclusions dans le Guide de l'utilisateur Amazon VPC.

Clusters alloués

Un groupe de sous-réseaux est une combinaison de sous-réseaux provenant du même VPC. Si un groupe de sous-réseaux pour un cluster alloué se trouve dans un compte sur lequel le VPC BPA est activé, les fonctionnalités suivantes sont bloquées :

- Création d'un cluster public
- Restauration d'un cluster public
- Modification d'un cluster privé pour en faire un cluster public
- Ajout d'un sous-réseau avec VPC BPA activé au groupe de sous-réseaux lorsqu'il existe au moins un cluster public au sein du groupe

Clusters sans serveur

Redshift sans serveur n'utilise pas de groupes de sous-réseaux. Au lieu de cela, chaque cluster possède son propre ensemble de sous-réseaux. Si un groupe de travail possède un compte sur lequel le VPC BPA est activé, les fonctionnalités suivantes sont bloquées :

- Création d'un groupe de travail accessible au public
- Modification d'un groupe de travail privé en groupe de travail public

- Ajout d’un sous-réseau avec VPC BPA activé au groupe de travail lorsque celui-ci est public

Contrôle du trafic réseau avec le routage VPC amélioré Redshift

Lorsque vous utilisez le routage VPC amélioré Amazon Redshift, Amazon Redshift force l'ensemble du trafic COPY et UNLOAD entre votre cluster et vos référentiels de données à traverser votre VPC basé sur le service Amazon VPC. Grâce au routage VPC amélioré, vous pouvez utiliser les fonctionnalités VPC standard, telles que les groupes de sécurité VPC, les listes de contrôle d'accès (ACL) réseau, les points de terminaison d'un VPC, les politiques de point de terminaison d'un VPC, les passerelles Internet et les serveurs de système de noms de domaine (DNS) comme décrit dans le Guide de l'utilisateur Amazon VPC. Ces fonctions vous permettent de contrôle le flux de données entre votre cluster Amazon Redshift et d’autres ressources. Lorsque vous utilisez le routage VPC amélioré pour acheminer le trafic via votre VPC, vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic COPY et UNLOAD.

Les clusters Amazon Redshift et les groupes de travail Amazon Redshift sans serveur prennent en charge le routage VPC amélioré. Vous ne pouvez pas utiliser le routage VPC amélioré avec Redshift Spectrum. Pour plus d’informations, consultez Interrogation de tables de lacs de données avec un routage VPC amélioré.

Si le routage VPC amélioré n'est pas activé, Amazon Redshift achemine le trafic via Internet, y compris le trafic vers d'autres services du réseau. AWS

> **Important**
>
> Comme le routage VPC amélioré affecte la façon dont Amazon Redshift accède à d'autres ressources, les commandes COPY et UNLOAD peuvent échouer, sauf si vous configurez votre VPC correctement. Vous devez créer spécifiquement un chemin d'accès réseau entre le VPC de votre cluster et vos ressources de données, comme décrit ci-après.

Lorsque vous exécutez une commande COPY ou UNLOAD sur un cluster dont le routage VPC amélioré est activé, votre VPC achemine le trafic vers la ressource spécifiée via le chemin d'accès réseau disponible, le plus strict ou le plus spécifique.

Par exemple, vous pouvez configurer les chemins suivants dans votre VPC :

- Points de terminaison VPC : pour le trafic vers un compartiment Amazon S3 situé dans la même AWS région que votre cluster ou groupe de travail, vous pouvez créer un point de terminaison VPC pour diriger le trafic directement vers le compartiment. Lorsque vous utilisez des points de terminaison d'un VPC, vous pouvez attacher une politique de point de terminaison pour gérer l'accès à Amazon S3. Pour plus d'informations sur l'utilisation des points de terminaison avec Amazon Redshift, consultez Contrôle du trafic de base de données avec les points de terminaison d'un VPC. Si vous utilisez Lake Formation, vous trouverez plus d'informations sur l'établissement d'une connexion privée entre votre VPC et AWS Lake Formation au niveau des points de AWS terminaison du VPC d'interface ().AWS PrivateLink

  > **Note**
  >
  > Lorsque vous utilisez des points de terminaison VPC Redshift avec des points de terminaison d'une passerelle VPC Amazon S3, vous devez activer le routage VPC amélioré dans Redshift. Pour plus d'informations, consultez Points de terminaison de passerelle pour Amazon S3.

- Passerelle NAT : vous pouvez vous connecter à un compartiment Amazon S3 dans une autre AWS région et vous pouvez vous connecter à un autre service du AWS réseau. Vous pouvez également accéder à une instance hôte en dehors du AWS réseau. Pour ce faire, configurez une passerelle de traduction d'adresses réseau (NAT), comme décrit dans le guide de l'utilisateur Amazon VPC.
- Passerelle Internet : pour vous connecter aux services AWS en dehors de votre VPC, vous pouvez attacher une Passerelle Internet à votre sous-réseau VPC, comme décrit dans le Guide de l'utilisateur Amazon VPC. Pour utiliser une passerelle Internet, votre cluster ou groupe de travail doit avoir une adresse IP publiquement accessible afin que d'autres services puissent communiquer avec lui.

Pour de plus amples informations, consultez Points de terminaison VPC dans le Guide de l'utilisateur Amazon VPC.

> **Note**
>
> Le routage VPC amélioré affecte également les appels que Redshift passe à AWS IAM Identity Center lorsqu'un utilisateur se connecte. Si votre cluster ou groupe de travail utilise l'authentification AWS IAM Identity Center, vous devez créer des points de terminaison VPC d'interface pour ces services. Dans le cas contraire, la connexion échoue. Pour plus

d'informations sur l'utilisation du routage VPC amélioré avec AWS IAM Identity Center, consultez. Utilisation AWS Authentification IAM Identity Center avec routage VPC amélioré

L'utilisation du routage VPC amélioré n'implique aucun coût supplémentaire. Des frais de transfert de données supplémentaires peuvent être appliqués pour certaines opérations, Il s'agit notamment d'opérations telles que UNLOAD vers Amazon S3 dans une autre AWS région. ou COPY depuis Amazon EMR ou SSH avec des adresses IP publiques. Pour plus d'informations sur la tarification, consultez Tarification d'Amazon EC2.

Rubriques

- Contrôle du trafic de base de données avec les points de terminaison d'un VPC
- Activation du routage VPC amélioré
- Interrogation de tables de lacs de données avec un routage VPC amélioré

Contrôle du trafic de base de données avec les points de terminaison d'un VPC

Vous pouvez utiliser un point de terminaison d'un VPC pour créer une connexion gérée entre votre cluster Amazon Redshift ou groupe de travail sans serveur situé dans un VPC et Amazon Simple Storage Service (Amazon S3). Lorsque vous procédez ainsi, le trafic COPY et UNLOAD entre votre base de données et vos données sur Amazon S3 reste dans votre Amazon VPC. Vous pouvez lier une politique de point de terminaison à votre point de terminaison pour gérer de plus près l'accès à vos données. Par exemple, vous pouvez ajouter une politique à votre point de terminaison d'un VPC qui autorise le déchargement des données uniquement vers un compartiment Amazon S3 spécifique de votre compte.

Pour utiliser les points de terminaison d'un VPC, créez un point de terminaison d'un VPC pour le VPC dans lequel votre entrepôt des données se trouve, puis activez le routage VPC amélioré. Vous pouvez activer le routage VPC amélioré lorsque vous créez votre cluster ou votre groupe de travail, ou vous pouvez modifier un cluster ou un groupe de travail dans un VPC pour utiliser le routage VPC amélioré.

Un point de terminaison d'un VPC utilise des tables de routage pour contrôler le routage du trafic entre un cluster ou un groupe de travail dans le VPC et dans Amazon S3. Tous les clusters et les groupes de travail dans des sous-réseaux associés aux tables de routage spécifiées utilisent automatiquement ce point de terminaison pour accéder au service.

Votre VPC utilise le chemin le plus spécifique ou le plus restrictif, qui correspond à votre trafic pour déterminer comment acheminer le trafic. Supposons, par exemple, que votre table de routage comporte un itinéraire pour l'ensemble du trafic Internet (0.0.0). 0/0) qui pointe vers une passerelle Internet et un point de terminaison Amazon S3. Dans ce cas, l'acheminement du point de terminaison est prioritaire sur tout le trafic destiné au service Amazon S3 Cela est dû au fait que la plage d'adresses IP pour le service Amazon S3 est plus spécifique que 0.0.0. 0/0. Dans cet exemple, tout le trafic Internet restant est acheminé vers votre passerelle Internet, y compris le trafic destiné aux compartiments Amazon S3 dans d'autres Régions AWS.

Pour obtenir plus d'informations sur la création de points de terminaison, consultez la section Create a VPC endpoint (Créer un point de terminaison VPC) dans le Guide de l'utilisateur Amazon VPC.

Vous utilisez les politiques de point de terminaison pour contrôler l'accès depuis votre cluster ou votre groupe de travail aux compartiments Amazon S3 qui contiennent vos fichiers de données. Pour un contrôle plus spécifique, vous pouvez éventuellement lier une politique de point de terminaison personnalisé. Pour plus d'informations, consultez Contrôle de l'accès aux services à l'aide de politiques de point de terminaison dans le Guide AWS PrivateLink .

> **Note**
>
> AWS Database Migration Service (AWS DMS) est un service cloud qui permet de migrer des bases de données relationnelles, des entrepôts de données et d'autres types de magasins de données. Il peut se connecter à n'importe quelle base de données AWS source ou cible, y compris une base de données Amazon Redshift compatible VPC, avec certaines restrictions de configuration. La prise en charge des points de terminaison Amazon VPC facilite le maintien de la sécurité réseau de bout en bout AWS DMS pour les tâches de réplication. Pour plus d'informations sur l'utilisation de Redshift avec AWS DMS, consultez la section Configuration des points de terminaison VPC en tant que points de terminaison AWS DMS source et cible dans le guide de l'utilisateur.AWS Database Migration Service

Il n'y a pas de frais supplémentaires pour l'utilisation de points de terminaison. Des frais standards s'appliquent pour le transfert de données et l'utilisation de ressources. Pour plus d'informations sur la tarification, consultez Tarification d'Amazon EC2.

Activation du routage VPC amélioré

Vous pouvez activer le routage VPC amélioré lorsque vous créez ou modifiez un cluster et lorsque vous créez ou modifiez un groupe de travail Amazon Redshift sans serveur.

Pour utiliser le routage VPC amélioré, votre cluster ou groupe de travail sans serveur doit répondre aux exigences et aux contraintes suivantes :

- Votre cluster doit se trouver dans un VPC.

  Si vous attachez un point de terminaison VPC Amazon S3, le point de terminaison VPC est uniquement utilisé pour accéder aux compartiments Amazon S3 dans la même région. AWS Pour accéder à des buckets dans une autre AWS région (sans utiliser le point de terminaison VPC) ou pour accéder à AWS d'autres services, rendez votre cluster ou votre groupe de travail sans serveur accessible au public ou utilisez une passerelle de traduction d'adresses réseau (NAT). Pour plus d'informations, consultez Création d'un cluster alloué Amazon Redshift ou d'un groupe de travail Amazon Redshift sans serveur dans un VPC.
- Vous devez activer la résolution DNS (Domain Name Service) dans votre VPC. Si vous utilisez votre propre serveur DNS, vous devez également vous assurer que les demandes DNS à Amazon S3 sont résolues correctement en adresses IP gérées par AWS. Pour plus d'informations, consultez Utilisation de DNS avec votre VPC dans le Amazon VPC Guide de l'utilisateur.
- Les noms d'hôte DNS doivent être activés dans votre VPC. Les noms d'hôte DNS sont activés par défaut.
- Vos politiques de point de terminaison d'un VPC doivent autoriser l'accès aux compartiments Amazon S3 utilisés avec les appels COPY, UNLOAD ou CREATE LIBRARY dans Amazon Redshift, y compris l'accès à tous les fichiers manifestes impliqués. Pour la commande COPY depuis des hôtes distants, vos politiques de point de terminaison doivent autoriser l'accès à chaque ordinateur hôte. Pour plus d'informations, consultez la rubrique Autorisations IAM pour les instructions COPY, UNLOAD et CREATE LIBRARY dans le Guide du développeur de base de données Amazon Redshift.

Pour activer le routage VPC amélioré pour un cluster alloué

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Provisioned clusters dashboard (Tableau de bord des clusters provisionnés) puis Create cluster (Créer un cluster) et saisissez les propriétés de Cluster details (Détails du cluster).
3. Pour afficher la section Configurations supplémentaires, choisissez de désactiver Utiliser les valeurs par défaut.
4. Accédez à la section Network and security (Réseau et sécurité).

5. Pour activer Enhanced VPC routing (Routage VPC amélioré), choisissez Turn on (Activer) pour forcer le trafic du cluster à passer par le VPC.
6. Choisissez Créer un cluster pour créer le cluster. Le cluster peut prendre plusieurs minutes pour être prêt à être utilisé.

Pour activer le routage VPC amélioré pour un Amazon Redshift sans serveur

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Serverless dashboard (Tableau de bord sans serveur), puis choisissez Create workgroup (Créer un groupe de travail) et saisissez les propriétés de votre groupe de travail.
3. Accédez à la section Network and security (Réseau et sécurité).
4. Sélectionnez Turn on enhanced VPC routing (Activer le routage VPC amélioré) pour acheminer le trafic réseau via le VPC.
5. Choisissez Next (Suivant) et terminez de saisir les propriétés de votre groupe de travail jusqu'à Create (Créer) le groupe de travail.

Interrogation de tables de lacs de données avec un routage VPC amélioré

Lorsque le routage VPC amélioré est activé, Amazon Redshift achemine le trafic via votre VPC. Les tables Data Lake stockent leurs données dans Amazon S3 et leurs métadonnées dans le AWS Glue Data Catalog, les deux étant situés en dehors de votre VPC. Pour que les requêtes du lac de données aboutissent, votre cluster ou groupe de travail doit être en mesure d'accéder à Amazon S3 et AWS Glue. Si vos tables de lacs de données sont gérées par AWS Lake Formation, celles-ci doivent également pouvoir atteindre Lake Formation. Le routage VPC amélioré affecte la manière dont Amazon Redshift accède à ces ressources externes. Les requêtes peuvent donc échouer si vous ne configurez pas correctement votre VPC.

Créez les points de terminaison VPC suivants dans le VPC et les sous-réseaux sur lesquels votre cluster ou groupe de travail s'exécute, en les associant aux tables de routage appropriées. Ces points de terminaison sont requis à la fois pour le moteur de requête de lac de données intégré et pour Amazon Redshift Spectrum :

- Point de terminaison de la passerelle Amazon S3 : fournit à votre cluster ou à votre groupe de travail un itinéraire via le AWS réseau vers Amazon S3 pour lire les fichiers de données des lacs de

données. Pour connaître les étapes à suivre, consultez la section Points de terminaison Gateway pour Amazon S3 dans le guide de l'utilisateur Amazon VPC.

- AWS Glue point de terminaison de l'interface : donne à votre cluster ou à votre groupe de travail un itinéraire AWS Glue Data Catalog vers le pour résoudre les schémas et les tables de lacs de données. Pour connaître les étapes à suivre, consultez la section Création d'un point de terminaison d'interface dans le guide de l'utilisateur Amazon VPC.
- AWS Point de terminaison de l'interface Lake Formation : obligatoire uniquement si vos tables de lacs de données sont gérées par AWS Lake Formation. Permet à votre cluster ou à votre groupe de travail d'accéder à Lake Formation. Pour connaître les étapes à suivre, consultez la section Création d'un point de terminaison d'interface dans le guide de l'utilisateur Amazon VPC.

La configuration du point de terminaison est la même quelle que soit la manière dont vous interrogez les tables externes, mais la manière dont le trafic est acheminé varie en fonction du moteur de requête. Les sections suivantes décrivent le comportement du moteur de requête de lac de données intégré sur les clusters provisionnés par RG et Amazon Redshift Serverless, et de Redshift Spectrum sur les clusters provisionnés RA3 et DC2.

Moteur de requête de lac de données intégré pour les clusters provisionnés par RG et Amazon Redshift Serverless

Les clusters provisionnés par RG et Amazon Redshift Serverless incluent un moteur de requête de lac de données intégré. Ce moteur fonctionne sur les propres ressources de calcul du cluster ou du groupe de travail, au sein de votre VPC. Lorsque le routage VPC amélioré est activé et que les points de terminaison VPC requis sont en place, l'accès à Amazon S3 AWS Glue provient de votre calcul intégré au VPC et passe par ces points de terminaison VPC. Ce trafic reste dans les limites de votre VPC et sur le AWS réseau. Cet accès est autorisé en fonction du rôle IAM attaché à votre cluster ou groupe de travail. Pour mieux gérer ce trafic, vous pouvez modifier le rôle IAM et la politique attachés au compartiment Amazon S3.

Amazon Redshift Spectrum pour les clusters provisionnés RA3 et DC2

Redshift Spectrum s'exécute sur des ressources AWS gérées détenues par Amazon Redshift mais situées en dehors de votre VPC. Par conséquent, même lorsque le routage VPC amélioré est activé, le trafic que Redshift Spectrum envoie à Amazon S3 ne passe pas par votre VPC, mais le cluster a toujours besoin des points de terminaison Amazon S3 et AWS Glue VPC décrits précédemment pour exécuter des requêtes de lac de données.

Le trafic entre Redshift Spectrum et Amazon S3 est acheminé de manière sécurisée via le réseau AWS privé, en dehors de votre VPC. In-flight le trafic est signé à l'aide du protocole Amazon Signature Version 4 (SigV4) et chiffré à l'aide du protocole HTTPS. Ce trafic est autorisé sur la base du rôle IAM attaché à votre cluster Amazon Redshift. Pour gérer le trafic Redshift Spectrum, vous pouvez modifier le rôle IAM de votre cluster et la politique associée à votre compartiment Amazon S3.

Configuration de la politique d'autorisations pour les requêtes du lac de données

Tenez compte des points suivants lorsque vous interrogez des tables de lacs de données dans Amazon S3 :

- Stratégies d’accès aux compartiments Amazon S3 et rôles IAM
- Autorisations pour endosser le rôle IAM
- Audit et journalisation des accès Amazon S3
- Accès à AWS Glue ou Amazon Athena

Stratégies d’accès aux compartiments Amazon S3 et rôles IAM

Vous pouvez contrôler l’accès aux données de vos compartiments Amazon S3 en utilisant d’une part une stratégie de compartiment associée au compartiment et d’autre part un rôle IAM associé à un cluster alloué.

Redshift Spectrum sur les clusters provisionnés ne peut accéder aux données stockées dans des compartiments Amazon S3 utilisant une politique de compartiment qui restreint l'accès aux seuls points de terminaison d'un VPC spécifiés. Utilisez plutôt une politique de compartiment qui restreint l'accès à certains principaux, tels qu'un AWS compte ou des utilisateurs spécifiques. Le moteur de requête de lac de données intégré aux clusters provisionnés par RG et Amazon Redshift Serverless peut accéder à ces compartiments lorsque le routage VPC amélioré est activé, car son accès Amazon S3 passe par vos points de terminaison VPC.

Pour le rôle IAM qui se voit autoriser l'accès au compartiment, utilisez une relation de confiance autorisant le rôle à être endossé uniquement par le principal du service Amazon Redshift. Lorsqu'il est associé à votre cluster, le rôle ne peut être utilisé que dans le cadre d'Amazon Redshift ; il ne peut pas être partagé en dehors du cluster. Pour plus d’informations, consultez Restriction de l'accès aux rôles IAM. Une politique de contrôle des services (SCP) peut également être utilisée pour restreindre davantage le rôle. Consultez Empêcher les utilisateurs et les rôles IAM d'apporter des modifications spécifiées, à l'exception d'un rôle administrateur spécifié dans le Guide de l'utilisateur AWS Organizations .

> **Note**
>
> Pour utiliser Redshift Spectrum, aucune stratégie IAM ne doit bloquer l'utilisation des URL présignées Amazon S3. Les URL présignées générées par Amazon Redshift Spectrum sont valides pendant 1 heure afin qu'Amazon Redshift dispose de suffisamment de temps pour charger tous les fichiers depuis le compartiment Amazon S3. Une URL présignée unique est générée pour chaque fichier scanné par Redshift Spectrum. Pour les stratégies de compartiment qui incluent une action `s3:signatureAge`, veillez à définir la valeur sur au moins 3 600 000 millisecondes.

L'exemple de politique de compartiment suivant autorise l'accès au compartiment spécifié appartenant au AWS compte`123456789012`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "BucketPolicyForSpectrum",
            "Effect": "Allow",
            "Principal": {
                "AWS": ["arn:aws:iam::123456789012:role/redshift"]
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucketVersions",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

Autorisations pour endosser le rôle IAM

Le rôle associé à votre cluster doit disposer d'une relation de confiance autorisant le rôle à être endossé uniquement par le service Amazon Redshift, comme indiqué ci-après.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Pour plus d'informations, consultez Politiques IAM pour Amazon Redshift Spectrum dans le Guide du développeur de base de données Amazon Redshift.

Audit et journalisation des accès Amazon S3

L'utilisation du routage VPC amélioré Amazon Redshift offre différents avantages, notamment l'enregistrement de l'ensemble du trafic COPY et UNLOAD dans les journaux de flux VPC. Le trafic provenant de Redshift Spectrum vers Amazon S3 ne passe pas par votre VPC ; il n'est donc pas enregistré dans les journaux de flux VPC. Lorsque Redshift Spectrum accède aux données dans Amazon S3, il effectue ces opérations dans le contexte du AWS compte et des privilèges de rôle respectifs. Vous pouvez journaliser et auditer l'accès à Amazon S3 en utilisant la journalisation de l'accès au serveur dans AWS CloudTrail et Amazon S3.

Assurez-vous que les plages d'adresses IP S3 sont ajoutées à votre liste des autorisations. Pour plus d'informations sur les plages d'adresses IP S3 requises, consultez Isolement de réseau.

AWS CloudTrail Journaux

Pour suivre tous les accès aux objets dans Amazon S3, y compris l'accès à Redshift Spectrum, activez la CloudTrail journalisation des objets Amazon S3.

Vous pouvez l'utiliser CloudTrail pour afficher, rechercher, télécharger, archiver, analyser et répondre à l'activité des comptes dans l'ensemble de votre AWS infrastructure. Pour plus d'informations, consultez Getting Started with CloudTrail.

Par défaut, CloudTrail suit uniquement les actions au niveau du bucket. Pour effectuer le suivi des actions au niveau de l'objet (par exemple `GetObject`), activez les événements de données et de gestion pour chaque compartiment enregistré.

Journalisation des accès au serveur Amazon S3

La journalisation des accès au serveur fournit des enregistrements détaillés pour les demandes soumises à un compartiment. Les informations des journaux d'accès peuvent s'avérer utiles en cas d'audit de sécurité ou d'audit des accès. Pour plus d'informations, consultez Comment activer la journalisation des accès au serveur dans le Guide de l'utilisateur Amazon Simple Storage Service.

Pour plus d'informations, consultez le billet AWS de blog sur la sécurité How to Use Bucket Policies and Apply Defense-in-Depth to Help Secure Your Amazon S3 Data.

Accès à AWS Glue ou Amazon Athena

Redshift Spectrum et le moteur de requête intégré au lac de données accèdent à votre catalogue de données dans ou AWS Glue Athena. Une autre option consiste à utiliser un metastore Hive dédié pour votre catalogue de données.

La méthode recommandée pour atteindre le AWS Glue Data Catalog est de créer un point de terminaison VPC d'interface (AWS PrivateLink) pour. AWS Glue Lorsque vous utilisez un point de terminaison d'interface VPC, la communication entre votre VPC et celui-ci AWS Glue est acheminée au sein du réseau. AWS Pour plus d'informations, consultez Création d'un point de terminaison d'interface.

Sinon, pour AWS Glue accéder aux points de terminaison publics d'Athena, configurez votre VPC avec une passerelle Internet ou une passerelle NAT, et configurez vos groupes de sécurité VPC pour autoriser le trafic sortant vers ces points de terminaison publics. Vous pouvez configurer les chemins suivants dans votre VPC :

- Passerelle Internet : pour vous connecter à AWS des services extérieurs à votre VPC, vous pouvez associer une passerelle Internet à votre sous-réseau VPC, comme décrit dans le guide de l'utilisateur Amazon VPC. Pour utiliser une passerelle Internet, un cluster alloué doit avoir une adresse IP publique afin que d'autres services puissent communiquer avec lui.

- Passerelle NAT : pour vous connecter à un compartiment Amazon S3 dans une autre AWS région ou à un autre service du AWS réseau, configurez une passerelle de traduction d'adresses réseau (NAT), comme décrit dans le guide de l'utilisateur Amazon VPC. Utilisez cette même configuration pour accéder à une instance de l'hôte en dehors du réseau AWS .

Événements Amazon Redshift

Amazon Redshift suit les événements du cluster et conserve les informations les concernant pendant plusieurs semaines dans votre AWS compte. Pour chaque événement, Amazon Redshift prend en charge les informations telles que la date à laquelle l'événement s'est produit, une description, la source de l'événement (un cluster, un groupe de paramètres ou un instantané, par exemple) et l'ID source.

Amazon Redshift fournit une notification préalable pour certains événements. Ces événements entrent dans la catégorie d'événement `pending`. Par exemple, nous envoyons une notification préalable si une mise à jour matérielle est requise pour l'un des nœuds de votre cluster. Vous pouvez vous abonner aux événements en attente (pending) de la même manière qu'aux autres événements Amazon Redshift. Pour de plus amples informations, veuillez consulter Abonnements aux notifications d'événements de cluster Amazon Redshift.

Vous pouvez utiliser la console de gestion Amazon Redshift, l'API Amazon Redshift ou les kits de développement logiciel pour obtenir des informations AWS sur les événements. Vous pouvez obtenir la liste de tous les événements ou vous pouvez appliquer des filtres, tels que la durée de l'événement ou ses dates de début et de fin, pour récupérer les informations sur les événements intervenus sur une période spécifique.

Vous pouvez aussi obtenir les événements qui ont été générées par un type de source spécifique, comme les événements de cluster ou de groupe de paramètres. La colonne Source affiche le nom et le type de ressource qui déclenche une action donnée.

Vous pouvez créer des abonnements aux notifications d'événements Amazon Redshift qui spécifient un ensemble de filtres d'événement. Quand se produit un événement qui correspond aux critères de filtre, Amazon Redshift utilise Amazon Simple Notification Service pour vous informer activement que l'événement a eu lieu.

Pour obtenir la liste des événements Amazon Redshift par type de source et par catégorie, consultez the section called "Notifications d'événement d'un cluster alloué"

Abonnements aux notifications d'événements de cluster Amazon Redshift

Amazon Redshift utilise le service Amazon Simple Notification Service (Amazon SNS) pour communiquer les notifications des événements Amazon Redshift. Vous activez les notifications

en créant un abonnement aux événements Amazon Redshift. Vous pouvez être informé quand un événement se produit pour un cluster, un instantané, un groupe de sécurité ou un groupe de paramètres donné. La solution la plus simple pour créer un abonnement consiste à utiliser la console Amazon SNS. Pour en savoir plus sur la création d'une rubrique Amazon SNS et sur l'abonnement, consultez Mise en route avec Amazon SNS.

Dans l'abonnement Amazon Redshift, vous spécifiez un ensemble de filtres pour les événements Amazon Redshift et une rubrique Amazon SNS. Lorsqu'un événement correspondant aux critères de filtrage se produit, Amazon Redshift publie un message de notification sur la rubrique Amazon SNS.

Amazon SNS transmet ensuite le message à tous les consommateurs Amazon SNS qui ont un abonnement Amazon SNS à la rubrique en question. Les messages envoyés aux clients Amazon SNS peuvent prendre n'importe quelle forme prise en charge par Amazon SNS pour AWS une région, comme un e-mail, un SMS ou un appel vers un point de terminaison HTTP. Par exemple, toutes les régions prennent en charge les notifications par e-mail, mais les notifications par SMS ne peuvent être créées que dans la région USA Est (Virginie du Nord).

> **Note**
>
> Actuellement, vous ne pouvez créer un abonnement à un événement qu'à une rubrique standard Amazon SNS (et non à une rubrique FIFO Amazon SNS). Pour plus d'informations, consultez Sources des évènements Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

Lorsque vous créez un abonnement aux notifications d'événement, vous spécifiez un ou plusieurs filtres d'événement. Amazon Redshift envoie des notifications par le biais de l'abonnement chaque fois que se produit un événement qui correspond à tous les critères de filtrage. Les critères de filtre incluent le type de source (par exemple, cluster ou instantané), l'ID de source (par exemple, le nom d'un cluster ou d'un instantané), la catégorie d'événement (par exemple, Monitoring or Security) et la gravité de l'événement (par exemple, INFO ou ERROR).

Si vous créez un abonnement à une notification d’évènement à l’aide de la CLI ou de l’API, vous devez créer une rubrique Amazon Simple Notification Service et vous abonner à cette rubrique avec la console Amazon SNS ou l’API Amazon SNS. Vous devrez également conserver l'Amazon Resource Name (ARN) de la rubrique, car il est utilisé lors de la soumission de commandes de la CLI ou d'actions d'API.

Vous pouvez facilement désactiver les notifications sans supprimer d'abonnement en réglant le bouton radio Enabled sur No dans le Console de gestion AWS ou en définissant le `Enabled` paramètre sur l'`false`utilisation de la CLI ou de l'API Amazon Redshift.

Un abonnement aux événements Amazon Redshift peut spécifier ces critères d'événement :

- Les valeurs pour le type source sont Cluster, Snapshot, Parameter-groups et Security-groups.
- ID source d'une ressource, comme `my-cluster-1` ou `my-snapshot-20130823`. L'ID doit être pour une ressource de la même région AWS que l'abonnement aux événements.
- Catégorie d'événement : les valeurs sont Configuration, Management, Monitoring, Security et Pending.
- Pour la gravité de l'événement, les valeurs sont INFO ou ERROR.

Les critères d'événement peuvent être spécifiés de façon indépendante, sauf que vous devez spécifier un type de source avant de pouvoir spécifier les ID source dans la console. Par exemple, vous pouvez spécifier une catégorie d'événement sans avoir besoin de spécifier un type de source, un ID source ou une gravité. Même si vous pouvez spécifier les ID source des ressources qui ne sont pas du type spécifié dans le type de source, aucune notification ne sera envoyée pour les événements de ces ressources. Par exemple, si vous spécifiez un type de source de cluster et l'ID d'un groupe de sécurité, aucun des événements déclenchés par ce groupe de sécurité ne correspond aux critères de filtre du type de source et, par conséquent, aucune notification ne sera envoyée pour ces événements.

Amazon Redshift envoie une notification pour tout événement qui correspond à tous les critères définis dans un abonnement. Quelques exemples d'ensembles d'événements renvoyés :

- L'abonnement spécifie Cluster comme type de source, my-cluster-1, comme ID source, Monitoring comme catégorie et ERROR comme niveau de gravité. L'abonnement n'enverra les notifications qu'aux événements de la catégorie Monitoring avec une gravité ERROR de my-cluster-1.
- L'abonnement spécifie Cluster comme type de source, Configuration comme catégorie et INFO comme niveau de gravité. L'abonnement n'enverra des notifications qu'aux événements de la catégorie Configuration avec une sévérité INFO de n'importe quel cluster Amazon Redshift du compte AWS .
- L'abonnement spécifie Configuration comme catégorie et INFO comme niveau de gravité. L'abonnement enverra des notifications pour les événements de configuration d'une gravité de type INFO à partir de n'importe quelle ressource Amazon Redshift du AWS compte.

- L'abonnement spécifie ERROR comme niveau de gravité. L'abonnement enverra des notifications pour tous les événements présentant une gravité d'ERREUR depuis n'importe quelle ressource Amazon Redshift du AWS compte.

Si vous supprimez ou renommez un objet dont le nom est référencé comme ID source d'un abonnement existant, l'abonnement demeure actif, mais n'a aucun événement à transmettre à partir de cet objet. Si, plus tard, vous créez un objet portant le même nom que celui référencé dans l'ID d'abonnement source, l'abonnement commence à envoyer les notifications pour les événements du nouvel objet.

Amazon Redshift publie les notifications d'événement sur une rubrique Amazon SNS, identifiée par son nom Amazon Resource Name (ARN). Lorsque vous créez un abonnement aux événements en utilisant la console Amazon Redshift, vous pouvez spécifier une rubrique Amazon SNS existante ou demander que la console crée la rubrique quand elle crée l'abonnement.

Toutes les notifications d'événement Amazon Redshift envoyées à la rubrique Amazon SNS sont à leur tour transmises à tous les consommateurs Amazon SNS abonnés à cette rubrique. Utilisez la console Amazon SNS pour apporter des modifications à la rubrique Amazon Redshift, comme l'ajout d'abonnements de consommateurs à la rubrique ou leur suppression.

Les sections suivantes répertorient l'ensemble des catégories et événements dont vous pouvez être informé. Elle contient aussi des informations sur l'abonnement et sur l'utilisation des abonnements aux événements Amazon Redshift.

Création d'un abonnement aux notifications d'événement

Vous pouvez créer un abonnement aux notifications d'événement Amazon Simple Notification Service (Amazon SNS) pour envoyer des notifications quand un événement se produit pour un cluster, un instantané, un groupe de sécurité ou un groupe de paramètres Amazon Redshift donné. Ces notifications sont envoyées à une rubrique SNS, qui à son tour transmet les messages aux clients SNS abonnés à la rubrique.

Les messages SNS adressés aux consommateurs peuvent prendre n'importe quelle forme de notification prise en charge par Amazon SNS pour AWS une région, comme un e-mail, un SMS ou un appel vers un point de terminaison HTTP. Par exemple, toutes les régions prennent en charge les notifications par e-mail, mais les notifications par SMS ne peuvent être créées que dans la région USA Est (Virginie du Nord). Pour plus d’informations, consultez Notifications d’événement d’un cluster alloué Amazon Redshift.

Pour créer un abonnement au événements

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Événements.
3. Choisissez l'onglet Abonnement aux événements, puis Créer des abonnements aux événements.
4. Entrez les propriétés de votre abonnement aux événements, par exemple le nom, la source, le type, la catégorie et la gravité. Vous pouvez également activer des rubriques Amazon SNS pour être averti des événements.
5. Choisissez Créer un abonnement aux événements pour créer votre abonnement.

Notifications d’événement d’un cluster alloué Amazon Redshift

Cette page décrit les ID d’événement et les catégories de chaque type de source Amazon Redshift.

Catégories et événements pour le type de source cluster

Le tableau suivant affiche la catégorie d’événement et la liste d’événements quand un cluster est le type de source.

Catégorie Amazon Redshift	ID de l’événement	Gravité de l’événement	Description
Configuration	REDSHIFT-EVENT-1000	INFO	Le groupe de paramètres [nom du groupe de paramètres] a été mis à jour à [heure]. Si vous avez modifié uniquement des paramètres dynamiques, les clusters associés sont désormais également modifiés. Si vous avez modifié des paramètres statiques, toutes les mises à jour, y compris les paramètres dynamiques, seront appliquées lorsque vous redémarrerez les clusters associés.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Configuration	REDSHIFT-EVENT-1001	INFO	Votre cluster [nom du cluster] Amazon Redshift a été modifié pour utiliser le groupe de paramètres [nom du groupe de paramètres] à [heure].
Configuration	REDSHIFT-EVENT-1500	ERROR	L'Amazon VPC [nom du VPC] n'existe pas. Vos modifications de configuration du cluster [nom du cluster] n'ont pas été appliquées. Veuillez consulter le Console de gestion AWS pour corriger le problème.
Configuration	REDSHIFT-EVENT-1501	ERROR	Les sous-réseaux client [nom des sous-réseaux] spécifiés pour l'Amazon VPC [nom du VPC] n'existent pas ou ne sont pas valides. Vos modifications de configuration du cluster [nom du cluster] n'ont pas été appliquées. Veuillez consulter le Console de gestion AWS pour corriger le problème.
Configuration	REDSHIFT-EVENT-1502	ERROR	Les sous-réseaux figurant dans le groupe de sous-réseaux de cluster [nom du groupe de sous-réseaux] n'ont aucune adresse IP disponible. Le cluster [nom du cluster] n'a pas pu être créé.
Configuration	REDSHIFT-EVENT-1503	ERROR	L'Amazon VPC [nom du VPC] n'a aucune passerelle Internet qui lui soit associée. Vos modifications de configuration du cluster [nom du cluster] n'ont pas été appliquées. Veuillez consulter le Console de gestion AWS pour corriger le problème.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Configuration	REDSHIFT-EVENT-1504	ERROR	Le module de sécurité matérielle (HSM) du cluster [nom du cluster] est inaccessible.
Configuration	REDSHIFT-EVENT-1505	ERROR	Le module de sécurité matérielle (HSM) du cluster [nom du cluster] ne peut pas être inscrit. Essayez une autre configuration.
Configuration	REDSHIFT-EVENT-1506	ERROR	Amazon Redshift a dépassé la limite de l'interface réseau elastic de votre compte. Supprimez jusqu'à [nombre maximum d'interfaces réseau élastiques] interfaces réseau élastiques ou demandez une augmentation limite du nombre d'interfaces réseau par AWS région avec EC2.
Configuration	REDSHIFT-EVENT-1509	ERROR	Le cluster [nom du cluster] Amazon Redshift ne peut pas être créé, car la limite de points de terminaison de VPC de votre compte a été atteinte. Supprimez les points de terminaison de VPC inutilisés ou demandez une augmentation de la limite des points de terminaison de VPC. Pour de plus amples informations, consultez Points de terminaison VPC dans le Guide de l'utilisateur Amazon VPC.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Configuration	REDSHIFT-EVENT-1510	ERROR	Nous avons détecté que la tentative de chargement des exemples de données sur votre cluster Amazon Redshift [nom du cluster] a échoué. Pour charger des exemples de données, configurez d'abord votre VPC pour qu'il ait accès aux compartiments Amazon S3, puis créez un nouveau cluster et chargez des exemples de données. Pour plus d'informations, consultez Activation du routage VPC amélioré dans le Guide de gestion Amazon Redshift.
Configuration	REDSHIFT-EVENT-1511	ERROR	Le cluster Amazon Redshift [nom du cluster] ne peut pas être créé, car vous avez dépassé la limite d'adresses IP Elastic de votre compte. Supprimez les adresses IP Elastic inutilisées ou demandez une augmentation de limite auprès d'Amazon EC2.
Gestion	REDSHIFT-EVENT-2000	INFO	Votre cluster [nom du cluster] Amazon Redshift a été créé et est prêt à être utilisé.
Gestion	REDSHIFT-EVENT-2001	INFO	Votre cluster [nom du cluster] Amazon Redshift a été supprimé à [heure]. Un instantané final [a / n'a pas] été enregistré.
Gestion	REDSHIFT-EVENT-2002	INFO	Les groupes de sécurité VPC pour le cluster [nom du cluster] ont été mis à jour à [heure UTC].
Gestion	REDSHIFT-EVENT-2003	INFO	La maintenance du cluster [nom du cluster] a démarré à [heure UTC].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Gestion	REDSHIFT-EVENT-2004	INFO	La maintenance du cluster [nom du cluster] a pris fin à [heure UTC].
Gestion	REDSHIFT-EVENT-2006	INFO	Le redimensionnement du cluster [nom du cluster] a démarré à [heure UTC]. Le cluster est en mode lecture seule.
Gestion	REDSHIFT-EVENT-2007	INFO	Une demande de redimensionnement du cluster [nom du cluster] a bien été reçue.
Gestion	REDSHIFT-EVENT-2008	INFO	Votre opération de restauration pour créer un instantané [nom de l'instantané] du cluster [nom du cluster] Amazon Redshift a commencé à [heure]. Pour contrôler la progression de la restauration, consultez la Console de gestion AWS.
Gestion	REDSHIFT-EVENT-2013	INFO	Votre cluster [nom du cluster] Amazon Redshift a été renommé à [heure].
Gestion	REDSHIFT-EVENT-2014	INFO	Une demande de restauration de table pour le cluster [nom du cluster] Amazon Redshift a été reçue.
Gestion	REDSHIFT-EVENT-2015	INFO	La restauration de table a été annulée pour le cluster [nom du cluster] Amazon Redshift à [heure].
Gestion	REDSHIFT-EVENT-2016	INFO	Le remplacement de votre cluster [nom du cluster] Amazon Redshift a commencé à [heure].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Gestion	REDSHIFT-EVENT-2017	INFO	La maintenance lancée par le client a démarré sur votre cluster Amazon Redshift [nom du cluster] à [heure]. Le cluster peut ne pas être disponible lors de la maintenance.
Gestion	REDSHIFT-EVENT-2018	INFO	La maintenance lancée par le client s'est terminée sur votre cluster Amazon Redshift [nom du cluster] à [heure].
Gestion	REDSHIFT-EVENT-2019	ERROR	La maintenance lancée par le client a échoué sur votre cluster Amazon Redshift [nom du cluster] à [heure]. Le cluster va revenir à son état initial.
Gestion	REDSHIFT-EVENT-2020	INFO	Le suivi de votre cluster Amazon Redshift [nom du cluster] a été modifié de [suivi de début] à [suivi de fin].
Gestion	REDSHIFT-EVENT-2021	ERROR	L'opération [opération] du cluster Amazon Redshift [nom du cluster] a échoué lors de l'acquisition de capacité à partir de notre groupe de capacité. Nous nous efforçons d'acquérir de la capacité mais pour l'instant nous avons annulé votre demande. Supprimez ce cluster et réessayez ultérieurement.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Gestion	REDSHIFT-EVENT-2022	ERROR	L'opération [opération] du cluster Amazon Redshift [nom du cluster] a échoué lors de l'acquisition de capacité à partir de notre groupe de capacité. Nous nous efforçons d'acquérir de la capacité mais pour l'instant nous avons annulé votre demande. La capacité est disponible dans [autres zones de disponibilité]. Supprimez ce cluster et réessayez dans une autre zone de disponibilité.
Gestion	REDSHIFT-EVENT-2023	ERROR	Nous avons détecté une panne matérielle sur votre cluster à un seul nœud Amazon Redshift [nom du cluster], qui peut avoir provoqué l'échec de requêtes ou une disponibilité intermittente du cluster. Le remplacement du cluster a échoué lors de l'acquisition de capacité à partir de notre groupe de capacité. Vous devrez restaurer un nouveau cluster à partir d'un instantané. Supprimez ce cluster, sélectionnez le dernier instantané disponible et restaurez un nouveau cluster à partir de cet instantané. Cette action met automatiquement à votre disposition du matériel sain.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Gestion	REDSHIFT-EVENT-2024	ERROR	Nous avons détecté une panne matérielle sur votre cluster à un seul nœud Amazon Redshift [nom du cluster], qui peut avoir provoqué l'échec de requêtes ou une disponibilité intermittente du cluster. Le remplacement du cluster a échoué lors de l'acquisition de capacité à partir de notre groupe de capacité. La capacité est disponible dans la zone de disponibilité : [autres zones de disponibilité]. Supprimez ce cluster, sélectionnez le dernier instantané disponible et restaurez un nouveau cluster à partir de cet instantané. Cette action met automatiquement à votre disposition du matériel sain.
Gestion	REDSHIFT-EVENT-3011	INFO	Un redimensionnement élastique du cluster « [nom du cluster] » Amazon Redshift a démarré à [heure]. Nous maintiendrons les connexions de la base de données pendant le redimensionnement. Certaines requêtes et connexions peuvent être arrêtées ou expirer pendant cette opération.
Gestion	REDSHIFT-EVENT-3012	INFO	Nous avons reçu une demande de redimensionnement élastique pour le cluster '[nom du cluster]' démarré à [heure]. Nous fournirons une notification d'événement lorsque le redimensionnement commencera.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
En attente	REDSHIFT-EVENT-2025	INFO	Votre base de données pour le cluster [nom du cluster] sera mise à jour entre [heure de début] et [heure de fin]. Votre cluster ne sera pas accessible. Planifiez en conséquence.
En attente	REDSHIFT-EVENT-2026	INFO	Votre cluster [nom du cluster] sera mis à jour entre [heure de début] et [heure de fin]. Votre cluster ne sera pas accessible. Planifiez en conséquence.
Contrôle	REDSHIFT-EVENT-2050	INFO	Un problème de matériel a été détecté sur le cluster Amazon Redshift [nom du cluster]. Une demande de remplacement a été lancée à [heure].
Contrôle	REDSHIFT-EVENT-3000	INFO	Votre cluster [nom du cluster] Amazon Redshift a été redémarré à [heure].
Contrôle	REDSHIFT-EVENT-3001	INFO	Un nœud de votre cluster [nom du cluster] Amazon Redshift a été automatiquement remplacé à [heure] et votre cluster fonctionne normalement.
Contrôle	REDSHIFT-EVENT-3002	INFO	Le redimensionnement de votre cluster [nom du cluster] Amazon Redshift est complet et votre cluster est disponible pour les lectures et les écritures. Le redimensionnement a commencé à [heure] et a nécessité [nombre d'heures] heures.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Contrôle	REDSHIFT-EVENT-3003	INFO	Le cluster [nom du cluster] Amazon Redshift a été créé avec succès à partir de l'instantané [nom de l'instantané] et est disponible pour être utilisé.
Contrôle	REDSHIFT-EVENT-3007	INFO	Votre instantané Amazon Redshift [nom de l'instantané] a été copié avec succès de [AWS région source] vers [AWS région de destination] à [heure].
Contrôle	REDSHIFT-EVENT-3008	INFO	La restauration de table a démarré pour le cluster [nom du cluster] Amazon Redshift à [heure].
Contrôle	REDSHIFT-EVENT-3009	INFO	La restauration de table s'est terminée avec succès pour le cluster [nom du cluster] Amazon Redshift à [heure].
Contrôle	REDSHIFT-EVENT-3010	ERROR	La restauration de table a échoué pour le cluster [nom du cluster] Amazon Redshift à [heure].
Contrôle	REDSHIFT-EVENT-3013	ERROR	L'opération de redimensionnement élastique demandée pour le cluster [nom du cluster] Amazon Redshift a échoué à [heure] à cause d'un(e) [motif].
Contrôle	REDSHIFT-EVENT-3014	INFO	Le cluster [nom du cluster] Amazon Redshift a été redémarré à [heure].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
En attente	REDSHIFT-EVENT-3015	INFO	Nous avons planifié un redémarrage de votre cluster [nom du cluster] pour maintenance entre [heure de début UTC] et [heure de fin UTC]. Votre cluster ne sera pas accessible pendant cette période. Nous vous recommandons de planifier la panne afin d'éviter tout contretemps.
Contrôle	REDSHIFT-EVENT-3016	INFO	Le cluster sera redémarré.
Contrôle	REDSHIFT-EVENT-3500	ERROR	Le redimensionnement de votre cluster [nom du cluster] Amazon Redshift a échoué. Le redimensionnement va être réessayé automatiquement dans quelques minutes.
Contrôle	REDSHIFT-EVENT-3501	ERROR	Votre opération de restauration pour créer le cluster [nom du cluster] Amazon Redshift à partir de l'instantané [nom de l'instantané] a échoué à [heure]. Réessayez l'opération.
Contrôle	REDSHIFT-EVENT-3504	ERROR	Le compartiment [nom du compartiment] Amazon S3 n'est pas valide pour la journalisation du cluster [nom du cluster].
Contrôle	REDSHIFT-EVENT-3505	ERROR	Le compartiment [nom du compartiment] Amazon S3 n'a pas les politiques IAM appropriées pour le cluster [nom du cluster].
Contrôle	REDSHIFT-EVENT-3506	ERROR	Le compartiment [nom du compartiment] Amazon S3 n'existe pas. La journalisation ne peut pas continuer pour le cluster [nom du cluster].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Contrôle	REDSHIFT-EVENT-3507	ERROR	Le cluster [nom du cluster] Amazon Redshift ne peut pas être créé à l'aide de l'EIP [adresse IP]. Cette adresse est déjà en cours d'utilisation.
Contrôle	REDSHIFT-EVENT-3508	ERROR	Le cluster [nom du cluster] Amazon Redshift ne peut pas être créé à l'aide de l'EIP [adresse IP]. Impossible de trouver l'adresse IP Elastic.
Contrôle	REDSHIFT-EVENT-3509	ERROR	Cross-region la copie instantanée n'est pas activée pour le cluster [nom du cluster].
Contrôle	REDSHIFT-EVENT-3510	ERROR	Le démarrage de la restauration de table a échoué pour le cluster [nom du cluster] Amazon Redshift à [heure]. Motif : [motif].
Contrôle	REDSHIFT-EVENT-3511	ERROR	La restauration de table a échoué pour le cluster [nom du cluster] Amazon Redshift à [heure].
Contrôle	REDSHIFT-EVENT-3512	ERROR	Un cluster [nom du cluster] Amazon Redshift a échoué en raison d'un problème matériel. Le cluster est automatiquement restauré depuis le dernier instantané [nom de l'instantané] créé à [heure].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Contrôle	REDSHIFT-EVENT-3513	ERROR	Un cluster [nom du cluster] Amazon Redshift a échoué en raison d'un problème matériel. Le cluster est automatiquement restauré depuis le dernier instantané [nom de l'instantané] créé à [heure]. Toutes les modifications apportées à la base de données par la suite devront être soumises à nouveau.
Contrôle	REDSHIFT-EVENT-3514	ERROR	Un cluster [nom du cluster] Amazon Redshift a échoué en raison d'un problème matériel. Le cluster est placé en état de défaillance matérielle. Supprimez le cluster et restaurez-le à partir du dernier instantané [nom de l'instantané] créé à [heure].
Contrôle	REDSHIFT-EVENT-3515	ERROR	Un cluster [nom du cluster] Amazon Redshift a échoué en raison d'un problème matériel. Le cluster est placé en état de défaillance matérielle. Supprimez le cluster et restaurez-le à partir du dernier instantané [nom de l'instantané] créé à [heure]. Toutes les modifications apportées à la base de données par la suite devront être soumises à nouveau.
Contrôle	REDSHIFT-EVENT-3516	ERROR	Le cluster [nom du cluster] Amazon Redshift a échoué en raison d'un problème matériel et il n'existe aucune sauvegarde du cluster. Le cluster est placé en état de défaillance matérielle et peut être supprimé.
Contrôle	REDSHIFT-EVENT-3519	INFO	Le redémarrage du cluster [nom du cluster] a commencé à [heure].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Contrôle	REDSHIFT-EVENT-3520	INFO	Le redémarrage du cluster [nom du cluster] s'est terminé [heure].
Contrôle	REDSHIFT-EVENT-3521	INFO	Nous avons détecté un problème de connectivité sur le cluster '[cluster name]'. Un contrôle de diagnostic automatisé a été initié à [time].
Contrôle	REDSHIFT-EVENT-3522	INFO	Action de récupération sur l'échec du cluster '[cluster name]' à [time]. L'équipe Amazon Redshift travaille sur une solution.
Contrôle	REDSHIFT-EVENT-3533	ERROR	Le redimensionnement de cluster sur « [nom du cluster] » a été annulé à [heure]. L'opération a été annulée en raison de [raison]. [action nécessaire].
Contrôle	REDSHIFT-EVENT-3534	INFO	Le redimensionnement élastique du cluster « [nom du cluster] » Amazon Redshift s'est terminé à [heure]. Le cluster est désormais disponible pour des opérations de lecture et d'écriture pendant que nous transférons les données. Certaines requêtes peuvent prendre plus de temps tant que le transfert de données n'est pas terminé.
Contrôle	REDSHIFT-EVENT-3537	INFO	Le transfert de données du cluster « [nom du cluster] » s'est terminé à [heure en UTC].
Contrôle	REDSHIFT-EVENT-3600	INFO	L'opération de redimensionnement demandée pour le cluster Amazon Redshift « [nom du cluster] » a été annulée dans le passé. La restauration s'est terminée à [heure].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
En attente	REDSHIFT-EVENT-3601	INFO	Un nœud sur votre cluster [nom du cluster] sera remplacé entre [heure de début] et [heure de fin]. Vous ne pouvez pas reporter cette maintenance. Planifiez en conséquence.
En attente	REDSHIFT-EVENT-3602	INFO	Le remplacement d'un nœud sur votre cluster [nom du cluster] est planifié entre [heure de début] et [heure de fin]. Votre cluster ne sera pas accessible. Planifiez en conséquence.
Gestion	REDSHIFT-EVENT-3603	INFO	L'opération de restauration pour créer le cluster [nom du cluster] à partir de l'instant ané [nom de l'instantané] a échoué en raison d'une erreur interne. Le cluster est placé en état de restauration incompatible et peut être supprimé. Essayez de restaurer l'instant ané dans un cluster avec une configuration différente.
Gestion	REDSHIFT-EVENT-3614	INFO	L'action planifiée [nom de l'action planifiée] a été créée à [heure en UTC]. Le premier appel est programmé à [heure en UTC].
Gestion	REDSHIFT-EVENT-3615	INFO	L'action planifiée [nom de l'action planifiée] est programmée à [heure en UTC].
Contrôle	REDSHIFT-EVENT-3616	INFO	L'action planifiée [nom de l'action planifiée] à [heure en UTC] s'est terminée avec le statut « SUCCEEDED ».
Contrôle	REDSHIFT-EVENT-3617	ERROR	L'action planifiée [nom de l'action planifiée] a été ignorée à [heure en UTC] en raison d'un délai.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Contrôle	REDSHIFT-EVENT-3618	INFO	L'opération de pause du cluster [nom du cluster] a démarré à [heure en UTC]. Mise en pause démarrée
Contrôle	REDSHIFT-EVENT-3619	INFO	Le cluster Amazon Redshift [nom du cluster] a été suspendu avec succès à [heure UTC].
Gestion	REDSHIFT-EVENT-3626	INFO	L'action planifiée [nom de l'action planifiée] a été modifiée à [heure en UTC]. Le premier appel est programmé à [heure en UTC].
Gestion	REDSHIFT-EVENT-3627	INFO	L'action planifiée [nom de l'action planifiée] a été supprimée à [heure en UTC].
Contrôle	REDSHIFT-EVENT-3628	ERROR	L'action planifiée [nom de l'action planifiée] à [heure en UTC] s'est terminée avec l'état « FAILED ».
Contrôle	REDSHIFT-EVENT-3629	INFO	Une demande de basculement interne du cluster [nom du cluster] a été initiée.
Contrôle	REDSHIFT-EVENT-3630	INFO	Amazon Redshift a réussi à relocaliser votre cluster [nom du cluster] Amazon Redshift depuis [zone de disponibilité] vers [zone de disponibilité] pour la récupération.
Gestion	REDSHIFT-EVENT-3631	INFO	Le cluster [nom du cluster] Amazon Redshift a reçu votre demande de relocalisation. Une fois le déplacement de zone de disponibilité terminé, Amazon Redshift envoie une notification d'événement.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Contrôle	REDSHIFT-EVENT-3632	INFO	Le cluster [nom du cluster] Amazon Redshift a été relocalisé avec succès de [zone de disponibilité] vers [zone de disponibilité]. Vous pouvez utiliser le cluster maintenant.
Contrôle	REDSHIFT-EVENT-3658	ERROR	EC2-Classic vers un échec de la EC2-VPC migration pour le cluster Redshift [identifiant du cluster].
Contrôle	REDSHIFT-EVENT-3659	INFO	EC2-Classic pour que EC2-VPC la migration soit réussie pour le cluster Redshift [identifiant du cluster].
Contrôle	REDSHIFT-EVENT-3660	INFO	Le cluster est placé en état de défaillance matérielle. Supprimez le EC2-Classic cluster et restaurez-le dans un EC2-VPC cluster à partir du dernier instantané [nom de l'instantané] créé à [heure en UTC].
Gestion	REDSHIFT-EVENT-3666	INFO	Le Multi-AZ cluster Amazon Redshift [nom du cluster] a détecté une défaillance à [heure en UTC] et a déclenché une restauration automatique.
Gestion	REDSHIFT-EVENT-3667	INFO	Le Multi-AZ cluster Amazon Redshift [nom du cluster] a été correctement restauré à [heure en UTC] et peut être utilisé dans [première zone de disponibilité]. Le calcul secondaire dans une autre zone de disponibilité sera bientôt disponible.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Contrôle	REDSHIFT-EVENT-3668	ERROR	Le Multi-AZ cluster Amazon Redshift [nom du cluster] n'a pas pu être restauré à [heure en UTC].
Gestion	REDSHIFT-EVENT-3669	INFO	Le Multi-AZ cluster Amazon Redshift [nom du cluster] a été correctement restauré à [heure en UTC] et peut être utilisé avec les ressources de calcul de [première zone de disponibilité] et de [deuxième zone de disponibilité].
Gestion	REDSHIFT-EVENT-3670	INFO	La maintenance du cluster Amazon Redshift [nom du cluster] a pris fin à [heure UTC] et il est disponible pour être utilisé avec des ressources de calcul dans [première zone de disponibilité]. Le calcul secondaire dans une autre zone de disponibilité sera bientôt disponible.
Gestion	REDSHIFT-EVENT-3671	INFO	Le redimensionnement du cluster Amazon Redshift [nom du cluster] a pris fin à [heure UTC] et il est disponible pour être utilisé dans [première zone de disponibilité]. Le calcul secondaire dans une autre zone de disponibilité sera bientôt disponible.
Gestion	REDSHIFT-EVENT-3672	INFO	Le Multi-AZ cluster Amazon Redshift [nom du cluster] a détecté une défaillance dans [deuxième zone de disponibilité] à [heure en UTC] et a déclenché une restauration automatique.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Gestion	REDSHIFT-EVENT-3673	INFO	L'opération Multi-AZ d'activation du cluster Amazon Redshift [nom du cluster] a débuté à [heure en UTC].
Gestion	REDSHIFT-EVENT-3674	INFO	L'opération d'activation Multi-AZ du cluster Amazon Redshift [nom du cluster] s'est terminée avec succès à [heure en UTC].
Contrôle	REDSHIFT-EVENT-3675	ERROR	L'opération Multi-AZ d'activation du cluster Amazon Redshift [nom du cluster] a échoué à [heure en UTC].
Gestion	REDSHIFT-EVENT-3676	INFO	L'opération de désactivation Multi-AZ pour votre Multi-AZ cluster Amazon Redshift [nom du cluster] a débuté à [heure en UTC].
Gestion	REDSHIFT-EVENT-3677	INFO	L'opération de désactivation Multi-AZ pour votre cluster Amazon Redshift [nom du cluster] s'est terminée avec succès à [heure en UTC].
Contrôle	REDSHIFT-EVENT-3678	ERROR	L'opération de désactivation Multi-AZ pour votre cluster Amazon Redshift [nom du cluster] a échoué à [heure en UTC].
Configuration	REDSHIFT-EVENT-3679	INFO	Le port du cluster Amazon Redshift [nom du cluster] a été modifié avec succès.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Configuration	REDSHIFT-EVENT-3680	ERROR	Amazon Redshift n'a pas pu créer le cluster [nom du cluster], car le rôle lié à un service (SLR) nécessaire à cette opération est inaccessible. Réessayez de le créer à partir de la console Amazon Redshift. Amazon Redshift créera le rôle SLR automatiquement.
Contrôle	REDSHIFT-EVENT-3684	ERROR	Votre compartiment Amazon S3 [nom du compartiment] a été chiffré avec une AWS KMS clé inconnue ou inaccessible. Modifiez le chiffrement de votre compartiment Amazon S3.
Gestion	REDSHIFT-EVENT-3685	ERROR	L'opération de restauration sur le cluster [nom du cluster] a échoué car l'espace disque disponible est insuffisant. L'opération est en cours de restauration. Essayez de restaurer vers un cluster avec une configuration différente.
Gestion	REDSHIFT-EVENT-3686	ERROR	L'opération de redimensionnement du cluster [nom du cluster] a échoué car l'espace disque disponible est insuffisant. L'opération est en cours de restauration. Essayez de redimensionner vers un cluster avec une configuration différente.
Gestion	REDSHIFT-EVENT-3687	INFO	Le redimensionnement demandé du cluster Amazon Redshift [nom du cluster] s'est terminé à [heure UTC].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Sécurité	REDSHIFT-EVENT-3688	ERROR	La rotation des clés de chiffrement de votre cluster Amazon Redshift [nom du cluster] n'a pas pu être effectuée.
DataSharing	REDSHIFT-EVENT-3689	INFO	L'opération d'enregistrement de votre espace de noms Amazon Redshift <nom du cluster> vers le compte Glue Data Catalog <id de compte> a été lancée à <heure UTC>
DataSharing	REDSHIFT-EVENT-3690	INFO	L'opération d'enregistrement de votre espace de noms Amazon Redshift <nom du cluster> vers le compte Glue Data Catalog <id de compte> s'est terminée avec succès à <heure UTC>
DataSharing	REDSHIFT-EVENT-3691	INFO	L'opération d'enregistrement de votre espace de noms Amazon Redshift <nom du cluster> vers le compte Glue Data Catalog <id de compte> a échoué à <heure UTC>
DataSharing	REDSHIFT-EVENT-3692	INFO	L'opération d'annulation de l'enregistrement de votre espace de noms Amazon Redshift <nom du cluster> à partir du compte Glue Data Catalog <id de compte> a été lancée à <heure UTC>
DataSharing	REDSHIFT-EVENT-3693	INFO	L'opération d'annulation de l'enregistrement de votre espace de noms Amazon Redshift <nom du cluster> à partir du compte Glue Data Catalog <id de compte> s'est terminée avec succès à <heure UTC>

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
DataSharing	REDSHIFT-EVENT-3694	INFO	L'opération d'annulation de l'enregistrement de votre espace de noms Amazon Redshift <nom du cluster> à partir du compte Glue Data Catalog <id de compte> a échoué à <heure UTC>
Sécurité	REDSHIFT-EVENT-4000	INFO	Vos informations d'identification d'administrateur pour votre cluster [nom du cluster] Amazon Redshift ont été mises à jour à [heure].
Sécurité	REDSHIFT-EVENT-4001	INFO	Le groupe de sécurité [nom du groupe de sécurité] a été modifié à [heure]. Les modifications se dérouleront automatiquement pour tous les clusters associés.
Sécurité	REDSHIFT-EVENT-4005	ERROR	Le cluster [nom du cluster] possède AWS KMS key des autorisations non valides. Votre cluster entrera dans l'état « INACCESSIBLE_KMS_KEY » et vous ne pourrez plus y accéder.
Sécurité	REDSHIFT-EVENT-4006	INFO	Le cluster [nom du cluster] a maintenant été restauré dans son état précédent car AWS KMS key les autorisations ont été restaurées.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Sécurité	REDSHIFT-EVENT-4500	ERROR	Un ou plusieurs groupes de sécurité que vous avez fournis pour le cluster Amazon Redshift [nom du cluster] sont introuvables. S'il existait des groupes de sécurité valides, ils ont été appliqués au cluster. Aucun groupe de sécurité non valide n'a été appliqué. Si vous modifiiez un cluster existant et qu'aucun groupe de sécurité n'était valide, le cluster a conservé ses groupes de sécurité d'origine. Si vous créiez un nouveau cluster et qu'aucun groupe de sécurité n'était valide, la création du cluster a échoué. Dans les deux cas, veuillez réessayer la requête avec des groupes de sécurité valides. Pour plus d'informations sur la gestion des groupes de sécurité dans Amazon Redshift, consultez Groupes de sécurité VPC dans le Guide de gestion Amazon Redshift.
Sécurité	REDSHIFT-EVENT-4501	ERROR	Le groupe de sécurité [nom du groupe de sécurité] spécifié dans Cluster Security Group [nom du groupe de sécurité du cluster] est introuvable. L'autorisation ne peut pas être finalisée.
Sécurité	REDSHIFT-EVENT-4502	ERROR	Les informations d'identification d'administrateur du cluster [nom du cluster] Amazon Redshift n'ont pas pu être mises à jour à [heure] à cause d'une activité simultanée. Laissez la charge de travail actuelle se terminer ou réduisez la charge de travail active, puis réessayez l'opération.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Sécurité	REDSHIFT-EVENT-4503	ERROR	Amazon Redshift ne peut pas accéder au secret de votre cluster [nom du cluster].
Sécurité	REDSHIFT-EVENT-4504	ERROR	Amazon Redshift ne peut pas accéder à la clé KMS [clé KMS] qui a été utilisée pour chiffrer le secret des informations d'identification d'administrateur de votre cluster [nom du cluster].
Sécurité	REDSHIFT-EVENT-4505	ERROR	Amazon Redshift ne peut pas effectuer la rotation du secret de votre cluster [nom du cluster], car une opération est en cours sur le cluster.
Sécurité	REDSHIFT-EVENT-4506	ERROR	Votre cluster Amazon Redshift [nom du cluster] est mis en pause. Amazon Redshift ne peut pas effectuer la rotation des secrets des clusters mis en pause.

Catégories et événements pour le type de source groupe de paramètres

Le tableau suivant affiche la catégorie d'événement et la liste d'événements quand un groupe de paramètres est le type source.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Configuration	REDSHIFT-EVENT-1002	INFO	Le paramètre [nom du paramètre] a été mis à jour de [valeur] à [valeur], à [heure].

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Configuration	REDSHIFT-EVENT-1003	INFO	Le groupe de paramètres de cluster [nom du groupe] a été créé.
Configuration	REDSHIFT-EVENT-1004	INFO	Le groupe de paramètres de cluster [nom du groupe] a été supprimé.
Configuration	REDSHIFT-EVENT-1005	INFO	Le groupe de paramètres de cluster [nom] a été mis à jour à [heure]. Si vous avez modifié uniquement des paramètres dynamiques, les clusters associés sont désormais également modifiés. Si vous avez modifié des paramètres statiques , toutes les mises à jour, y compris les paramètres dynamiques, seront appliquée s lorsque vous redémarrerez les clusters associés.

Catégories et événements pour le type de source groupe de sécurité

Le tableau suivant affiche la catégorie d'événement et la liste d'événements quand un groupe de sécurité est le type source.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Sécurité	REDSHIFT-EVENT-4002	INFO	Le groupe de sécurité du cluster [nom du groupe] a été créé.
Sécurité	REDSHIFT-EVENT-4003	INFO	Le groupe de sécurité du cluster [nom du groupe] a été supprimé.
Sécurité	REDSHIFT-EVENT-4004	INFO	Le groupe de sécurité du cluster [nom du groupe] a été modifié à [heure]. Les

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
			modifications seront appliquées automatiquement à tous les clusters associés.

Catégories et événements pour le type de source instantané

Le tableau suivant affiche la catégorie d'événement et la liste d'événements quand un snapshot est le type source.

Catégorie Amazon Redshift	ID de l'événement	Gravité de l'événement	Description
Gestion	REDSHIFT-EVENT-2009	INFO	Un instantané utilisateur [nom de l'instantané] du cluster [nom du cluster] Amazon Redshift a démarré à [heure]. Pour contrôler la progression de l'instantané, consultez Console de gestion AWS.
Gestion	REDSHIFT-EVENT-2010	INFO	L'instantané utilisateur [nom de l'instantané] de votre cluster [nom du cluster] Amazon Redshift a été annulé à [heure].
Gestion	REDSHIFT-EVENT-2011	INFO	L'instantané utilisateur [nom de l'instantané] du cluster [nom du cluster] Amazon Redshift a été supprimé à [heure].
Gestion	REDSHIFT-EVENT-2012	INFO	L'instantané final [nom de l'instantané] du cluster [nom du cluster] Amazon Redshift a démarré à [heure].
Contrôle	REDSHIFT-EVENT-3004	INFO	L'instantané utilisateur [nom de l'instantané] de votre cluster [nom du cluster] Amazon Redshift s'est terminé avec succès à [heure].

Catégorie Amazon Redshift	ID de l’événement	Gravité de l’événement	Description
Contrôle	REDSHIFT-EVENT-3005	INFO	L’instantané final [nom] de votre cluster [nom] Amazon Redshift s’est terminé avec succès à [heure].
Contrôle	REDSHIFT-EVENT-3006	INFO	L’instantané final [nom de l’instantané] du cluster [nom du cluster] Amazon Redshift a été annulé à [heure].
Contrôle	REDSHIFT-EVENT-3502	ERROR	L’instantané final [nom de l’instantané] du cluster [nom du cluster] Amazon Redshift a échoué à [heure]. L’équipe étudie le problème. Accédez à Console de gestion AWS et réessayez l’opération.
Contrôle	REDSHIFT-EVENT-3503	ERROR	L’instantané utilisateur [nom de l’instant ané] de votre cluster [nom du cluster] Amazon Redshift a échoué à [heure]. L’équipe étudie le problème. Rendez-vous sur le site Console de gestion AWS pour réessayer l'opération.

Notifications d'événements Amazon Redshift sans serveur avec Amazon EventBridge

Amazon Redshift Serverless utilise Amazon EventBridge pour gérer les notifications d'événements afin de vous tenir au courant des modifications apportées à votre entrepôt de données. Amazon EventBridge est un service de bus d'événements sans serveur que vous pouvez utiliser pour connecter vos applications à des données provenant de diverses sources. Dans ce cas, la source de l’événement est Amazon Redshift. Les événements, qui sont des modifications surveillées dans un environnement, sont automatiquement envoyés EventBridge depuis votre entrepôt de données Amazon Redshift. Les événements sont diffusés en temps quasi réel.

Les fonctionnalités EventBridge incluent la fourniture d'un environnement vous permettant de rédiger des règles d'événements, qui peuvent spécifier les actions à entreprendre pour des événements spécifiques. Vous pouvez également définir des cibles, c'est-à-dire des ressources auxquelles un événement EventBridge peut être envoyé. Une cible peut inclure une destination d'API, un groupe de CloudWatch journaux Amazon, etc. Pour plus d'informations sur les règles, consultez les EventBridge règles d'Amazon. Pour plus d'informations sur les cibles, consultez la section Amazon EventBridge Targets.

Les événements peuvent être classés par gravité et par catégorie. Les filtres suivants sont disponibles :

- Resource filtering (Filtrage par ressources) : recevez des messages en fonction de la ressource à laquelle les événements sont associés. Les ressources incluent un groupe de travail, un instantané, etc.
- Time window filtering (Filtrage par plages horaires) : délimitez les événements sur une période spécifique.
- Category filtering (Filtrage par catégorie) : recevez des notifications d'événements pour tous les événements des catégories spécifiées.

Le tableau suivant comprend les événements Amazon Redshift sans serveur, avec des métadonnées supplémentaires :

Catégorie Amazon Redshift	ID d'événement externe	Gravité de l'événement	Description du message
RateChange	REDSHIFT-SERVERLESS-EVENT-1001	INFO	Le changement de RPU de base du groupe de travail a réussi à <time in UTC>.
RateChange	REDSHIFT-SERVERLESS-EVENT-1002	ERROR	Le changement de RPU de base du groupe de travail a

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
			échoué à <time in UTC>.
Contrôle	REDSHIFT-SERVERLESS-EVENT-1003	INFO	Le logiciel a été mis à jour sur votre entrepôt des données Amazon Redshift <endpoint name> à <time in UTC>.
Configuration	REDSHIFT-SERVERLESS-EVENT-1011	ERROR	Amazon Redshift sans serveur n’a pas pu créer le groupe de travail [nom du groupe de travail], car le rôle SLR (Service Linked Role) nécessaire à cette opération n’est pas accessible. Réessayez de le créer dans la console Amazon Redshift. Amazon Redshift créera le rôle SLR automatiquement.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Contrôle	REDSHIFT-SERVERLESS-EVENT-1029	ERROR	La modification du RPU de base du groupe de travail n’a pas pu être effectuée à [heure en UTC] car l’espace disque disponible est insuffisant. Réessayez avec une autre configuration.
Contrôle	REDSHIFT-SERVERLESS-EVENT-1500	ERROR	Le groupe de travail <workgroup name> ne peut pas être créé ou mis à jour, car vous avez dépassé la limite d’adresses IP Elastic de votre compte. Supprimez les adresses IP Elastic inutilisées ou demandez une augmentation de limite auprès d’Amazon EC2.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Contrôle	REDSHIFT-SERVERLESS-EVENT-1501	ERROR	Le sous-réseau <subnet id> n’a aucune adresse IP disponible. Cela empêchera les types de requêtes suivants de s'exécuter correctement sur le groupe de travail <workgroup name>: EMR, requêtes fédérées, provenant d' COPY/UNLOAD Amazon EC2. Pour corriger le problème, libérez des adresses IP de votre sous-réseau en supprimant les ENI.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Contrôle	REDSHIFT-SERVERLESS-EVENT-1502	ERROR	Le sous-réseau <subnet id> n’a aucune adresse IP disponible. <workgroup name>Cela empêchera les types de requêtes Amazon EMR, Redshift fédérées COPY/UNLOAD, Redshift et Redshift ML de s'exécuter correctement dans le groupe de travail. Pour corriger le problème, libérez les adresses IP de votre sous-réseau en supprimant les Interfaces réseau Elastic (ENI) inutilisées.
Gestion	REDSHIFT-SERVERLESS-EVENT-1008	INFO	Votre groupe de travail Amazon Redshift <workgroup name> a été créé et est prêt à être utilisé.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Gestion	REDSHIFT-SERVERLESS-EVENT-1009	INFO	Votre groupe de travail Amazon Redshift <workgroup name> a été supprimé à <time in UTC>.
Contrôle	REDSHIFT-SERVERLESS-EVENT-1000	INFO	L’instantané <snapshot name> s’est terminé à <time in UTC>.
Gestion	REDSHIFT-SERVERLESS-EVENT-1004	INFO	La restauration à partir d’un instantané sur l’espace de noms <namespace name> s’est terminée à <time in UTC>.
Gestion	REDSHIFT-SERVERLESS-EVENT-1005	ERROR	La restauration à partir d’un instantané de l’espace de noms <namespace name> a échoué à <time in UTC>.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Gestion	REDSHIFT-SERVERLESS-EVENT-1006	INFO	La restauration à partir d’un point de récupération de l’espace de noms <namespace name> s’est terminée à <time in UTC>.
Gestion	REDSHIFT-SERVERLESS-EVENT-1007	INFO	La restauration à partir d’un point de récupération de l’espace de noms <namespace name> a échoué à <time in UTC>.
Sécurité	REDSHIFT-SERVERLESS-EVENT-1012	ERROR	Amazon Redshift ne peut pas accéder au secret de votre espace de noms <nom de l’espace de noms>.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Sécurité	REDSHIFT-SERVERLESS-EVENT-1013	ERROR	Amazon Redshift ne peut pas accéder à la clé KMS qui a été utilisée pour chiffrer le secret des informations d’identification d’administrateur de votre espace de noms <nom de l’espace de noms>.
Sécurité	REDSHIFT-SERVERLESS-EVENT-1014	ERROR	Amazon Redshift ne peut pas effectuer la rotation du secret de votre espace de noms <nom de l’espace de noms>, car une opération est en cours sur le groupe de travail.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Sécurité	REDSHIFT-SERVERLESS-EVENT-1015	ERROR	Aucun groupe de travail n’est associé à votre espace de noms <nom de l’espace de noms>. Amazon Redshift peut uniquement effectuer la rotation des secrets pour les espaces de noms auxquels des groupes de travail sont attachés.
Sécurité	REDSHIFT-SERVERLESS-EVENT-1016	INFO	Informations d’identification d’administrateur mises à jour pour votre espace de noms <nom de l’espace de noms> à <heure UTC>.
Sécurité	REDSHIFT-SERVERLESS-EVENT-1030	INFO	L’opération d’enregistrement de votre espace de noms Amazon Redshift <nom de l’espace de noms> vers le compte Glue Data Catalog <id de compte> a été lancée à <heure UTC>.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Sécurité	REDSHIFT-SERVERLESS-EVENT-1031	INFO	L’opération d’enregistrement de votre espace de noms Amazon Redshift <nom de l’espace de noms> vers le compte Glue Data Catalog <id de compte> s’est terminée avec succès à <heure UTC>.
Sécurité	REDSHIFT-SERVERLESS-EVENT-1032	INFO	L’opération d’enregistrement de votre espace de noms Amazon Redshift <nom de l’espace de noms> vers le compte Glue Data Catalog <id de compte> a échoué à <heure UTC>.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Sécurité	REDSHIFT-SERVERLESS-EVENT-1033	INFO	L’opération d’annulation de l’enregistrement de votre espace de noms Amazon Redshift <nom de l’espace de noms> à partir du compte Glue Data Catalog <id de compte> a été lancée à <heure UTC>.
Sécurité	REDSHIFT-SERVERLESS-EVENT-1034	INFO	L’opération d’annulation de l’enregistrement de votre espace de noms Amazon Redshift <nom de l’espace de noms> à partir du compte Glue Data Catalog <id de compte> s’est terminée avec succès à <heure UTC>.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Sécurité	REDSHIFT-SERVERLESS-EVENT-1035	INFO	L’opération d’annulation de l’enregistrement de votre espace de noms Amazon Redshift <nom de l’espace de noms> à partir du compte Glue Data Catalog <id de compte> a échoué à <heure UTC>.
Gestion	REDSHIFT-SERVERLESS-EVENT-1036	ERROR	La mise à jour du suivi initiée par le client a échoué sur votre groupe de travail Redshift sans serveur <nom du groupe de travail>. Redonner au groupe de travail son suivi initial.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Gestion	REDSHIFT-SERVERLESS-EVENT-1037	ERROR	La mise à jour du suivi a échoué sur votre groupe de travail Redshift sans serveur <nom du groupe de travail>. La mise à jour du suivi a échoué pour votre groupe de travail Amazon Redshift sans serveur car le groupe de travail était occupé à ce moment-là. Par conséquent, le groupe de travail a retrouvé son suivi initial. Pour réessayer de mettre à jour le suivi, attendez que le groupe de travail soit moins actif, puis réessayez de mettre à jour le suivi.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Gestion	REDSHIFT-SERVERLESS-EVENT-1038	INFO	Le suivi de votre groupe de travail Amazon Redshift <nom du groupe de travail> a été modifié. Le changement de suivi est terminé.
Namespace	REDSHIFT-SERVERLESS-EVENT-1039	ERROR	Les <namespace name> AWS KMS key autorisations de l'espace de noms ne sont pas valides. Votre espace de noms entrera dans l’état « INACCESSIBLE_KMS_KEY » et vous ne pourrez plus y accéder.
Namespace	REDSHIFT-SERVERLESS-EVENT-1040	INFO	L'espace de noms <namespace name>a maintenant été restauré à son état précédent car AWS KMS key les autorisations ont été restaurées.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Namespace	REDSHIFT-SERVERLESS-EVENT-1045	INFO	Le partage de données de votre espace <datashare name>de noms Redshift Serverless <namespace name>a été supprimé en raison d'une restauration sans serveur.
Namespace	REDSHIFT-SERVERLESS-EVENT-1046	INFO	Consumer <consumer principle id>for datashare <datashare name>sur votre espace de noms Redshift Serverless <namespace name>a été révoqué en raison d'une restauration sans serveur.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Namespace	REDSHIFT-SERVERLESS-EVENT-1047	INFO	<namespace name>L'accessibilité publique a changé pour le partage de données <datashare name>sur votre espace de noms Redshift Serverless en raison de la restauration sans serveur.
Sécurité	REDSHIFT-SERVERLESS-EVENT-1048	ERROR	Votre demande de désactivation de l'intégration du Redshift-Secrets gestionnaire pour l'espace de noms <namespace name>a échoué en raison d'un problème interne. Réessayez l'opération de désinscription manuellement pour résoudre ce problème.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Sécurité	REDSHIFT-SERVERLESS-EVENT-1049	ERROR	Votre demande d'adhésion à l'intégration du Redshift-Secrets gestionnaire pour l'espace de noms <namespace name>n'a pas pu être traitée correctement en raison d'un problème interne. Faites pivoter manuellement le secret associé à votre espace de noms Redshift Serverless pour résoudre ce problème.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Sécurité	REDSHIFT-SERVERLESS-EVENT-1050	ERROR	Votre demande de réinitialisation des informations d'identification d'administrateur sur l'espace de noms <namespace name>a échoué en raison d'un problème interne. Réessayez l'opération pour réinitialiser les informations d'identification de l'utilisateur administrateur.

Zero-ETL notifications d'événements d'intégration avec Amazon EventBridge

Zero-ETL L'intégration utilise Amazon EventBridge pour gérer les notifications d'événements afin de vous tenir au courant des modifications apportées à vos intégrations. Amazon EventBridge est un service de bus d'événements sans serveur que vous pouvez utiliser pour connecter vos applications à des données provenant de diverses sources. Dans ce cas, la source de l’événement est Amazon Redshift. Les événements, qui sont des modifications surveillées dans un environnement, sont automatiquement envoyés EventBridge depuis votre entrepôt de données Amazon Redshift. Les événements sont diffusés en temps quasi réel.

EventBridge fournit un environnement dans lequel vous pouvez écrire des règles d'événements, qui peuvent spécifier les actions à entreprendre pour des événements spécifiques. Vous pouvez également définir des cibles, c'est-à-dire des ressources auxquelles un événement EventBridge peut être envoyé. Une cible peut inclure une destination d'API, un groupe de CloudWatch journaux

Amazon, etc. Pour plus d'informations sur les règles, consultez EventBridge les règles Amazon. Pour plus d'informations sur les cibles, consultez la section Amazon EventBridge Targets.

Les événements peuvent être classés par gravité et par catégorie. Les filtres suivants sont disponibles :

- Filtrage par ressources : recevez des messages en fonction de la ressource à laquelle les événements sont associés. Les ressources incluent un groupe de travail ou un instantané.
- Time window filtering (Filtrage par plages horaires) : délimitez les événements sur une période spécifique.
- Category filtering (Filtrage par catégorie) : recevez des notifications d'événements pour tous les événements des catégories spécifiées.

Le tableau suivant inclut des événements d'intégration zéro ETL, avec des métadonnées supplémentaires :

Catégorie Amazon Redshift	ID d'événement externe	Gravité de l'événement	Description du message
Contrôle	REDSHIFT-INTEGRATION-EVENT-0000	INFO	<time in UTC>Votre intégration Zero-ETL <integration name>a été créée et est devenue ACTIVE sur.
Contrôle	REDSHIFT-INTEGRATION-EVENT-0001	INFO	<time in UTC>Votre intégration Zero-ETL <integration name>a été supprimée à.
Contrôle	REDSHIFT-INTEGRATION-EVENT-0002	INFO	<time in UTC>Votre intégration Zero-ETL <integration name>a

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
			lancé la suppression à.
Contrôle	REDSHIFT-INTEGRATION-EVENT-0003	INFO	Votre intégration Zero-ETL <integration name>synchronise les données transactionnelles avec l'entrepôt de données Amazon Redshift.
Contrôle	REDSHIFT-INTEGRATION-EVENT-0004	WARNING	Amazon Redshift ne peut pas répliquer la table car elle ne contient pas de clé primaire. Ajoutez des clés primaires à la table source et la table sera automatiquement resynchronisée.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Contrôle	REDSHIFT-INTEGRATION-EVENT-0005	WARNING	Amazon Redshift ne peut pas répliquer le tableau car une ou plusieurs colonnes utilisent un type de données non pris en charge. <schema name>Modifiez votre intégration pour exclure cette table du filtre, ou supprimez des colonnes de la table source et exécutez « ALTER DATABASE <Redshift database name>INTEGRATION REFRESH TABLE ». <table name>'pour synchroniser cette table.
Contrôle	REDSHIFT-INTEGRATION-EVENT-0006	ERROR	Impossible de créer l’intégration. Supprimez et recréez l’intégration. Si l'erreur persiste, contactez le AWS Support.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Contrôle	REDSHIFT-INTEGRATION-EVENT-0007	ERROR	Impossible de charger les données en raison d'une erreur interne. Supprimez et recréez l’intégration. Si l'erreur persiste, contactez le AWS Support.
Contrôle	REDSHIFT-INTEGRATION-EVENT-0008	ERROR	L'autorisation a échoué car les autorisations ont été révoquées du cluster de base de données source. Vérifiez l'autorisation de la clé KMS si vous utilisez une clé gérée par le client (CMK) pour chiffrer l'intégration. Supprimez et recréez ensuite l'intégration.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Contrôle	REDSHIFT-INTEGRATION-EVENT-0009	ERROR	Impossible d’envoyer des données à Amazon Redshift, car le nombre de tables et de schémas dépasse la limite d’Amazon Redshift. Supprimez et recréez l’intégration.
Contrôle	REDSHIFT-INTEGRATION-EVENT-0012	ERROR	Une restauration à partir du point de récupération a été invoquée dans l’espace de noms sans serveur de destination. Supprimez et recréez l’intégration.
Contrôle	REDSHIFT-INTEGRATION-EVENT-0013	INFO	Votre intégration Zero-ETL <integration name>est désormais ACTIVE.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Contrôle	REDSHIFT-INTEGRATION-EVENT-0014	ERROR	Votre intégration <integration name>est en état d'échec car nous ne sommes pas en mesure de la modifier en raison d'une erreur interne. Supprimez et recréez l’intégration. Si l'erreur persiste, contactez le AWS Support.
Opération	REDSHIFT-INTEGRATION-EVENT-0016	INFO	Votre intégration Zero-ETL <integration name>est en train de traiter une demande de modification.
Opération	REDSHIFT-INTEGRATION-EVENT-0017	INFO	Votre modification de l’intégration zéro ETL <nom de l’intégration> a été appliquée.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Opération	REDSHIFT-INTEGRATION-EVENT-0018	WARNING	Le cluster Amazon Redshift cible est mis en pause. Attendez que le cluster soit suspendu, puis reprenez le cluster pour continuer à diffuser des données.
Opération	REDSHIFT-INTEGRATION-EVENT-0019	WARNING	Le cluster Amazon Redshift cible est suspendu. Le cluster doit être rétabli afin de continuer à diffuser des données.
Opération	REDSHIFT-INTEGRATION-EVENT-0020	WARNING	Le cluster Amazon Redshift cible est en cours de reprise. Attendez que le cluster soit actif pour continuer la diffusion des données.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Contrôle	REDSHIFT-INTEGRATION-EVENT-0025	ERROR	Une restauration sans serveur a été invoquée dans l'espace de noms sans serveur de destination, et votre intégration est désactivée car elle n'est pas disponible dans le snapshot restauré. Restaurez un instantané créé lorsque l'intégration est disponible, ou supprimez l'intégration.
Configuration	REDSHIFT-INTEGRATION-EVENT-1000	ERROR	Un ou plusieurs paramètres du cluster de bases de données Aurora source sont mal configurés. Corrigez le groupe de paramètres et redémarrez le cluster pour appliquer les modifications, puis recréez l’intégration.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Configuration	REDSHIFT-INTEGRATION-EVENT-1001	ERROR	L’intégration a échoué, car la valeur du paramètre enable_case_sensitive_identifier est incorrecte. Définissez la valeur sur true pour le cluster de bases de données Aurora source, puis supprimez et recréez l’intégration.
Configuration	REDSHIFT-INTEGRATION-EVENT-1002	ERROR	L’intégration a échoué, car la valeur du paramètre cdc_insert_enabled est incorrecte. Définissez la valeur sur true pour le cluster de bases de données Aurora source, puis supprimez et recréez l’intégration.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Configuration	REDSHIFT-INTEGRATION-EVENT-1003	ERROR	Le paramètre binlog_format du groupe de paramètres du cluster de bases de données source doit être défini sur ROW. Corrigez le groupe de paramètres et redémarrez le cluster pour appliquer la modification, puis recréez l’intégration.
Configuration	REDSHIFT-INTEGRATION-EVENT-1004	ERROR	Impossible de charger les données, car le paramètre de cluster binlog_transaction_compression est activé. Définissez la valeur du paramètre sur OFF et redémarrez l’instance de l’enregistreur pour appliquer la modification, puis recréez l’intégration.

Catégorie Amazon Redshift	ID d’événement externe	Gravité de l’événement	Description du message
Configuration	REDSHIFT-INTEGRATION-EVENT-1005	ERROR	Impossible de charger les données, car le paramètre de cluster binlog_row_value_options est défini sur PARTIAL_JSON, ce qui n’est pas pris en charge. Corrigez le groupe de paramètres et redémarrez l’instance de l’enregistreur pour appliquer la modification, puis recréez l’intégration.
Configuration	REDSHIFT-INTEGRATION-EVENT-1006	WARNING	Impossible d’analyser le filtre d’intégration. Corrigez la syntaxe du filtre.

Quotas et limites d’Amazon Redshift

Amazon Redshift dispose de quotas qui limitent l'utilisation de plusieurs ressources de votre AWS compte par région. AWS Il y a une valeur par défaut pour chaque quota et certains quotas sont ajustables.

Quotas pour les objets Amazon Redshift

Amazon Redshift dispose de quotas qui limitent l’utilisation de plusieurs types d’objet. Une valeur par défaut est définie pour chacun d’entre eux.

Nom du quota	AWS valeur par défaut	Ajustable	Description
AWS comptes que vous pouvez autoriser à restaurer un instantané par instantané	20	Non	Nombre maximal de AWS comptes que vous pouvez autoriser à restaurer un instantané, par instantané.
AWS comptes que vous pouvez autoriser à restaurer un instantané par AWS KMS key	100	Non	Nombre maximal de AWS comptes que vous pouvez autoriser à restaurer un instantané, par clé KMS. Autrement dit, si vous avez 10 instantanés chiffrés avec une seule clé KMS, vous pouvez autoriser 10 comptes AWS pour restaurer chaque instantané, ou autres combinaisons qui s’ajoutent jusqu’à 100 comptes, sans dépasser 20 comptes pour chaque instantané.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Rôles IAM du cluster permettant à Amazon Redshift d'accéder à d'autres services AWS	50 [1]	Non	Nombre maximal de rôles IAM que vous pouvez associer à un cluster pour autoriser Amazon Redshift à accéder à AWS d'autres services pour l'utilisateur propriétaire du cluster et des rôles IAM. [1] Le quota est de 10 dans les cas suivants Régions AWS : us-iso-east-1, us-iso-west-1, us-isob-east-1.
Niveau de simultanéité (emplacements de requête) pour toutes les files d’attente WLM manuelles définies par l’utilisateur	50	Non	Emplacements de requête maximum pour toutes les files d’attente définies par l’utilisateur définies par la gestion manuelle de la charge de travail.
Clusters de mise à l’échelle de la simultanéité	10	Oui	Nombre maximal de clusters de mise à l’échelle de la simultanéité.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Nœuds DC2 dans un cluster	128	Oui	Nombre maximal de nœuds DC2 que vous pouvez allouer à un cluster. Pour plus d'informations sur les limites de nœud pour chaque type de nœud, consultez Clusters et nœuds dans Amazon Redshift.
Abonnements aux événements	20	Oui	Le nombre maximum d'abonnements à des événements pour ce compte dans la AWS région actuelle.
Nœuds	200	Oui	Nombre maximal de nœuds sur toutes les instances de base de données pour ce compte dans la AWS région actuelle.
Groupes de paramètres	20	Non	Le nombre maximum de groupes de paramètres pour ce compte dans la AWS région actuelle.
Nœuds RG dans un cluster	128	Oui	Le nombre maximum de nœuds RG que vous pouvez allouer à un cluster. Pour plus d'informations sur les limites de nœud pour chaque type de nœud, consultez Clusters et nœuds dans Amazon Redshift.
Nœuds RA3 dans un cluster	128	Oui	Nombre maximal de nœuds RA3 que vous pouvez allouer à un cluster. Pour plus d'informations sur les limites de nœud pour chaque type de nœud, consultez Clusters et nœuds dans Amazon Redshift.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Redshift-managed Points de terminaison VPC connectés à un cluster	30	Oui	Le nombre maximal de points de terminaison Redshift-managed VPC que vous pouvez connecter à un cluster. Pour plus d'informations sur les points de terminaison Redshift-managed VPC, consultez. Redshift-managed Points de terminaison VPC
Bénéficiaires du cluster accessibles via un point de terminaison Redshift-managed VPC	10	Oui	Le nombre maximum de bénéficiaires qu'un propriétaire de cluster peut autoriser à créer un point de terminaison Redshift-managed VPC pour un cluster. Pour plus d'informations sur les points de terminaison Redshift-managed VPC, consultez. Redshift-managed Points de terminaison VPC
Redshift-managed Points de terminaison VPC par autorisation	10	Oui	Le nombre maximum de points de terminaison Redshift-managed VPC que vous pouvez créer par autorisation. Pour plus d'informations sur les points de terminaison Redshift-managed VPC, consultez. Redshift-managed Points de terminaison VPC
Nœuds réservés	200	Oui	Le nombre maximum de nœuds réservés pour ce compte dans la AWS région actuelle.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Schémas dans chaque base de données par cluster	9 900	Non	Nombre maximal de schémas que vous pouvez créer dans chaque base de données, par cluster. Toutefois, les schémas `pg_temp_*` ne sont pas pris en compte dans ce quota.
Groupes de sécurité	20	Oui	Le nombre maximum de groupes de sécurité pour ce compte dans la AWS région actuelle.
Taille de ligne unique lors du chargement par COPY	64	Non	Taille maximale (en Mo) d'une seule ligne lors du chargement à l'aide de la commande COPY. Il s'agit de la taille maximale d'un seul enregistrement non analysé que la commande COPY peut scanner ; un objet SUPER individuel dans la ligne est limité indépendamment à 16 Mo.
Instantanés	700	Oui	Le nombre maximum de captures d'écran utilisateur pour ce compte dans la AWS région actuelle.
Groupes de sous-réseaux	50	Oui	Le nombre maximum de groupes de sous-réseaux pour ce compte dans la AWS région actuelle.
Sous-réseaux dans un groupe de sous-réseaux	20	Oui	Nombre maximal de sous-réseaux pour un groupe de sous-réseaux.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Tableaux pour le type de nœud de `rg.large` cluster avec un cluster à nœud unique	9 900	Non	Nombre maximal de tables pour le type de nœud de cluster `rg.large` avec un cluster à nœud unique. Cette limite inclut les tables permanentes, les tables temporaires, les tables d'unités de partage des données et les vues matérialisées. Les tables externes sont comptées comme des tables temporaires. Les tables temporaires incluent les tables temporaires définies par l'utilisateur et les tables temporaires créées par Amazon Redshift pendant le traitement des requêtes ou la maintenance du système. Les vues et les tables système ne sont pas incluses dans cette limite.
Tables pour le type de nœud de `rg.large` cluster avec un cluster à plusieurs nœuds	20 000	Non	Le nombre maximal de tables pour le type de `rg.large` nœud avec un cluster à plusieurs nœuds. Cette limite inclut les tables permanentes, les tables temporaires, les tables d'unités de partage des données et les vues matérialisées. Les tables externes sont comptées comme des tables temporaires. Les tables temporaires incluent les tables temporaires définies par l'utilisateur et les tables temporaires créées par Amazon Redshift pendant le traitement des requêtes ou la maintenance du système. Les vues et les tables système ne sont pas incluses dans cette limite.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Tables pour le type de nœud de `rg.xlarge` cluster.	20 000	Non	Nombre maximal de tables pour le type de nœud de cluster `rg.xlarge` . Cette limite inclut les tables permanentes, les tables temporaires, les tables d'unités de partage des données et les vues matérialisées. Les tables externes sont comptées comme des tables temporaires. Les tables temporaires incluent les tables temporaires définies par l'utilisateur et les tables temporaires créées par Amazon Redshift pendant le traitement des requêtes ou la maintenance du système. Les vues et les tables système ne sont pas incluses dans cette limite.
Tables pour le type de nœud de cluster `rg.4xlarge`	200 000	Non	Nombre maximal de tables pour le type de nœud de cluster `rg.4xlarge` . Cette limite inclut les tables permanentes, les tables temporaires, les tables d'unités de partage des données et les vues matérialisées. Les tables externes sont comptées comme des tables temporaires. Les tables temporaires incluent les tables temporaires définies par l'utilisateur et les tables temporaires créées par Amazon Redshift pendant le traitement des requêtes ou la maintenance du système. Les vues et les tables système ne sont pas incluses dans cette limite.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Tables pour le type de nœud de cluster `rg.12xlarge`	200 000	Non	Nombre maximal de tables pour le type de nœud de cluster `rg.12xlarge` . Cette limite inclut les tables permanentes, les tables temporaires, les tables d'unités de partage des données et les vues matérialisées. Les tables externes sont comptées comme des tables temporaires. Les tables temporaires incluent les tables temporaires définies par l'utilisateur et les tables temporaires créées par Amazon Redshift pendant le traitement des requêtes ou la maintenance du système. Les vues et les tables système ne sont pas incluses dans cette limite.
Tables pour le type de nœud de cluster `ra3.large`	9 900	Non	Nombre maximal de tables pour le type de nœud de cluster `ra3.large` . Cette limite inclut les tables permanentes, les tables temporaires, les tables d'unités de partage des données et les vues matérialisées. Les tables externes sont comptées comme des tables temporaires. Les tables temporaires incluent les tables temporaires définies par l'utilisateur et les tables temporaires créées par Amazon Redshift pendant le traitement des requêtes ou la maintenance du système. Les vues et les tables système ne sont pas incluses dans cette limite.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Tables pour le type de nœud de cluster `ra3.xlplus` avec un cluster à nœud unique.	9 900	Non	Nombre maximal de tables pour le type de nœud de cluster `ra3.xlplus` avec un cluster à nœud unique. Cette limite inclut les tables permanentes, les tables temporaires, les tables d'unités de partage des données et les vues matérialisées. Les tables externes sont comptées comme des tables temporaires. Les tables temporaires incluent les tables temporaires définies par l'utilisateur et les tables temporaires créées par Amazon Redshift pendant le traitement des requêtes ou la maintenance du système. Les vues et les tables système ne sont pas incluses dans cette limite.
Tables pour le type de nœud de cluster `ra3.xlplus` avec un cluster à plusieurs nœuds.	20 000	Non	Nombre maximal de tables pour le type de nœud de cluster `ra3.xlplus` avec un cluster à plusieurs nœuds. Cette limite inclut les tables permanentes, les tables temporaires, les tables d'unités de partage des données et les vues matérialisées. Les tables externes sont comptées comme des tables temporaires. Les tables temporaires incluent les tables temporaires définies par l'utilisateur et les tables temporaires créées par Amazon Redshift pendant le traitement des requêtes ou la maintenance du système. Les vues et les tables système ne sont pas incluses dans cette limite.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Tables pour le type de nœud de cluster `ra3.4xlarge`	200 000	Non	Nombre maximal de tables pour le type de nœud de cluster `ra3.4xlarge` . Cette limite inclut les tables permanentes, les tables temporaires, les tables d'unités de partage des données et les vues matérialisées. Les tables externes sont comptées comme des tables temporaires. Les tables temporaires incluent les tables temporaires définies par l'utilisateur et les tables temporaires créées par Amazon Redshift pendant le traitement des requêtes ou la maintenance du système. Les vues et les tables système ne sont pas incluses dans cette limite.
Tables pour le type de nœud de cluster `ra3.16xlarge`	200 000	Non	Nombre maximal de tables pour le type de nœud de cluster `ra3.16xlarge` . Cette limite inclut les tables permanentes, les tables temporaires, les tables d'unités de partage des données et les vues matérialisées. Les tables externes sont comptées comme des tables temporaires. Les tables temporaires incluent les tables temporaires définies par l'utilisateur et les tables temporaires créées par Amazon Redshift pendant le traitement des requêtes ou la maintenance du système. Les vues et les tables système ne sont pas incluses dans cette limite.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Tables pour le type de nœud de cluster `dc2.large`	9 900	Non	Nombre maximal de tables pour le type de nœud de cluster `dc2.large` . Cette limite inclut les tables permanentes, les tables temporaires, les tables d'unités de partage des données et les vues matérialisées. Les tables externes sont comptées comme des tables temporaires. Les tables temporaires incluent les tables temporaires définies par l'utilisateur et les tables temporaires créées par Amazon Redshift pendant le traitement des requêtes ou la maintenance du système. Les vues et les tables système ne sont pas incluses dans cette limite.
Tables pour le type de nœud de cluster `dc2.8xlarge`	200 000	Non	Nombre maximal de tables pour le type de nœud de cluster `dc2.8xlarge` . Cette limite inclut les tables permanentes, les tables temporaires, les tables d'unités de partage des données et les vues matérialisées. Les tables externes sont comptées comme des tables temporaires. Les tables temporaires incluent les tables temporaires définies par l'utilisateur et les tables temporaires créées par Amazon Redshift pendant le traitement des requêtes ou la maintenance du système. Les vues et les tables système ne sont pas incluses dans cette limite.
Nombre de bases de données	60	Non	Le nombre maximum autorisé de bases de données dans un cluster Amazon Redshift. Cela exclut les bases de données créées à partir d'unités de partage des données.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Délai d'expiration pour les sessions en veille ou inactives	4 heures	Non	Ce paramètre s'applique uniquement au cluster. Pour plus d'informations sur la définition du délai d'inactivité de la session pour un utilisateur, consultez ALTER USER dans le Manuel du développeur de bases de données Amazon Redshift. Le paramètre utilisateur est prioritaire sur le paramètre de cluster.
Délai d'expiration des transactions inactives	6 heures	Non	Période maximale d'inactivité pour une transaction ouverte avant qu'Amazon Redshift mette fin à la session associée à la transaction. Ce paramètre est prioritaire sur tous les paramètres de délai d'expiration d'inactivité définis par l'utilisateur. Il s'applique au cluster.
Procédures stockées dans une base de données	10 000	Non	Nombre maximal de procédures stockées. Consultez Limites et différences en matière de prise en charge des procédures stockées pour connaître les autres limites.
Nombre maximum de connexions pour les nœuds RG	2 000	Non	Le nombre maximal de connexions à un cluster RG. Il s'agit d'une limite stricte qui s'applique à tous les types de nœuds RG et qui ne peut pas être augmentée.
Nombre maximal de connexions pour les nœuds RA3	2 000	Non	Nombre maximal de connexions à un cluster RA3. Il s'agit d'une limite stricte qui s'applique à tous les types de nœuds RA3 et qui ne peut pas être augmentée.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Nombre maximal de connexions pour les nœuds DC2	Varie	Non	Le nombre maximal de connexions à un cluster dc2.large est de 500. Le nombre maximal de connexions à un cluster dc2.8xlarge est de 2 000.
Nombre de rôles Amazon Redshift dans un cluster	1 000	Oui	Nombre maximal de rôles Amazon Redshift que vous pouvez créer par cluster. Pour plus d'informations sur les rôles de contrôle d'accès basé sur les rôles (RBAC), consultez la section Contrôle Role-based d'accès (RBAC) dans le manuel Amazon Redshift Database Developer Guide

Quotas pour les objets Amazon Redshift sans serveur

Amazon Redshift dispose de quotas qui limitent l’utilisation de plusieurs types d’objets dans votre espace de noms Amazon Redshift sans serveur. Une valeur par défaut est définie pour chacun d’entre eux.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Nombre de bases de données	100	Non	Nombre maximal autorisé de bases de données dans un espace de noms Amazon Redshift sans serveur. Cela exclut les bases de données créées à partir d’unités de partage des données.
Nombre de schémas	9 900	Non	Nombre maximal autorisé de schémas dans un espace de noms Amazon Redshift sans serveur.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Nombre de tables	200 000	Non	Nombre maximal autorisé de tables dans un espace de noms Amazon Redshift sans serveur.
Unités de stockage gérées Redshift pour les entrepôts de données utilisant 4 unités de traitement Redshift (RPU)	jusqu'à 32 To	Non	Stockage RMS maximal pris en charge pour un entrepôt de données doté de 4 RPU. Dans la limite de 32 To, Amazon Redshift utilise quelques centaines de Mo de stockage en interne.
Unités de stockage gérées par Redshift pour les entrepôts de données utilisant 8, 16 ou 24 unités de traitement Redshift (RPU)	jusqu'à 128 To	Non	Stockage RMS maximal pris en charge pour un entrepôt de données comportant 8, 16 ou 24 RPU. Dans la limite de 128 To, Amazon Redshift utilise quelques centaines de Mo de stockage en interne.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Délai d'expiration pour les sessions en veille ou inactives	1 heure	Non	Pour plus d'informations sur la définition du délai d'inactivité de la session pour un utilisateur, consultez ALTER USER dans le Manuel du développeur de bases de données Amazon Redshift. Le paramètre utilisateur est prioritaire.
Délai d'expiration une requête en cours d'exécution	86 399 secor (24 heures)	Non	Durée maximale d'exécution d'une requête avant qu'Amazon Redshift ne la termine.
Délai d'expiration des transactions inactives	6 heures	Non	Période maximale d'inactivité pour une transaction ouverte avant qu'Amazon Redshift sans serveur mette fin à la session associée à la transaction. Ce paramètre est prioritaire sur tous les paramètres de délai d'expiration d'inactivité définis par l'utilisateur.
Nombre maximum de connexions	2000	Non	Le nombre maximum de connexions autorisées pour se connecter à un groupe de travail.
Nombre de groupes de travail	25	Oui	Nombre de groupes de travail pris en charge.
Nombre d'espaces de noms	25	Oui	Nombre d'espaces de noms pris en charge.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Nombre de rôles Amazon Redshift dans un groupe de travail	1 000	Oui	Nombre maximal de rôles Amazon Redshift que vous pouvez créer par groupe de travail. Pour plus d'informations sur les rôles de contrôle d'accès basé sur les rôles (RBAC), consultez la section Contrôle Role-based d'accès (RBAC) dans le manuel Amazon Redshift Database Developer Guide
Unités de traitement Redshift (RPU) de base par Compte AWS	La valeur la plus élevée de 3 200 RPU ou 1,5 fois le maximum de vos RPU de base agrégées des six mois précédents.	Oui	Le Compte AWS quota pour les RPU de base Redshift Serverless est le plus élevé entre 3 200 RPU ou 1,5 fois le maximum des RPU de base cumulées des six mois précédents. .

Pour obtenir plus d’informations sur la façon dont la facturation d’Amazon Redshift sans serveur est affectée par la configuration du délai d’expiration, consultez Facturation pour Amazon Redshift sans serveur.

Quotas pour l'API de données Amazon Redshift

Amazon Redshift dispose de quotas qui limitent l'utilisation de l'API de données Redshift. Une valeur par défaut est définie pour chacun d'entre eux. Pour plus d'informations sur l'API de données Amazon Redshift, consultez Utilisation de l'API de données Amazon Redshift.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Transactions par seconde (TPS) pour l'API `BatchExecuteStatement`	20	Non	Le nombre maximum de demandes d'opérations par seconde sans être limité.
Transactions par seconde (TPS) pour l'API `CancelStatement`	3	Non	Le nombre maximum de demandes d'opérations par seconde sans être limité.
Transactions par seconde (TPS) pour l'API `DescribeStatement`	100	Non	Le nombre maximum de demandes d'opérations par seconde sans être limité.
Transactions par	3	Non	Le nombre maximum de demandes d'opérations par seconde sans être limité.

Nom du quota	AWS valeur par défaut	Ajustable	Description
seconde (TPS) pour l'API `DescribeTable`			
Transactions par seconde (TPS) pour l'API `ExecuteStatement`	30	Non	Le nombre maximum de demandes d'opérations par seconde sans être limité.
Transactions par seconde (TPS) pour l'API `GetStatementResult`	20	Non	Le nombre maximum de demandes d'opérations par seconde sans être limité.
Transactions par seconde (TPS) pour l'API `ListDatabases`	3	Non	Le nombre maximum de demandes d'opérations par seconde sans être limité.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Transactions par seconde (TPS) pour l'API `ListSchemas`	3	Non	Le nombre maximum de demandes d'opérations par seconde sans être limité.
Transactions par seconde (TPS) pour l'API `ListStatements`	3	Non	Le nombre maximum de demandes d'opérations par seconde sans être limité.
Transactions par seconde (TPS) pour l'API `ListTables`	3	Non	Le nombre maximum de demandes d'opérations par seconde sans être limité.

Quotas pour les objets de l'éditeur de requêtes v2

Amazon Redshift dispose de quotas qui limitent l'utilisation de plusieurs types d'objet dans votre éditeur de requêtes v2 Amazon Redshift. Une valeur par défaut est définie pour chacun d'entre eux.

Nom du quota	AWS valeur par défaut	Ajustable	Description
Connexions	500	Oui	Nombre maximal de connexions que vous pouvez créer à l'aide de l'éditeur de requêtes v2 dans ce compte, dans la région actuelle.
Principaux actifs par compte	50	Oui	Nombre maximal de principaux simultanées qui peuvent utiliser l'éditeur de requêtes v2 dans ce compte dans la région actuelle.
Requêtes enregistrées	2 500	Oui	Nombre maximal de requêtes enregistrées que vous pouvez créer à l'aide de l'éditeur de requêtes v2 dans ce compte, dans la région actuelle.
Versions des requêtes	20	Oui	Nombre maximal de versions par requête que vous pouvez créer à l'aide de l'éditeur de requêtes v2 dans ce compte, dans la région actuelle.
Diagrammes enregistrés	500	Oui	Nombre maximal de diagrammes enregistrés que vous pouvez créer à l'aide de l'éditeur de requêtes v2 dans ce compte, dans la région actuelle.
Taille des données récupérées par requête	100	Non	Taille maximale, en mégaoctets, des données extraites par requête par l'éditeur de requêtes v2 dans ce compte dans la région actuelle.
Taille des données récupérées par 100 lignes	5	Non	Taille maximale, en mégaoctets, des données extraites pour une page de résultats de requêtes (100 lignes) par l'éditeur de requêtes v2 dans ce compte dans la région actuelle.
Nombre maximal de connexion	3	Non	Nombre maximal de connexions à la base de données par utilisateur (y compris les sessions isolées). Cette valeur peut aller de 1 à 10 et est définie par l'adminis

Nom du quota	AWS valeur par défaut	Ajustable	Description
s simultané es			trateur de l'éditeur de requêtes v2 dans Account settings (Paramètres du compte). Si vous atteignez la limite définie par votre administrateur, envisagez d'utiliser des sessions partagées plutôt que des sessions isolées lors de l'exécution de votre instance SQL. Pour plus d'informations sur les connexions, consultez Ouverture de l'éditeur de requête v2. Pour en savoir plus sur la définition de la limite, consultez Paramètres du compte.

Quotas et limites pour les objets Amazon Redshift Spectrum

Amazon Redshift Spectrum présente les quotas et limites suivants :

- Le nombre maximum de bases de données par AWS compte lors de l'utilisation d'un AWS Glue Data Catalog. Pour cette valeur, consultez Quotas de service AWS Glue dans le Référence générale d'Amazon Web Services.
- Nombre maximal de tables par base de données lors de l'utilisation d'un AWS Glue Data Catalog. Pour cette valeur, consultez Quotas de service AWS Glue dans le Référence générale d'Amazon Web Services.
- Nombre maximal de partitions par table lors de l'utilisation d'un AWS Glue Data Catalog. Pour cette valeur, consultez Quotas de service AWS Glue dans le Référence générale d'Amazon Web Services.
- Le nombre maximum de partitions par AWS compte lors de l'utilisation d'un AWS Glue Data Catalog. Pour cette valeur, consultez Quotas de service AWS Glue dans le Référence générale d'Amazon Web Services.
- Le nombre maximum de colonnes pour les tables externes lorsque vous utilisez un AWS Glue Data Catalog, 1 597 lorsque les pseudocolonnes sont activées et 1 600 lorsque les pseudocolonnes ne le sont pas.
- La taille maximale d'une valeur de chaîne dans un fichier ION ou JSON lors de l'utilisation d'un AWS Glue Data Catalog est de 16 Ko. La chaîne peut être tronquée si vous atteignez cette limite.

- Vous pouvez ajouter 100 partitions au maximum à l'aide d'une seule instruction ALTER TABLE
- Toutes les données S3 doivent se trouver dans la même AWS région que le cluster Amazon Redshift.
- Les horodatages dans ION et JSON doivent utiliser le format ISO8601.
- La compression externe de fichiers ORC n'est pas prise en charge.
- Text, OpenCSV et Regex SERDEs ne prennent pas en charge les délimiteurs octaux supérieurs à '\177'.
- Vous devez spécifier un prédicat sur la colonne de partition pour éviter les lectures à partir de toutes les partitions.

  Par exemple, le prédicat suivant filtrera sur la colonne `ship_dtm`, mais n'appliquera pas le filtre à la colonne de partition `ship_yyyymm` :

  `WHERE ship_dtm > '2018-04-01'.`

  Pour ignorer les partitions superflues, vous devez ajouter un prédicat `WHERE ship_yyyymm = '201804'`. Ce prédicat limite les opérations de lecture à la partition `\ship_yyyymm=201804\`.

Ces restrictions ne s'appliquent pas à un metastore Apache Hive.

Contraintes d'affectation de noms

Le tableau ci-dessous décrit les contraintes d'affectation de noms dans Amazon Redshift.

Identifiant du cluster	• Un identificateur de cluster ne doit contenir que des caractères minuscules. • Il doit contenir entre 1 et 63 caractères alphanumériques ou traits d'union. • Son premier caractère doit être une lettre. • Il ne peut pas se terminer par un trait d'union ou contenir deux traits d'union consécutifs. •

	Il doit être unique pour tous les clusters au sein d'un compte AWS .
Nom de la base de données	• Le nom d'une base de données doit contenir entre 1 et 64 caractères alphanumériques. • Il doit contenir uniquement des lettres minuscules. • Il ne peut pas être un mot réservé. Pour voir une liste des mots réservés, consultez Mots réservés dans le Manuel du développeur de base de données Amazon Redshift.
Nom du point de terminaison d'un point de terminaison Redshift-managed VPC	• Le nom du point de terminaison doit contenir entre 1 et 30 caractères. • Les caractères valides sont les A-Z suivants : a-z, 0-9 et tiret (-). • Le premier caractère doit être une lettre. • Le nom ne peut pas contenir deux traits d'union consécutifs ou se terminer par un trait d'union.

Nom de l’utilisateur administrateur	• Un nom d’utilisateur administrateur doit contenir uniquement des caractères minuscules. • Il doit contenir entre 1 et 128 caractères alphanumériques. • Son premier caractère doit être une lettre. • Il ne peut pas être un mot réservé. Pour voir une liste des mots réservés, consultez Mots réservés dans le Manuel du développeur de base de données Amazon Redshift.
Mot de passe administrateur	• Un mot de passe d’administrateur doit contenir entre 8 et 64 caractères. • Il doit contenir au moins une lettre en majuscule. • Il doit contenir au moins une lettre en minuscule. • Il doit comporter un chiffre. • Il peut utiliser n’importe quels caractères ASCII avec des codes ASCII 33 à 126, sauf ’ (guillemet simple), " (guillemets doubles), :, \, / ou @.
Nom du groupe de paramètres	• Un nom de groupe de paramètres doit comporter entre 1 et 255 caractères alphanumériques ou tirets. • Il doit contenir uniquement des caractères minuscules. • Son premier caractère doit être une lettre. • Il ne peut pas se terminer par un trait d’union ou contenir deux traits d’union consécutifs.

Nom du groupe de sécurité du cluster	• Un nom de groupe de sécurité de cluster ne doit pas comporter plus de 255 caractères alphanumériques ou tirets. • Il doit contenir uniquement des caractères minuscules. • Ce ne peut pas être **`Default`**. • Il doit être unique pour tous les groupes de sécurité créés par votre AWS compte.
Nom du groupe de sous-réseau	• Un nom de groupe de sous-réseaux ne doit pas comporter plus de 255 caractères alphanumériques ou tirets. • Il doit contenir uniquement des caractères minuscules. • Ce ne peut pas être **`Default`**. • Il doit être unique pour tous les groupes de sous-rése aux créés par votre AWS compte.
Identifiant d'instantané de cluster	• Un identifiant d'instantané de cluster ne doit pas comporter plus de 255 caractères alphanumériques ou tirets. • Il doit contenir uniquement des caractères minuscules. • Ce ne peut pas être **`Default`**. • Il doit être unique pour tous les identifiants instantanés créés par votre AWS compte.

Étiqueter les ressources dans Amazon Redshift.

Dans AWS, les balises sont des étiquettes définies par l'utilisateur qui se composent de paires clé-valeur. Amazon Redshift prend en charge l'étiquetage pour fournir des métadonnées sur les ressources en un coup d'œil et pour classer vos rapports de facturation en fonction de la répartition des coûts. Pour utiliser des balises pour la répartition des coûts, vous devez d'abord activer ces balises dans le AWS Billing and Cost Management service. Pour plus d'informations sur la configuration et l'utilisation des balises à des fins de facturation, consultez Utilisation des balises de répartition des coûts pour les rapports de facturation personnalisés et Configuration de votre rapport mensuel de répartition des coûts.

Les étiquettes ne sont pas nécessaires pour les ressources dans Amazon Redshift, mais elles contribuent à fournir un contexte. Vous voudrez peut-être baliser les ressources avec les métadonnées sur les centres de coût, les noms de projet et autres informations pertinentes associées à la ressource. Par exemple, supposons que vous souhaitiez suivre quelles ressources appartiennent à un environnement de test et quelles ressources appartiennent à un environnement de production. Vous pouvez créer une clé nommée `environment` et fournir la valeur `test` ou `production` pour identifier les ressources utilisées dans chaque environnement. Si vous utilisez le balisage dans d'autres AWS services ou si vous avez des catégories standard pour votre entreprise, nous vous recommandons de créer les mêmes paires clé-valeur pour les ressources dans Amazon Redshift pour des raisons de cohérence.

Les balises sont conservées pour les ressources une fois que vous avez redimensionné un cluster et que avez restauré un instantané d'un cluster au sein de la même région. Cependant, comme les balises ne sont pas conservées si vous copiez un instantané sur une autre région, vous devez recréer les balises dans la nouvelle région. Si vous supprimez une ressource, les balises associées sont supprimées.

Chaque ressource possède un ensemble de balises, lequel constitue un ensemble d'une ou de plusieurs balises affectées à la ressource. Chaque ressource peut avoir jusqu’à 50 balises par ensemble de balises. Vous pouvez ajouter des balises lorsque vous créez une ressource et après qu'une ressource a été créée. Vous pouvez ajouter des étiquettes aux types de ressources suivants dans Amazon Redshift :

- CIDR/IP
- Cluster
- Groupe de sécurité du cluster

- Règle de trafic entrant de groupe de sécurité de cluster
- Groupe de sécurité Amazon EC2
- Connexion du module de sécurité matériel (HSM)
- Certificat de client HSM
- Groupe de paramètres
- Instantané
- Groupe de sous-réseaux
- Intégration (intégration zéro ETL

Pour utiliser le balisage à partir de la console Amazon Redshift, votre utilisateur peut joindre la politique gérée par AWS `AmazonRedshiftFullAccess`. Pour un exemple de politique IAM avec des autorisations d'étiquetage limitées que vous pouvez attacher à un utilisateur de la console Amazon Redshift, consultez Exemple 7 : Autoriser un utilisateur à labéliser des ressources avec la console Amazon Redshift. Pour plus d'informations sur le balisage, voir What is AWS Resource Groups ? .

Balisage des exigences

Les balises possèdent les exigences suivantes :

- Les clés ne peuvent pas être préfixées par `aws:`.
- Les clés doivent être uniques par ensemble de balises.
- Une clé doit comporter entre 1 et 128 caractères autorisés.
- Une valeur doit comprendre entre 0 et 256 caractères autorisés.
- Les valeurs ne doivent pas être uniques par ensemble de balises.
- Les caractères autorisés pour les clés et les valeurs sont les lettres Unicode, les chiffres, les espaces et les symboles suivants : _ . : / = + - @.
- Les clés et les valeurs sont sensibles à la casse.

Gestion des balises de ressources

La procédure suivante explique comment utiliser les balises de vos ressources.

Pour gérer les étiquettes de vos ressources Amazon Redshift

1. Connectez-vous à la console Amazon Redshift Console de gestion AWS et ouvrez-la à l'adresse. https://console.aws.amazon.com/redshiftv2/
2. Dans le menu de navigation, choisissez Configurations, puis choisissez Gérer les balises.
3. Entrez vos choix pour les ressources et choisissez quelles balises ajouter, modifier ou supprimer. Choisissez ensuite Gérer les balises des ressources que vous avez choisies.

   Les ressources que vous pouvez baliser incluent les clusters, les groupes de paramètres, les groupes de sous-réseaux, les certificats de clients HSM, les connexions HSM et les instantanés.
4. Sur la page de navigation Manage tags (Gérer les étiquettes), choisissez Review and apply tag changes (Vérifier et appliquer les modifications d'étiquettes), puis choisissez Apply (Appliquer) pour enregistrer vos modifications.

AWS Backup intégration avec Amazon Redshift

AWS Backup est un service entièrement géré qui vous aide à centraliser et à automatiser la protection des données dans l'ensemble AWS des services, dans le cloud et sur site.

Avec AWS Backup Amazon Redshift, vous pouvez configurer des politiques de protection des données et surveiller l'activité des différentes ressources Amazon Redshift en un seul endroit. Vous pouvez également créer et stocker des instantanés sur des clusters alloués Amazon Redshift et des espaces de noms sans serveur. Cela vous permet d'automatiser et de consolider les tâches de sauvegarde que vous deviez effectuer séparément auparavant, sans aucun processus manuel.

> **Note**
>
> No-backup les tables ne sont pas prises en charge pour les clusters provisionnés RG ou RA3 et les groupes de travail Amazon Redshift Serverless. Une table marquée comme non sauvegardée dans un cluster RG ou RA3 ou un groupe de travail sans serveur est traitée comme une table permanente qui sera toujours sauvegardée lors de la prise d'un instantané, et toujours restaurée lors de la restauration à partir d'un instantané. Pour éviter les coûts liés aux instantanés pour les tables sans sauvegarde, tronquez-les avant de prendre un instantané.

Une sauvegarde, ou point de restauration, représente le contenu d'une ressource, telle qu'un cluster Amazon Redshift, à une heure spécifiée. AWS Backup enregistre les sauvegardes dans des coffres-forts de sauvegarde, que vous pouvez organiser en fonction des besoins de votre entreprise. Les termes point de récupération et sauvegarde sont utilisés indifféremment. Pour plus d'informations AWS Backup, consultez la section Création, maintenance et restauration de sauvegardes dans le Guide du AWS Backup développeur.

Amazon Redshift est intégré de manière native à. AWS Backup Cela vous permet de définir vos plans de sauvegarde et d'affecter des ressources Amazon Redshift aux plans de sauvegarde. AWS Backup automatise la création de snapshots manuels Amazon Redshift et stocke ces instantanés en toute sécurité dans un coffre de sauvegarde que vous désignez dans votre plan de sauvegarde. Pour de plus amples informations sur les coffres-forts, consultez Coffres-forts de sauvegarde dans le Guide du développeur AWS Backup . Dans le plan de sauvegarde, vous pouvez définir la fréquence de sauvegarde, la fenêtre de sauvegarde, le cycle de vie ou le coffre-fort de sauvegarde. Pour

plus d’informations sur les plans de sauvegarde, consultez Plans de sauvegarde dans le Guide du développeur AWS Backup .

Pour plus d’informations sur la création et la restauration d’instantanés Amazon Redshift sans serveur sans utiliser AWS Backup, consultez Instantanés et points de récupération. Pour plus d'informations sur la création et la restauration d'instantanés de clusters provisionnés par Amazon Redshift sans utiliser, consultez. AWS Backup Instantanés et sauvegardes Amazon Redshift

Rubriques

- Considérations relatives à l'utilisation AWS Backup avec Amazon Redshift
- Restrictions d'utilisation AWS Backup avec Amazon Redshift
- Gestion AWS Backup avec Amazon Redshift

Considérations relatives à l'utilisation AWS Backup avec Amazon Redshift

Voici les points à prendre en compte lors de l'utilisation AWS Backup d'Amazon Redshift :

- AWS Backup pour Amazon Redshift est disponible là où Amazon Redshift AWS Backup et Amazon Redshift sont disponibles de la même manière. Régions AWS Pour savoir où cette option AWS Backup est disponible, consultez la section Points de terminaison et quotas Amazon Redshift dans. Références générales AWS
- Pour commencer à l'utiliser AWS Backup, vérifiez que vous avez rempli toutes les conditions requises. Pour plus d’informations, consultez Prérequis dans le Guide du développeur AWS Backup .
- Inscrivez-vous affirmativement au service. AWS Backup Opt-in les choix s'appliquent au compte spécifique et Région AWS. Si vous souhaitez utiliser des sauvegardes dans plusieurs régions avec un compte donné, vous devez vous connecter à chaque région avec ce compte. Pour plus d’informations, consultez les Activation de la gestion des services avec AWS Backup dans le Guide du développeur AWS Backup .
- AWS Backup l'intégration pour Amazon Redshift prend uniquement en charge les instantanés manuels pour les clusters provisionnés et les espaces de noms sans serveur.
- Une fois que vous avez utilisé AWS Backup pour gérer les paramètres des instantanés, vous ne pouvez plus continuer à gérer les paramètres des instantanés manuels à l'aide d'Amazon Redshift.

Au lieu de cela, vous pouvez continuer à gérer les paramètres à l'aide d'un AWS Backup plan. Pour plus d'informations, consultez Plans de sauvegarde dans le Guide du développeur AWS Backup .

- Restaurer des instantanés d'un entrepôt de données entier dans un espace de noms sans serveur constitue un changement destructeur. Toutes les données existantes dans l'espace de noms cible sont perdues lorsque vous restaurez un instantané d'entrepôt de données dans cet espace de noms. Cela s'applique uniquement à la restauration des instantanés de l'entrepôt de données. La restauration d'instantanés d'une seule table dans un espace de noms ne supprime pas les données existantes.
- Pour restaurer un instantané sur un cluster alloué, vous devez disposer d'une politique IAM avec l'autorisation `RestoreFromClusterSnapshot`. Pour restaurer un instantané dans un espace de noms sans serveur, vous devez disposer d'une politique IAM avec l'autorisation `RestoreFromSnapshot`. Ces autorisations s'appliquent au type d'entrepôt de données cible, et non au type d'instantané source. Par exemple, pour restaurer un instantané de cluster dans un espace de noms, vous aurez besoin de l'autorisation `RestoreFromSnapshot`, pas `RestoreFromClusterSnapshot`. Pour de plus amples informations sur la gestion des politiques IAM, consultez Identity and Access Management dans Amazon Redshift.

Restrictions d'utilisation AWS Backup avec Amazon Redshift

Les limites d'utilisation AWS Backup avec Amazon Redshift sont les suivantes :

- Vous ne pouvez pas l'utiliser AWS Backup pour gérer les instantanés automatisés Amazon Redshift. Pour gérer des instantanés automatisés, utilisez des balises. Pour plus d'informations sur le balisage des ressources, consultez Étiquetage des ressources Amazon Redshift.
- Lorsque vous restaurez des tables individuelles à partir d'un instantané, vous ne pouvez pas effectuer de restauration à partir d'un instantané de cluster alloué vers un espace de noms sans serveur ou vice versa. Vous pouvez restaurer des instantanés complets dans n'importe quelle configuration. Par exemple, vous pouvez restaurer toutes les bases de données d'un instantané de cluster alloué dans un espace de noms sans serveur, mais vous ne pouvez pas restaurer une seule table de ce même instantané vers le même espace de noms.

Gestion AWS Backup avec Amazon Redshift

Pour protéger les ressources de vos entrepôts de données Amazon Redshift, vous pouvez utiliser la AWS Backup console ou utiliser par programmation l' AWS Backup API ou (). AWS Command

Line Interface AWS CLI Lorsque vous devez récupérer une ressource, vous pouvez utiliser la AWS Backup console ou le AWS CLI pour rechercher et récupérer la ressource dont vous avez besoin. Pour de plus amples informations, veuillez consulter AWS Command Line Interface.

Lorsque vous utilisez AWS Backup Amazon Redshift, vous pouvez effectuer les actions suivantes :

- Créez des sauvegardes périodiques qui déclenchent automatiquement des instantanés Amazon Redshift. Les sauvegardes périodiques sont utiles pour répondre à vos besoins de conservation des données à long terme. Pour en savoir plus, consultez Sauvegardes Amazon Redshift dans le Guide du développeur AWS Backup .
- Automatisez la planification et la rétention des sauvegardes en configurant les plans de sauvegarde de manière centralisée.
- Restaurez un cluster mis en service ou un espace de noms sans serveur dans la sauvegarde enregistrée de votre choix. Vous pouvez choisir de restaurer toutes les données de l'instantané ou une seule table à partir de celui-ci. Vous définissez la fréquence à laquelle vous souhaitez sauvegarder vos ressources. Pour plus d'informations sur la restauration d'instantanés de clusters alloués, consultez Restaurer un cluster Amazon Redshift dans le Guide du développeur AWS Backup . Pour plus d'informations sur la restauration des instantanés d'espaces de noms sans serveur, consultez Restauration Amazon Redshift sans serveur dans le Guide du développeur AWS Backup .

Versions de cluster pour Amazon Redshift

Amazon Redshift publie régulièrement des versions de cluster. Vos clusters Amazon Redshift sont corrigés pendant la fenêtre de maintenance de votre système. La date d'application du correctif dépend de vos paramètres Région AWS et de ceux de votre fenêtre de maintenance. Vous pouvez consulter et modifier vos paramètres de fenêtre de maintenance à partir de la console Amazon Redshift. Pour plus d'informations sur la maintenance, consultez Maintenance du cluster.

Vous pouvez consulter la version de votre cluster dans l'onglet Maintenance de la console Amazon Redshift. Vous pouvez également voir la version du cluster dans la sortie de la commande SQL :

```
SELECT version();
```

> **Note**
>
> Les mises à jour critiques qui affectent le comportement d'Amazon Redshift sont introduites au fur et à mesure de l'évolution d'Amazon Redshift. Pour suivre ces changements, prendre des mesures et éviter d'éventuelles perturbations de vos charges de travail, consultez Changements de comportement dans Amazon Redshift.

Rubriques

- Correctif 205 d'Amazon Redshift
- Correctif 204 d'Amazon Redshift
- Correctif 203 d'Amazon Redshift
- Correctif 202 d'Amazon Redshift
- Correctif 201 d'Amazon Redshift
- Patch 200 d'Amazon Redshift
- Correctif 199 d'Amazon Redshift
- Correctif 198 d'Amazon Redshift
- Correctif 197 d'Amazon Redshift
- Patch 196 d'Amazon Redshift
- Correctif 195 d'Amazon Redshift
- Correctif 194 d'Amazon Redshift

- Correctif 193 d'Amazon Redshift
- Correctif 192 d'Amazon Redshift
- Correctif 191 d'Amazon Redshift
- Patch 190 d'Amazon Redshift
- Correctif 189 d'Amazon Redshift
- Correctif 188 d'Amazon Redshift
- Correctif 187 d'Amazon Redshift
- Correctif 186 d'Amazon Redshift
- Correctif 185 d'Amazon Redshift
- Correctif 184 d'Amazon Redshift
- Correctif 183 d'Amazon Redshift
- Correctif 182 d'Amazon Redshift
- Correctif 181 d'Amazon Redshift
- Correctif 180 d’Amazon Redshift
- Correctif 179 d’Amazon Redshift
- Correctif 178 d’Amazon Redshift
- Correctif 177 d’Amazon Redshift
- Correctif 176 d’Amazon Redshift
- Correctif 175 d’Amazon Redshift
- Correctif 174 d’Amazon Redshift
- Correctif 173 d’Amazon Redshift
- Correctif 172 d’Amazon Redshift
- Correctif 171 d’Amazon Redshift
- Correctif 170 d’Amazon Redshift
- Correctif 169 d’Amazon Redshift
- Correctif 168 d’Amazon Redshift

Correctif 205 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.477953 — Version actuelle du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 6 octobre 2026
- 1.0.434008 — CURRENT Track, version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiée le 16 septembre 2026

Nouvelles fonctionnalités et améliorations de ce correctif

- Iceberg MV : vues matérialisées stockées dans Iceberg offrant une actualisation incrémentielle et un recalcul complet.
- Les tables système incluent désormais une `external_user_id` colonne qui enregistre l'identité durable IAM ou IAM Identity Center associée à chaque requête, ce qui permet de filtrer par utilisateur les événements du cycle de vie du cluster.
- Les requêtes Amazon Redshift Spectrum sur des tables externes prennent désormais en charge la lecture des fichiers compressés gzip et Text/CSV bzip2.
- Ajout de la prise en charge du mot clé IAM_ROLE « SESSION » pour COPY et UNLOAD, permettant aux clients d'utiliser des informations d'identification FAS liées à la session pour accéder à Amazon S3 au lieu de spécifier un ARN de rôle IAM explicite.
- Ajouté`ALTER DATABASE ... INTEGRATION REFRESH REMEDIABLE TABLES`, qui resynchronise les tables zéro ETL signalées par un avertissement de date dupliquée à la demande, éventuellement étendues à un schéma.
- Ajout de la CloudWatch métrique `IntegrationLatestSourceCommit` Amazon pour les intégrations sans ETL, qui indique le dernier temps de validation de la source observé afin que vous puissiez distinguer une source inactive d'un pipeline bloqué.
- Amazon Redshift permet désormais à un administrateur d'augmenter la longueur minimale requise pour les mots de passe des utilisateurs de base de données en utilisant `ALTER SYSTEM SET passwd_min_length = N` (8—32).
- Correction d'un problème d'`ALTER IDENTITY PROVIDER ... ENABLE`échec dû à une erreur de paramètres incorrects sur les fournisseurs d'identité Azure configurés pour créer automatiquement des rôles.
- Amazon Redshift prend désormais en charge l'échange de clés hybride post-quantique (`X25519MLKEM768`) pour les connexions TLS.
- Amazon Redshift prend désormais en charge une `DEBUG` autorisation sur les bases de données de catalogues d'autorisations fédérées, ce qui permet à une identité globale, à un groupe IAM Identity Center (iDC) ou aux administrateurs d'un compte client de consulter les enregistrements

de journalisation sécurisés non expurgés pour les données protégées par le contrôle d'accès fin (FGAC).

- Amazon Redshift prend désormais en charge les autorisations étendues grâce à Metadata Security.
- Les tables Iceberg peuvent désormais être créées avec une contrainte de colonne NOT NULL.
- Les événements CloudTrail d'audit Amazon pour les appels d' Redshift-initiated API Amazon incluent désormais un `queryUuid` champ de corrélation avec les tables système.
- Pour des raisons de cohérence, la `user_query_uuid` colonne a été renommée `query_uuid` dans les tables et les vues du système.
- Amélioration des performances et de la disponibilité des requêtes sur les clusters avec des intégrations zéro ETL en cas de forte simultanéité des requêtes.
- Les contrôles d'autorisation sur les tables comportant un grand nombre de colonnes et peu d'autorisations au niveau des colonnes sont désormais plus rapides, ce qui accélère les requêtes de métadonnées et les outils clients qui répertorient les privilèges des tables.
- Stabilité améliorée pour les requêtes utilisant des UDF Lambda dans les agrégats.
- L'élimination automatique des ballonnements permet désormais au superbloc de rétrécir pour s'adapter à son ensemble d'embouts sous tension, évitant ainsi d'avoir à récupérer le ballonnement par le biais du Superblock Vacuum (SBV).
- Tri automatique des tableaux amélioré pour réduire la croissance de l'espace de stockage sur les tables comportant un grand nombre de colonnes.
- Correction d'un problème qui pouvait empêcher l'exécution de l'aspirateur automatique sur un cluster jusqu'à ce que celui-ci soit redémarré.
- Correction d'un problème qui pouvait provoquer le redémarrage d'un cluster lors d'une opération de mise sous vide sur des clusters utilisant la gestion automatique de la charge de travail avec le dimensionnement simultané.
- Correction d'un bogue qui pouvait entraîner des erreurs d'inférence de type pour les CTE récursifs contenant des chaînes littérales.
- Correction d'un problème à cause duquel les requêtes PostgreSQL fédérées pouvaient se bloquer sur une base de données distante qui ne répondait pas et ignorait les demandes d'annulation.
- Correction d'un rare redémarrage du cluster provoqué par un double relâchement dans la gestion de l'état de charge COPY sous pression sur la mémoire.
- Correction d'un problème en raison duquel les commandes de `SHOW` découverte ne pouvaient pas obtenir de résultats lorsqu'un schéma long était défini dans la `LIKE` clause.

- Correction d'un problème en raison duquel la création ou la publication d'un partage de données pouvait échouer sur un cluster ayant atteint son nombre maximal de rôles de base de données.
- L'annulation d'une `DROP DATABASE` commande entraîne désormais la fin de la commande par une erreur au lieu de provoquer un redémarrage inattendu du cluster.
- Fiabilité améliorée des procédures stockées qui interrogent plusieurs fois les tables Iceberg, puis une requête sur une table locale lorsque le dimensionnement simultané est utilisé.
- Fiabilité améliorée des sessions qui associent des curseurs Iceberg à des requêtes autres que celles d'Iceberg lorsque le dimensionnement de la simultanéité est activé.
- Ajout de la possibilité de rendre annulable l'attente IPC du fdisk fetch-block afin qu'un ACK perdu devienne une requête destructible au lieu d'un blocage impossible à tuer.
- Amélioration de la fiabilité du processus interne utilisé lors du redimensionnement élastique en ligne afin de le rendre plus deterministic/robust performant.

Correctif 204 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.436211 — Version du cluster provisionné par TRAILING Track pour Amazon Redshift et version pour groupe de travail Amazon Redshift Serverless — Publiée le 22 septembre 2026
- 1.0.436211 — CURRENT Track, version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiée le 10 septembre 2026
- 1.0.416217 — CURRENT Track, version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiée le 25 août 2026
- 1.0.394035 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 11 août 2026

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajout du support pour les clusters rg.large à nœud unique. Il s'agit de la version de cluster minimale requise pour créer un cluster rg.large à nœud unique.
- Ajout d'une colonne query_uuid aux tables et aux vues système, fournissant un identifiant de requête unique au monde qui persiste tout au long des cycles de cluster. pause/resume
- Ajout de user_query_id à la table stl_udf_log pour supprimer la dépendance aux jointures stl_user_query_map dans les définitions de vue sys_.

- Ajout de deux nouvelles CloudWatch métriques Amazon IntegrationLatestDetectedChange et, pour les intégrations sans ETL IntegrationLatestAppliedChange, afin de permettre le suivi de l'état de la réplication.
- Ajout de l'option AUTO_REMEDIATION pour CREATE DATABASE et ALTER DATABASE sur les bases de données d'intégration sans ETL. Lorsque AUTO_REMEDIATION est défini, Amazon Redshift resynchronise automatiquement les tables présentant des problèmes de réplication. Les détails apparaissent dans svv_integration_table_state.reason.
- Ajout de la prise en charge de la lecture, de la création et de l'écriture dans les tables Apache Iceberg v3 à l'aide du moteur natif Amazon Redshift. Cela inclut la prise en charge des valeurs par défaut, du lignage des lignes et des vecteurs de suppression pour tous les types de données précédemment pris en charge. Support pour les types de données Variant, Géographie et Géométrie n'est pas inclus dans cette version et sera annoncé dans un futur correctif.
- Après la mise à niveau d'une table Iceberg vers la version 3, le type Iceberg est mappé au `timestamptz` type Amazon Redshift. `TIMESTAMPTZ` Dans les tables Iceberg v2, `timestamptz` est mappé au type Amazon `TIMESTAMP` Redshift. Avec la version 3, cela signifie que vos requêtes génèrent l'horodatage en fonction de leur fuseau horaire.
- Ajout de la prise en charge de `CURSOR` s qui dépassent la taille maximale du jeu de résultats pour le type d'instance. Lorsque le jeu de résultats d'un curseur dépasse la capacité de disque disponible, Amazon Redshift transmet automatiquement les données de dépassement à Amazon S3. Cette fonctionnalité peut être activée par cluster sur demande auprès du AWS Support.
- Ajout de nouvelles colonnes de métriques de regroupement à la table `stl_fasma_data_cache_stats` système pour surveiller l'activité du cache.
- L'analyse syntaxique et sémantique des requêtes faisant référence aux Late Binding Views (LBV) s'effectue désormais sur les clusters de consommateurs. Cela élimine un goulot d'étranglement du côté du producteur dans le traitement du LBV.
- Amazon Redshift ML active désormais l'option de chiffrement du trafic inter-conteneurs lorsqu'il envoie `CreateAutoMLJob` et demande `CreateProcessingJob` à Amazon. SageMaker Cela correspond au paramètre déjà appliqué `BuildTrainingRequest` et empêche les alertes du scanner de sécurité.
- Performances d'intégration zéro ETL améliorées pour les charges de travail à haute fréquence afin de réduire le délai de réplication pour les tables comportant de nombreuses mises à jour simultanées.
- Zero-ETL les intégrations signalent désormais correctement les données source dépassant la longueur de colonne cible en tant qu'erreur non récupérable.

- Stabilité d'intégration Zero-ETL améliorée après le redémarrage du cluster.
- Les schémas vides sont désormais automatiquement nettoyés lorsqu'une modification du filtre de table sur une intégration zéro ETL supprime toutes les tables d'un schéma.
- Amélioration du message d'erreur lors de la tentative de suppression de la base de données sur une base de données avec une intégration zéro-ETL active.
- Les intégrations DynamoDB Zero-ETL respectent désormais les options ACCEPTINVCHARS et TRUNCATECOLUMNS lors de l'ensemencement initial et de la réplication continue. Les tables continuent à se répliquer lorsque la source contient des UTF-8 caractères non valides.
- Performances de requêtes améliorées sur les clusters dotés d'intégrations zéro ETL, en particulier pour les charges de travail qui répliquent de nombreuses bases de données ou tables.
- Performances améliorées pour les charges de travail à l'aide de tables temporaires, réduction de la charge d'accès aux catalogues et amélioration du débit global.
- Les commandes de découverte SHOW telles que SHOW TABLES, SHOW SCHEMAS, SHOW COLUMNS et SHOW GRANTS renvoient désormais jusqu'à 133 500 objets. Ainsi, les listes de métadonnées sur les schémas et les bases de données contenant un très grand nombre d'objets réussissent au lieu d'échouer avec une erreur de limite de ligne de 10 000.
- Lorsqu'une commande DROP USER est rejetée parce que l'utilisateur possède toujours des objets ou détient des privilèges, le message d'erreur nomme désormais l'objet bloquant spécifique et indique le nombre d'autres dépendances restantes.
- Amazon Redshift met désormais en cache les informations d'identification du rôle IAM sur le nœud principal. Cela réduit le temps de récupération pour les requêtes COPY, UNLOAD, Amazon Redshift Spectrum et Lambda UDF. Les informations d'identification fréquemment utilisées sont réutilisées entre les requêtes, ce qui améliore le temps de démarrage des requêtes.
- AWS L'authentification IAM Identity Center fonctionne désormais sur les clusters et les groupes de travail avec le routage VPC amélioré activé.
- Détection améliorée de l'état du disque pour les types de nœuds RG afin d'éviter les corrections matérielles automatiques inutiles sur les clusters fonctionnant sur un disque normal. I/O
- Performances de partage de données améliorées en omettant une copie supplémentaire dans le processus principal.
- Prise en charge étendue de la taille des consommateurs pour les requêtes d'écriture dans plusieurs entrepôts.
- Stabilité améliorée pour les User-Defined fonctions Lambda sans arguments dans les jointures.
- Correction d'un problème dans le calcul de la clé de tri MDDL lorsque les prédicats incluent IDF.

- Correction d'un problème en raison duquel les requêtes sur des tables externes, des objets de partage de données et des références entre bases de données échouaient avec le message « transaction en lecture seule » lorsqu'elles étaient exécutées dans les transactions BEGIN READ ONLY.
- Correction d'une situation rare dans laquelle un COPY ou un INSERT s'exécutant en même temps que l'optimisation automatique d'une table sur la même table pouvait provoquer le redémarrage du cluster.
- Correction d'une erreur de codage rare qui pouvait entraîner l'échec de l'optimisation automatique des tables sur les tables accessibles via le partage de données créées sur d'anciennes versions de cluster.
- Correction d'une situation rare dans laquelle le vide automatique sur des tables présentant une distribution de données asymétrique pouvait provoquer le redémarrage du cluster.
- Correction d'un problème en raison duquel une tâche de copie automatique pouvait arrêter de progresser et bloquer d'autres opérations de copie automatique sur le même cluster.
- Correction d'une situation rare dans laquelle une commande COPY pouvait provoquer le redémarrage du cluster en raison d'une course lors du nettoyage des requêtes.
- Problème résolu : svl_s3query_summary.s3query_returned_rows pouvait signaler une ligne supplémentaire pour les requêtes comportant une clause LIMIT sur des tables externes.
- Correction d'un rare redémarrage de cluster qui pouvait se produire pendant le bootstrap sur des clusters avec des intégrations zéro ETL et aucune tâche Auto COPY configurée.
- Correction d'un problème lié à l'analyse des champs COPY lors de l'utilisation d'un délimiteur de caractères multiples avec l'option ESCAPE.
- Correction d'un problème en raison duquel les commandes COPY et UNLOAD échouaient lorsque les utilisateurs connectés via IAM Identity Center fournissaient des informations d'identification temporaires explicites à l'aide du paramètre CREDENTIALS.
- Correction d'un problème dans SHOW CONSTRAINTS qui pouvait provoquer le redémarrage du cluster.
- Problème résolu : l'autorisation CONNECT accordée à un rôle empêchait les utilisateurs d' AWS IAM Identity Center du groupe mappé de se connecter aux bases de données avec les autorisations fédérées Amazon Redshift activées.
- Correction d'un problème en raison duquel l'exécution des requêtes utilisant UNNEST sur des baies SUPER était incorrectement bloquée sur des clusters de dimensionnement simultanés.

- Correction d'un problème en raison duquel la fonction ARRAY_SORT pouvait échouer en raison d'une erreur de navigation par chemin lorsqu'elle était appliquée à des structures SUPER imbriquées.
- Correction d'un problème à cause duquel des expressions partiQL ou SUPER profondément imbriquées pouvaient provoquer le redémarrage du cluster.
- Correction d'un problème en raison duquel la fonction TO_NUMBER pouvait échouer lorsque la chaîne de format spécifiait une précision supérieure à 38.
- Correction d'un problème en raison duquel la rotation des clés de chiffrement pouvait corrompre les clés des tables greffées, ce qui pouvait entraîner des échecs d'accès aux données.
- Correction de situations d'interblocage des opérations de stockage susceptibles de provoquer le blocage des requêtes ou le manque de réactivité des nœuds.
- Correction d'un crash rare lors de la gestion des blocs de disque susceptible de provoquer le redémarrage des nœuds.
- Correction d'un crash causé par un manque de mémoire lors de l'allocation de blocs qui pouvait entraîner le redémarrage des nœuds.
- Correction d'un crash en cas de saturation du disque lors de l'attribution de la réplication par blocs, susceptible de provoquer le redémarrage des nœuds.

Correctif 203 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.417950 — Version du cluster provisionné par TRAILING Track pour Amazon Redshift et version pour groupe de travail Amazon Redshift Serverless — Publiée le 26 août 2026
- 1.0.417950 — CURRENT Track, version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiée le 25 août 2026
- 1.0.400034 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 17 août 2026
- 1.0.384821 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 4 août 2026
- 1.0.377293 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 25 juillet 2026
- 1.0.365190 — Version actuelle du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 21 juillet 2026

- 1.0.347559 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 6 juillet 2026

Nouvelles fonctionnalités et améliorations de ce correctif

- Une nouvelle colonne a été ajoutée à stl_alter_dist_sort pour indiquer si les opérations ALTER DISTKEY et ALTER SORTKEY ont été exécutées sur le cluster principal, un consommateur de partage de données ou un cluster de dimensionnement simultané.
- Ajout de la syntaxe SHOW GRANTS FOR GROUP pour découvrir les autorisations accordées à un groupe d'utilisateurs spécifique.
- Observabilité améliorée de l'intégration zéro ETL en ajoutant un statut de réussite granulaire pour les points de contrôle, permettant ainsi un suivi plus précis de la progression de la réplication dans les tables système.
- A introduit une gestion élégante des UTF-8 caractères non pris en charge dans les schémas de tables sources et les métadonnées DDL dans le cadre des intégrations sans ETL, évitant ainsi les échecs d'intégration.
- Amazon Redshift prend désormais en charge le dimensionnement simultané pour actualiser les vues matérialisées (MV) en streaming connectées à Amazon Kinesis Data Streams (KDS).
- À partir du correctif 203, Amazon Redshift commence à imposer la fin du support pour les UDF Python existants. La création de nouveaux UDF Python a été abandonnée dans le patch 198, et toute prise en charge des UDF Python prend fin après le 30 juin 2026. Migrez vos UDF Python existants vers des UDF Lambda pour garantir le fonctionnement continu. Pour obtenir des conseils de migration, consultez Amazon Redshift Python : le support des fonctions définies par l'utilisateur prendra fin après le 30 juin 2026 et les bonnes pratiques relatives aux fonctions définies par l'utilisateur Amazon Redshift Lambda sur le blog Big Data. AWS Pour plus de détails sur les changements de comportement, voirLes fonctions scalaires Python définies par l’utilisateur ne seront plus prises en charge après le 30 juin 2026.
- Les tables chargées avec COPY depuis Amazon Redshift Spectrum, avec des codages de colonne explicites, ou dans des tables non vides peuvent désormais bénéficier de l'attribution automatique de DISTKEY lorsque la table possède une clé primaire, ce qui améliore les performances des requêtes pour les jointures sur la clé primaire.
- Mise à jour du message d'erreur ALTER TABLE... ALTER DISTKEY sur les tables de partage de données pour afficher le nom de la table destinée aux clients.

- Réduction de l'activité en arrière-plan due au vide automatique sur les clusters contenant un très grand nombre de tables, améliorant ainsi la stabilité des clusters qui subissaient auparavant une activité de maintenance excessive.
- Performances de requêtes optimisées en combinant des sous-requêtes avec des filtres, une agrégation et des fonctions de fenêtre incompatibles dans certains cas.
- Précision d'horodatage améliorée pour les requêtes de voyage dans le temps sur des tables sans ETL avec le mode historique d'Amazon DynamoDB suite à une resynchronisation des tables.
- Zero-ETL les intégrations n'entrent plus dans une boucle de resynchronisation lors du traitement des points de contrôle CDC sur des tables avec certaines configurations de clés primaires.
- Amélioration du signalement des erreurs d'intégration Zero-ETL pour les expressions de filtre de canal non valides.
- Le texte de la requête d'origine n'est plus masqué par Secure Logging (s'applique aux requêtes portant sur une vue externe de AWS Lake Formation ou une base de données avec des autorisations Amazon Redshift fédérées).
- Amélioration des performances d'ANALYZE pour les grandes tables jusqu'à 30 %.
- Performances améliorées pour les requêtes utilisant les User-Defined fonctions AWS Lambda avec les agrégations ROLLUP.
- Amélioration des performances de requête pour la clause ORDER BY with LIMIT en évitant les analyses de données inutiles sur la table externe de Hash Join.
- Réduction de la consommation de mémoire lors des opérations de balayage de l'arborescence en arrière-plan, éliminant ainsi les pannes de nœuds sur l'ensemble du parc. Limitation de l'encombrement mémoire lié au balayage arborescent des nœuds de calcul en mettant en œuvre le déchargement par lots compté des survivants, empêchant ainsi une croissance illimitée de la mémoire en cas de perte de métadonnées élevée. Tree-sweep les chemins sont désormais fermés à la fin de la rediffusion de l'arborescence en arrière-plan.
- Amélioration de la reprise après incident après les échecs de lecture d'Amazon S3, éliminant ainsi les pannes de nœuds. L'itérateur Trickle Tree est désormais correctement réinitialisé après un échec de lecture d'Amazon S3, ce qui garantit que les lectures suivantes sont réessayées correctement au lieu de renvoyer silencieusement des données périmées ou incomplètes.
- Correction d'un problème à cause duquel les tables modifiées avec ALTER TABLE... ALTER DISTSTYLE AUTO après un redimensionnement de cluster adaptatif pouvaient rester indéfiniment à l'état En attente dans sys_restore_state.
- Correction d'un problème en raison duquel la vue système SYS_QUERY_TEXT pouvait afficher le texte de la requête sans espaces ou diviser les mots de manière incorrecte aux limites des blocs.

- Correction d'un échec de démarrage dû à des intégrations zéro ETL pour les clusters créés entre août 2023 et mars 2024, en raison d'incohérences dans les métadonnées du catalogue Amazon Redshift.
- Correction d'un problème à cause duquel SHOW GRANTS affichait incorrectement les autorisations accordées à un groupe d'utilisateurs ayant le « rôle » identity_type.
- Correction d'un problème à cause duquel les requêtes pouvaient être bloquées indéfiniment pendant la gestion de la suspension de session.
- Correction d'un problème à cause duquel les non-superutilisateurs utilisant SYSLOG ACCESS UNRESTRICTED ne pouvaient voir que leurs propres données de session dans sys_session_history au lieu de voir les sessions de tous les utilisateurs comme prévu.
- Correction d'un problème en raison duquel les limites de connexion de base de données ou d'utilisateur définies à 1 000 ou plus étaient tronquées, empêchant ainsi le nombre correct de connexions.
- Correction d'un problème en raison duquel les requêtes pouvaient être bloquées indéfiniment en raison de la pression de la mémoire.
- Correction d'un problème à cause duquel les points de terminaison Amazon Redshift Serverless pouvaient être brièvement indisponibles pendant la pause des opérations.
- Correction d'un problème en raison duquel les commandes COPY avec certaines combinaisons de paramètres pouvaient échouer de façon inattendue lors de la compilation des requêtes.
- Problème résolu : les requêtes utilisant APPROXIMATE PERCENTILE_DISC avec GROUP BY pouvaient échouer en raison d'une erreur de compilation.
- Correction d'un problème de résultats erronés en raison duquel les requêtes utilisant des expressions COLLATE pouvaient renvoyer des valeurs de colonne incorrectes.
- Correction d'un problème en raison duquel les fonctions LEAST et GREATEST avec des valeurs de type SUPER pouvaient entraîner l'échec des requêtes.
- Correction d'un problème de résultats erronés dans REGEXP_REPLACE, à cause duquel les chaînes de remplacement contenant des références à des groupes de capture pouvaient produire une sortie tronquée.
- Correction d'une corruption potentielle des données lors de lectures de re-réplication abandonnées. Résolution d'un problème de double absence qui pouvait se produire lorsqu'une lecture de re-réplication était abandonnée en plein vol, empêchant ainsi une éventuelle corruption de la mémoire ou des pannes.

Correctif 202 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.369760 — Version du cluster provisionné par TRAILING Track pour Amazon Redshift et version pour groupe de travail Amazon Redshift Serverless — Publiée le 29 juillet 2026
- 1.0.377292 — Version du cluster provisionné par TRAILING Track pour Amazon Redshift et version pour groupe de travail Amazon Redshift Serverless — Publiée le 25 juillet 2026
- 1.0.377292 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 25 juillet 2026
- 1.0.358853 — TRAILING Track, version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiées le 21 juillet 2026
- 1.0.358853 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 14 juillet 2026
- 1.0.343555 — Version actuelle du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 29 juin 2026
- 1.0.340728 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 22 juin 2026
- 1.0.331549 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 16 juin 2026
- 1.0.323213 — CURRENT Track, version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiée le 3 juin 2026
- 1.0.314775 — Version actuelle du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 28 mai 2026

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajout du support pour les types de nœuds RG (multi-nœuds rg.large et rg.12xlarge). Il s'agit de la version de cluster minimale requise pour migrer vers rg.large et rg.12xlarge.
- Ajout de la possibilité pour les superutilisateurs de supprimer les fournisseurs d'identité IAM Identity Center désactivés de type Lakehouse
- Des requêtes de maintenance interne étiquetées « JIT ANALYZE » sont apparues dans les tables système STL_QUERY et STL_QUERYTEXT. Ces requêtes sont automatiquement exécutées

par Amazon Redshift pour collecter des statistiques de tables externes et optimiser les plans de requêtes. Aucune action du client n’est requise.

- Nous avons optimisé la validation de l'identité du flux Kinesis afin de réduire les appels d'API DescribeStreamSummary ``. Cela évitera d'atteindre les quotas de l'API Kinesis pour les clients de Redshift qui possèdent de nombreux MV Kinesis Stream. Consultez la section de documentation de Redshift Streaming pour plus de détails.
- Amélioration des performances d'exécution des requêtes en utilisant l'agrégation Top K pour les requêtes comportant les clauses GROUP BY, ORDER BY et LIMIT, réduisant ainsi la quantité de données traitées lors des agrégations.
- Performances améliorées pour les requêtes sur les tables partitionnées du catalogue de données AWS Glue en transférant les prédicats de filtres composés (OR, IN, NOT IN) vers l' GetPartitions API Glue, réduisant ainsi le nombre de partitions récupérées.
- Performances améliorées pour les requêtes utilisant les fonctions Lambda avec User-Defined les fonctions Window.
- Performances améliorées pour des requêtes spécifiques à l'aide des User-Defined fonctions Lambda dans les filtres de jointure des jointures par hachage.
- Stabilité améliorée pour les requêtes qui utilisent des UDF Lambda dans les jointures.
- Autoriser l'utilisation de l'ARN comme nom de AWS Lambda lors de la création de fonctions Lambda. User-Defined
- Performances de requête améliorées en optimisant l'utilisation de la mémoire pour les expressions COALESCE et CASE WHEN.
- Applique un filtrage avancé aux requêtes contenant des sous-plans évalués une seule fois et dont les résultats sont réutilisés en tant que constantes pendant le reste de l'exécution.
- Performances améliorées lors de la première exécution de requêtes à l'aide de ST_Transform
- Compatibilité améliorée avec Apache Iceberg en acceptant les fichiers de suppression positionnelle contenant des index de ligne dupliqués, qui peuvent être produits par compactage AWS Glue.
- Compatibilité améliorée avec Apache Iceberg en acceptant les chemins s3a ://dans les références de fichiers de suppression.
- Gestion améliorée des erreurs de récupération au niveau de la partition Spectrum lors du traitement de tables mal configurées
- Stabilité améliorée de la procédure stockée qui invoque des UDF SQL imbriqués dans les bases de données via USE

- Messages d'erreur améliorés pour les opérations non prises en charge sur les procédures stockées, telles que leur ajout ou leur suppression dans des partages de données.
- Correction d'un bogue qui empêchait la détection des informations VPC du client lorsque l'EVR était utilisé. Ces informations ne sont nécessaires que pour l'entraînement des modèles Redshift ML locaux et n'ont aucune incidence sur les autres fonctionnalités de Redshift. Cela n'a pas empêché l'utilisation des modèles Redshift ML entraînés existants.
- Correction d'un problème à cause duquel des ID de requête dupliqués pouvaient apparaître dans les tables système après une pause du cluster et reprendre lorsque le compteur d'ID de requête interne était proche de sa valeur maximale.
- Correction d'un problème à cause duquel les requêtes sur les tables système STL pouvaient renvoyer des résultats incomplets après un Multi-AZ basculement en raison d'une incohérence de la mise en cache interne
- Correction d'un problème en raison duquel le champ « est AutoIncremented » dans les descriptions de lignes étendues pouvait renvoyer des valeurs incorrectes pour les colonnes IDENTITY
- Correction d'un problème en raison duquel les fonctions ARRAY_CONTAINS et ARRAY_POSITION ne renvoyaient pas la valeur NULL comme prévu lorsqu'elles recevaient des entrées NULL.
- Correction d'un problème rare en raison duquel les requêtes comportant plusieurs prédicats de filtre combinés lors de scans vectorisés pouvaient échouer de façon inattendue.
- Correction d'un problème rare à cause duquel des opérations COPY simultanées pouvaient provoquer une instabilité du cluster lors du chargement des données
- Correction d'un problème selon lequel les opérations de maintenance automatiques telles que l'aspiration et l'analyse pouvaient provoquer une instabilité du cluster lors de l'arrêt du processus
- Correction d'un problème en raison duquel les requêtes pouvaient échouer une fois que l'accélération des requêtes courtes de gestion de la charge de travail (WLM) était désactivée puis réactivée de manière dynamique
- Correction d'un problème à cause duquel les requêtes relatives au voyage dans le temps étaient effectuées sur des tables sans ETL en mode historique.
- Correction d'un problème en raison duquel les intégrations sans ETL pouvaient ne plus répondre lors de l'arrêt simultané du client
- Correction d'un problème à cause duquel des tables sans ETL partageant une partition source pouvaient déclencher une resynchronisation inutile
- Correction d'un problème en raison duquel les mises à jour de l'état de la table d'intégration zéro ETL pouvaient échouer lorsque le champ de motif interne dépassait la longueur autorisée

- Correction d'un problème en raison duquel les intégrations zéro-ETL rencontraient des erreurs lors des modifications de colonnes sur une table partitionnée Aurora PostgreSQL

Correctif 201 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.331388 — Version du cluster provisionné par TRAILING Track pour Amazon Redshift et version pour groupe de travail Amazon Redshift Serverless — Publiée le 16 juin 2026
- 1.0.331388 — CURRENT Track, version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiée le 15 juin 2026
- 1.0.326225 — Version actuelle du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 8 juin 2026
- 1.0.319797 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 3 juin 2026
- 1.0.313685 — Version actuelle du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 27 mai 2026
- 1.0.300094 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 12 mai 2026
- 1.0.298697 — Version actuelle du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 7 mai 2026
- 1.0.292316 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 4 mai 2026
- 1.0.280974 — Version actuelle du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 22 avril 2026

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajout du support pour les types de nœuds RG (multi-nœuds rg.xlarge et rg.4xlarge). Il s'agit de la version de cluster minimale requise pour migrer vers rg.xlarge et rg.4xlarge.
- Ajout du support pour les tables ALTER sur Iceberg.
- Ajout du support pour écrire sur les tables Iceberg montées en dessous AwsDataCatalog.
- Ajout de la prise en charge de la commande SHOW GRANTS lors de la connexion à une base de données à l'aide de la commande USE.

- Ajout de la prise en charge des commandes SHOW GRANTS et SHOW COLUMN GRANTS pour les identités dotées d'autorisations fédérées.
- Ajout de la prise en charge de l'actualisation automatique des vues matérialisées en tant que charge de travail utilisateur avec capacité de pointe sur Amazon Redshift Serverless.
- Autorisez AutoWLM à affecter plus de mémoire de cluster aux requêtes écrites dans des tables larges.
- Amazon Redshift a amélioré les performances des requêtes de la vue système SVV_ATTACHED_MASKING_POLICY, en réduisant le temps d'exécution sur les instances disposant d'un grand nombre d'autorisations et en joignant des politiques de masquage dynamique des données.
- Mise à niveau de la bibliothèque librdkafka vers la version 2.13.x à partir de la version 2.8.x afin de fournir les dernières corrections de bogues et améliorations de performances.
- Performances améliorées pour les requêtes utilisant les User-Defined fonctions Lambda dans la clause HAVING des agrégats.
- Performances améliorées pour les requêtes utilisant des fonctions Lambda avec User-Defined des fonctions de fenêtre.
- Stabilité améliorée pour les User-Defined fonctions Lambda sans arguments.
- Amélioration des performances d'exécution des requêtes de table Datalake lors de l'utilisation des clauses ORDER BY et LIMIT en éliminant les analyses de données inutiles.
- Messages d'erreur améliorés pour les intégrations sans ETL afin de fournir des informations plus claires sur les contraintes non prises en charge, les instructions DDL non prises en charge, la perte de précision des dates, les incohérences de longueur de caractères sur plusieurs octets et les tables sources ignorées.
- Résilience d'intégration zéro ETL améliorée en gérant de manière élégante les échecs d'acquisition d'informations d'identification lors des contrôles de l'état de réplication.
- Performances améliorées des intégrations sans ETL lors de l'exécution de tâches de réplication simultanées.
- Résultats de requête de voyage dans le temps améliorés pour les tables zéro ETL avec des lignes fréquemment mises à jour afin de garantir que chaque version de ligne historique reflète son horodatage de suppression individuel.
- Correction de certains cas extrêmes où le cluster principal n'était pas correctement redimensionné lors de la AI-driven mise à l'échelle.

- Correction d'un problème en raison duquel Amazon CloudWatch Metrics pouvait signaler le nombre de requêtes ayant échoué en double lorsque les requêtes étaient expulsées et réessayées par le service de gestion de la charge de travail (WLM).
- Correction d'un problème à cause duquel COPY et Redshift Table Copy pouvaient produire une incompatibilité entre les styles de distribution.
- Correction d'un problème lié au calcul incorrect des lignes de fin de tri des partitions qui pouvait affecter les résultats d'analyse à plage restreinte.
- Correction d'un problème en raison duquel les opérations d'aspiration automatique pouvaient échouer en cas de chute simultanée d'une table.
- Correction d'un problème en raison duquel VACUUM pouvait utiliser une version de table périmée lors de l'acquisition de la relation, ce qui pouvait entraîner des erreurs.
- Assurez-vous que la carte des transactions sous vide est correctement nettoyée sur les clusters éclatés.
- Correction d'un problème en raison duquel les requêtes sur des tables répliquées sans ETL pouvaient échouer en cas d'accès via le partage de données.
- Correction d'un problème lié à la réplication des données d'intégration sans ETL qui pouvait entraîner le redémarrage du cluster.
- Correction d'un problème en raison duquel les intégrations sans ETL avec le mode historique DynamoDB pouvaient échouer lors des opérations de mise à jour et de fusion.
- Correction d'un problème en raison duquel les tables d'intégration Zero-ETL pouvaient afficher un nombre de lignes incorrect dans la console Amazon Redshift.
- Correction d'un problème qui empêchait les groupes de travail Amazon Redshift Serverless de s'interrompre pendant les opérations d'intégration sans ETL.
- Correction d'un problème à cause duquel les fichiers Avro vides provoquaient l'échec de l'ingestion de COPY. Les fichiers Avro vides sont désormais ignorés et l'ingestion se poursuit sans erreur.
- Correction d'un problème de somme de contrôle d'en-tête de bloc périmé lors de la rediffusion d'Epsilon Tree lors de l'utilisation d'un superbloc indépendant de la position.

Patch 200 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.314426 — TRAILING Track, version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiées le 27 mai 2026

- 1.0.293472 — TRAILING Track, version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiées le 7 mai 2026
- 1.0.293472 — CURRENT suit la version du cluster provisionné par Amazon Redshift et la version du groupe de travail Amazon Redshift Serverless — Publiée le 30 avril 2026
- 1.0.266483 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 9 avril 2026
- 1.0.257586 — Version actuelle du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 27 mars 2026

Nouvelles fonctionnalités et améliorations de ce correctif

- Correction d'un problème en raison duquel les opérations INSERT pouvaient échouer sur les tables à l'aide de clés de tri multidimensionnelles de mise en page des données.
- Amélioration des recommandations d'Amazon Redshift Advisor concernant les clés de tri MDDL (Multidimensional Data Layout) pour les tables qui bénéficieraient d'un tri basé sur la charge de travail.
- Mise à l' AI-driven échelle et optimisations Redshift Serverless améliorées avec des signaux d'utilisation du disque améliorés, permettant des décisions de dimensionnement plus précises et plus réactives.
- Mise à l' AI-driven échelle et optimisations Redshift Serverless améliorées pour déterminer intelligemment une capacité initiale lorsque vous migrez un instantané de cluster provisionné vers un espace de noms sans serveur.
- Correction d'un problème en raison duquel les requêtes de partage de données utilisant la propagation d'identité IAM Identity Center pouvaient échouer lorsque le jeton d'identité mis en cache expirait chez le consommateur.
- Correction d'un problème en raison duquel la synchronisation des groupes IAM Identity Center pouvait entraîner l'échec des opérations de maintenance en arrière-plan ultérieures.
- Correction d'un problème selon lequel la mise à jour de la configuration d'un fournisseur d'identité IAM Identity Center avec un ARN d'application différent pouvait entraîner le redémarrage du cluster.
- Correction d'un problème en raison duquel les requêtes de partage de données avec propagation d'identité IAM Identity Center pouvaient échouer dans certaines AWS régions.
- Fiabilité améliorée de l'intégration d'IAM Identity Center en garantissant que les modifications de configuration du fournisseur d'identité sont systématiquement propagées.

- Plans de requête optimisés pour certaines sous-requêtes NOT EXISTS corrélées en les décorrélant en anti-jointures.
- Correction d'un problème selon lequel DROP TABLE IF EXISTS sur les tables Apache Iceberg pouvait signaler à tort un échec de requête au lieu de signaler un succès lorsque la table cible n'existait pas.
- Ajout d'un message d'erreur approprié lorsque les utilisateurs tentent d'exécuter ANALYZE sur les tables du catalogue.
- Spectrum COPY est désormais disponible pour tous, ce qui élimine la dépendance à l'égard des tables temporaires pour les opérations Spectrum-based COPY.
- Fiabilité Auto COPY améliorée en limitant les lectures des files d'attente de notifications S3 lorsque les tâches de persistance durables ne peuvent pas suivre le rythme, réduisant ainsi le besoin d'opérations de listage S3 pour réconcilier l'état COPY JOB.
- La mise à l'échelle de la concurrence est désormais généralement disponible pour les opérations de lecture et d'écriture sur des tables sans ETL.
- Correction d'un problème de concurrence lié à la réplication CDC sans ETL qui pouvait provoquer le redémarrage du cluster lorsque des validations simultanées sur le disque interféraient avec le suivi de l'état des tables non validées.
- Fiabilité d'ingestion zéro ETL améliorée par le CDC en utilisant la position d'ingestion la plus récente à la fois dans la table et dans l'état du client pour filtrer les données déjà appliquées.
- Correction d'un problème de fiabilité des données lié à la resynchronisation des tables Zero-ETL, en raison duquel les anciens points de contrôle déjà appliqués pouvaient être réingérés après une défaillance des tables, en suivant correctement les limites inférieures des points de contrôle et l'état de resynchronisation tout au long du cycle de vie de resynchronisation.
- Messages d'erreur zéro ETL améliorés avec des raisons d'échec plus claires, y compris des informations sur le dépassement de la longueur des colonnes et les erreurs de UTF-8 caractères non valides.
- Amélioration de la vue système SYS_LUDF_DETAIL pour indiquer la durée en microsecondes au lieu de millisecondes pour une meilleure observabilité.
- Correction d'un problème en raison duquel la création de tâches Auto COPY était incorrectement autorisée dans les bases de données Zero-ETL.
- Amélioration des performances des requêtes sur les tables protégées par la sécurité au niveau des lignes (RLS) en classant les fonctions intégrées supplémentaires en activant le transfert des prédicats pour les modèles de requêtes courants dont les performances étaient auparavant dégradées. RLS-safe

- Ajout de la prise en charge des opérations DELETE, UPDATE et MERGE sur les tables Apache Iceberg.
- Ajout de la prise en charge des superblocs indépendants de la position, permettant des temps de redémarrage prévisibles du cluster quel que soit le volume de données.
- Activation GUID-based du cache disque, supprimant la dépendance du cache disque sur la position des superblocs et permettant des temps de redémarrage du cluster prévisibles quel que soit le volume de données.
- Optimisation améliorée de la distribution automatique des tables : les tables dotées d'une seule clé primaire peuvent désormais être converties automatiquement de la distribution ALL à la distribution KEY, ce qui améliore les performances des requêtes et réduit les frais de stockage.
- Correction d'un problème en raison duquel les opérations VACUUM pouvaient échouer ou produire des résultats incorrects en raison d'un conflit lorsque les opérations VACUUM et DML simultanées accédaient au même objet de stockage.
- Correction d'un problème en raison duquel VACUUM FULL pouvait échouer sur certaines tables en raison d'un accès mémoire hors limites lors du traitement de chaînes de partitions spéciales.
- Correction d'un problème en raison duquel les opérations ALTER TABLE OWNER pouvaient autoriser à tort le transfert de la propriété de l'objet à l'utilisateur bootstrap interne.
- Correction d'un problème de course dans lequel les opérations VACUUM simultanées et la réutilisation de tables intermédiaires pouvaient provoquer une instabilité du cluster.
- Correction d'un problème en raison duquel VACUUM FULL ou VACUUM SORT sur de grandes tables pouvaient échouer en raison d'une erreur interne lorsque le nombre de partitions traitées dépassait une limite interne.
- Correction d'un problème en raison duquel la collecte des statistiques de partition en arrière-plan pouvait échouer lorsqu'une table était supprimée alors que les statistiques étaient agrégées à partir de clusters distants.
- Amélioration des performances des opérations VACUUM SORT en évitant les actualisations inutiles des données et en réduisant le temps et les ressources nécessaires pour effectuer le vide sur des tables triées.
- Correction d'un problème selon lequel un accès incorrect aux données des partitions internes pendant les opérations de mise sous vide pouvait provoquer des erreurs inattendues ou une instabilité du cluster.
- Correction d'un problème en raison duquel les opérations ALTER TABLE pouvaient incorrectement transférer la propriété de la table à un utilisateur non privilégié. Les changements de propriétaire

pendant les opérations ALTER sont désormais correctement limités aux seuls utilisateurs autorisés.

- Correction d'un problème rare selon lequel une vérification interne des limites lors d'opérations de mise sous vide pouvait entraîner des échecs de requête inutiles sur des tables contenant un grand nombre de partitions.
- Correction d'un problème en raison duquel la collecte de statistiques d'arrière-plan pouvait échouer ou générer des erreurs en cas de suppression de tables, améliorant ainsi la stabilité du cluster.
- Correction d'un problème en raison duquel les opérations d'aspiration pouvaient utiliser des métadonnées de table périmées, ce qui risquait de provoquer un comportement incorrect lors du vide sur des tables avec des modifications de schéma simultanées.
- Publication d'une nouvelle amélioration de la compilation de requêtes qui améliore les performances pour les nouvelles requêtes (premières exécutions de requêtes) dans le correctif P198 d'Amazon Redshift sur le circuit de maintenance ACTUEL. Désormais, cette fonctionnalité est également activée sur toutes les versions, à commencer par le patch P200 d'Amazon Redshift.

Correctif 199 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.266409 — Version du cluster provisionné par TRAILING Track pour Amazon Redshift et version pour groupe de travail Amazon Redshift Serverless — Publiée le 20 avril 2026
- 1.0.252420 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 25 mars 2026
- 1.0.232773 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 5 mars 2026

Nouvelles fonctionnalités et améliorations de ce correctif

- Publication d'une nouvelle amélioration de la compilation de requêtes qui améliore les performances pour les nouvelles requêtes (premières exécutions de requêtes) dans le cadre du programme Redshift CURRENT Maintenance Track. La piste TRAILING suivra dans une prochaine mise à jour.
- La prise en charge des subventions au niveau des colonnes accordées par un consommateur à l'aide des autorisations fédérées Redshift a été activée pour un nouveau bénéficiaire ou un nouveau producteur.

- Les autorisations fédérées Amazon Redshift permettent d'interroger des tables externes via des Late Binding Views (LBV).
- ALTER EXTERNAL SCHEMA peut désormais être utilisé avec le type de schéma externe KINESIS pour modifier les paramètres IAM_ROLE et REGION d'un schéma externe existant.
- Ajout du support de restauration pour les NO-BACKUP tables sur les entrepôts de données Redshift RA3 et Serverless. Étant donné que ces types d'instances ne prennent pas en charge NO-BACKUP cette fonctionnalité, les tables marquées comme telles NO-BACKUP sont toujours incluses dans les instantanés et sont désormais correctement restaurées en tant que tables permanentes.
- Amazon Redshift prend désormais en charge l'écriture sur des tables externes lorsque vous êtes connecté à l'aide de rôles IAM ou d'utilisateurs IAM. Auparavant, seules les opérations de lecture sur des tables externes étaient prises en charge avec l'authentification basée sur les rôles IAM. Avec cette mise à jour, Redshift utilise correctement vos informations d'identification de session IAM lors de l'écriture de données sur Amazon S3 pour des tables externes, ce qui permet un accès complet en lecture et en écriture.
- Pour actualiser automatiquement les MV des streams de Kafka, nous utilisons désormais une heuristique plus efficace pour déterminer s'il y a de nouveaux enregistrements à ingérer. Cela réduira la quantité de données transférées par les courtiers Kafka pour cette vérification et réduira le temps de latence lors du démarrage de l'actualisation MV suivante.
- Opérations de sauvegarde et de restauration améliorées pour utiliser le chiffrement FIPS-compliant SHA384, en remplacement du hachage MD5 existant
- Performances améliorées pour les requêtes combinant des User-Defined fonctions Lambda et des instructions UNNEST
- Performances améliorées pour les requêtes utilisant les User-Defined fonctions Lambda sur les tables et les vues système
- Performances d'exécution des requêtes améliorées lors de l'utilisation des clauses ORDER BY et LIMIT en éliminant les analyses de données inutiles
- Mise à l' AI-driven échelle et optimisations Redshift Serverless améliorées avec une gamme étendue de RPU prises en charge, prenant désormais en charge un minimum de 8 RPU
- Les requêtes Auto REFRESH pour les vues matérialisées (VM) Amazon Redshift sont désormais traitées comme des requêtes utilisateur plutôt que comme des processus autonomes en arrière-plan. Les requêtes Auto REFRESH sont désormais exécutées avec la même priorité que les autres requêtes utilisateur et ne sont plus différées par des processus autonomes en arrière-plan. La fonctionnalité de changement de comportement MV Auto REFRESH n'est activée que pour les

clusters provisionnés Amazon Redshift sur la version ACTUELLE du correctif P198 et versions ultérieures. Il est actuellement désactivé sur Serverless.

- Planification améliorée des tâches automatiques afin de mieux hiérarchiser les tâches critiques pour l'utilisateur telles que l'ingestion du streaming, la copie automatique (COPY JOB) et l'actualisation automatique des vues matérialisées.
- Correction d'un problème où pg_last_query_id () renvoyait incorrectement l'ID de requête réécrit au lieu de l'ID de requête utilisateur pour les clusters Multi-AZ
- Résout un problème en raison duquel SHOW GRANTS ne parvenait pas à traiter les références d'objets en une seule partie.
- Correction d'un problème en raison duquel DROP TABLE entrait en conflit avec l'outil automatique d'horodatage de l'opérateur de reconstruction du catalogue en raison de mises à jour simultanées sur pg_class_extended, en omettant la suppression pendant DROP TABLE et en permettant au programme de travail d'horodatage de faire le ménage lors de sa prochaine exécution.
- Correction d'un problème d'analyse du filtre de canal zéro ETL lorsque les noms de base de données, de schéma ou de table contenaient des mots clés include/exclude
- Correction d'un problème de course qui pouvait survenir lorsque les opérations d'aspiration s'exécutaient simultanément avec des opérations de table sans ETL
- Correction d'un problème en raison duquel les intégrations Zero-ETL tentaient incorrectement des opérations de resynchronisation au lieu de passer à un état d'erreur lorsque le contexte de chiffrement KMS changeait
- Correction d'une condition de course dans les intégrations sans ETL qui pouvait survenir lors du redémarrage du cluster alors que la réplication des données était active
- Correction d'un problème en raison duquel la commande SHOW TABLES renvoyait une erreur lorsque le propriétaire de la table avait été supprimé

Correctif 198 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.239402 — Version du cluster provisionné par TRAILING Track pour Amazon Redshift et version pour groupe de travail Amazon Redshift Serverless — Publiée le 18 mars 2026
- 1.0.227967 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 25 février 2026

- 1.0.224252 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 19 février 2026
- 1.0.219674 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 11 février 2026
- 1.0.212832 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 10 février 2026
- 1.0.204436 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 4 février 2026

Nouvelles fonctionnalités et améliorations de ce correctif

- Publication d'une nouvelle amélioration de la compilation de requêtes qui améliore les performances pour les nouvelles requêtes (premières exécutions de requêtes) dans le cadre du programme Redshift CURRENT Maintenance Track. La piste TRAILING suivra dans une prochaine mise à jour.
- Améliore les requêtes INTERSECT et EXCEPT en appliquant des règles de classement appropriées lors de la comparaison de colonnes à des valeurs constantes.
- Permet l'actualisation automatique des vues matérialisées créées manuellement pour les exécuter sur des clusters de dimensionnement simultanés.
- Améliore les performances de connexion en permettant des connexions directes entre les clusters principaux et en adaptant les clusters en simultané, en réduisant le temps de latence et en éliminant les limites de débit de connexion.
- Améliore la classification des erreurs pour les intégrations sans ETL, ce qui facilite l'identification des causes profondes et le débogage des problèmes.
- Supprime les messages d'erreur de SYS_QUERY_HISTORY pour les requêtes exécutées avec succès, fournissant ainsi des enregistrements d'historique des requêtes plus propres.
- Améliore la précision de l'enregistrement du temps de compilation pour les requêtes en rafale dans SYS_QUERY_HISTORY, fournissant ainsi de meilleures informations sur les performances.
- Prend en charge les fonctions de tableau : ARRAY_CONTAINS, ARRAY_POSITION, ARRAYS_OVERLAP, ARRAY_INTERSECTION, ARRAY_SORT, ARRAY_UNION, ARRAY_DISTINCT, ARRAY_EXCEPT et ARRAY_POSITIONS.
- Ajoute la prise en charge de la fonction GET_NUMBER_ATTRIBUTES qui renvoie le nombre d'attributs d'un objet SUPER.

- Active le délai d'inactivité en cas d'échec des transactions afin d'améliorer la gestion des ressources.
- Ajoute la prise en charge du type d'objet TEMPLATE qui permet de définir des paramètres de mise en forme réutilisables, éliminant ainsi le besoin de les spécifier manuellement pour chaque opération.
- Améliore les performances des requêtes qui invoquent des User-Defined fonctions Lambda (LUDF) sur des expressions de table communes (CTE).
- Améliore les performances des requêtes qui invoquent des User-Defined fonctions Lambda (LUDF) dans la clause THEN des expressions CASE.
- La création de nouvelles User-Defined fonctions Python est obsolète. Les UDF Python existants seront pris en charge jusqu'au 30 juin 2026. Migrez vers Lambda User-Defined Functions (LUDFs) pour bénéficier d'un support continu.
- Améliore l'observabilité des fonctions User-Defined Lambda (LUDFs) grâce à une nouvelle table système, SYS_LUDF_DETAIL. Ce tableau enregistre les informations et les mesures relatives aux LUDF utilisés dans les requêtes.
- Les requêtes Auto REFRESH pour les vues matérialisées (VM) Amazon Redshift sont désormais traitées comme des requêtes utilisateur plutôt que comme des processus autonomes en arrière-plan. Les requêtes Auto REFRESH sont désormais exécutées avec la même priorité que les autres requêtes utilisateur et ne sont plus différées par des processus autonomes en arrière-plan. La fonctionnalité de changement de comportement MV Auto REFRESH n'est activée que pour les clusters provisionnés Amazon Redshift sur la version ACTUELLE du correctif P198 et versions ultérieures. Il est actuellement désactivé sur Serverless.

Correctif 197 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.237947 — Version du cluster provisionné par TRAILING Track pour Amazon Redshift et version pour groupe de travail Amazon Redshift Serverless — Publiée le 10 mars 2026
- 1.0.198462 — TRAILING Track, version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiées le 28 janvier 2026
- 1.0.198462 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 21 janvier 2026
- 1.0.194394 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 14 janvier 2026

- 1.0.187928 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 9 janvier 2026
- 1.0.179517 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 16 décembre 2025
- 1.0.176066 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 9 décembre 2025
- 1.0.166219 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 21 novembre 2025

Nouvelles fonctionnalités et améliorations de ce correctif

- Autonomics globale pour les clusters du maillage, Autonomics prend désormais en compte la charge de travail de l'ensemble du maillage pour optimiser Vacuum, Analyze et ATO.
- Créez et actualisez des vues matérialisées à partir de plusieurs entrepôts de données Amazon Redshift.
- Ajout du support pour stocker des chaînes littérales allant jusqu'à 16 000 000 octets dans les types de données SUPER
- Ajout de la fonction GET_NUMBER_ATTRIBUTES (super_object) qui renvoie le nombre total d'attributs contenus dans un objet SUPER.
- Les restrictions de compatibilité des correctifs de version sont appliquées aux opérations de restauration de tables. Lorsque vous tentez de restaurer une table, la sauvegarde ne peut être utilisée que sur des clusters exécutant la même version de correctif que lors de la création de la sauvegarde, une version de correctif inférieure à la sauvegarde ou une version de correctif supérieure à la sauvegarde.
- Amélioration de l'opérateur LIKE pour gérer correctement les espaces blancs de fin dans les modèles lors de l'utilisation du type de données CHAR.
- Introduction de 4 nouvelles fonctions H3 spatiales fonctionnant sur des hiérarchies de cellules : H3_Resolution, H3_, H3_ et H3_ToParent. ToChildren IsValid
- Active les autorisations fédérées Amazon Redshift qui simplifie la gestion des autorisations dans plusieurs entrepôts de données Redshift en vous permettant de définir les autorisations de données une seule fois et de les appliquer automatiquement dans tous les entrepôts de votre entreprise. Compte AWS

- Permet des autorisations au niveau de l'objet, un contrôle d'accès précis au niveau des colonnes, des autorisations délimitées et des autorisations au niveau de la base de données sur les objets du catalogue des autorisations fédérées Amazon Redshift.
- Active les opérations de politique RLS CREATE, ALTER, ATTACH, DETACH et DROP sur le catalogue d'autorisations fédérées Amazon Redshift.
- Permet d'activer ou de désactiver la sécurité au niveau des lignes pour les relations dans Amazon Redshift Federated Permissions Catalog.
- Activez les opérations de politique de masquage CREATE, ALTER, ATTACH, DETACH et DROP sur les objets du catalogue d'autorisations fédérées Amazon Redshift.
- Permet à SHOW POLICIES d'afficher les politiques RLS et de masquage sur une base de données connectée, ainsi que les pièces jointes relatives aux relations dans les objets du catalogue Amazon Redshift Federated Permissions.
- Permet aux utilisateurs de base de données d'assumer un rôle IAM pour effectuer des requêtes sur des objets du catalogue Amazon Redshift Federated Permissions Catalog.
- Commande SHOW GRANTS améliorée pour prendre en charge la visibilité des subventions entre les bases de données au sein d'un même cluster Redshift.
- Ajout de la prise en charge de la commande SHOW COLUMN GRANTS pour simplifier la découverte des contrôles d'accès au niveau des colonnes.
- Ajout de la prise en charge de la commande SHOW PROCEDURES afin de simplifier la découverte des métadonnées des procédures stockées.
- Ajout de la prise en charge de la commande SHOW FUNCTIONS pour simplifier la découverte des métadonnées des fonctions définies par l'utilisateur.
- La commande SHOW PARAMETERS a été introduite pour afficher les métadonnées des paramètres des fonctions et des procédures stockées.
- Introduction de la commande SHOW CONSTRAINTS pour afficher les métadonnées de contrainte pour les fonctions et les procédures stockées.
- Ajout de la prise en charge des opérations CREATE/CREATE OR REPLACE/DROP VIEW sur le catalogue d'autorisations fédérées Amazon Redshift et sur les bases de données croisées au sein du même cluster Redshift.
- Amélioration de la gestion du classement des chaînes constantes dans certaines requêtes INTERSECT ou EXCEPT.
- SHOW TABLES amélioré pour afficher un message d'avertissement au lieu d'échouer lorsque les informations d'identification FAS sont manquantes pour AWS Glue Data Catalog l'accès.

- Commande SHOW COLUMNS améliorée avec des colonnes de métadonnées supplémentaires pour les clés de tri, le style de distribution, le codage et les informations de classement.
- Ajout de la colonne grantor_name à la sortie SHOW GRANTS et inclusion standardisée de database_name dans tous les ensembles de résultats SHOW GRANTS.
- Commande SHOW TABLES améliorée avec des colonnes supplémentaires : table_owner, last_altered_time, last_modified_time, dist_style et table_sub_type.
- Support de l'authentification du centre d'identité : Amazon Redshift prend désormais en charge l'authentification IAM Identity Center via les nouvelles `GetIdentityCenterAuthToken` opérations d'API. Cette fonctionnalité permet un accès fédéré aux clusters Amazon Redshift et aux groupes de travail sans serveur en utilisant les identités Identity Center existantes. Les principaux avantages incluent l'accès par authentification unique à l'aide des informations d'identification Identity Center, une sécurité renforcée grâce à des jetons d'authentification cryptés, une journalisation complète des audits pour garantir la conformité et une intégration parfaite avec la configuration existante d'Identity Center. Les opérations d'API génèrent des jetons d'authentification limités à des identifiants de cluster ou à des noms de groupes de travail spécifiques. Les exigences incluent des informations d'identification améliorées avec des informations d'identité intégrées à Identity Center et des autorisations IAM appropriées pour l'accès aux API.

Patch 196 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.179872 — TRAILING Track, version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiées le 8 janvier 2026
- 1.0.163480 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 20 novembre 2025
- 1.0.160807 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 14 novembre 2025
- 1.0.155905 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 11 novembre 2025

Nouvelles fonctionnalités et améliorations de ce correctif

- Optimisation des plans pour les sous-requêtes IN et EXISTS corrélées en les décorrélant en semi-jointures.
- Extension de la commande SHOW TABLE pour inclure les informations de classement pour chaque colonne.

Correctif 195 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.172541 — TRAILING Track, version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiées le 8 décembre 2025
- 1.0.162991 — TRAILING Track, version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiées le 20 novembre 2025
- 1.0.151179 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 4 novembre 2025
- 1.0.148180 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 31 octobre 2025
- 1.0.142459 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 24 octobre 2025

Nouvelles fonctionnalités et améliorations de ce correctif

- Permet d'écrire dans des tables Iceberg à l'aide des commandes CREATE TABLE, CREATE TABLE AS SELECT, INSERT INTO et SQL.
- Ajoute la prise en charge du type de données SUPER dans les bases de données avec un classement insensible à la casse.
- Met à jour la version de la base de données de fuseaux horaires de l’IANA vers 2025b.
- Ajoute la prise en charge de la fonction TZDB_VERSION. Cette fonction affiche la version actuellement utilisée de la base de données de fuseaux horaires de l’IANA.
- Amazon Redshift applique désormais les restrictions de compatibilité des correctifs. Les sauvegardes créées sur des versions de correctif qui ont plus d’une version de correctif en avance sur le cluster actuel ne sont plus autorisées à effectuer des opérations de restauration de tables.

- Étend les fonctionnalités UNNEST pour prendre en charge les expressions JOIN. Auparavant, UNNEST était limité aux références à une seule table.
- Ajoute la prise en charge de la fonction JIT (Just In Time) ANALYZE. JIT ANALYZE collecte automatiquement, intelligemment et efficacement l'ensemble minimal de statistiques dont l'optimiseur de requêtes d'Amazon Redshift a besoin pour générer des plans d'exécution des requêtes efficaces, permettant aux clients d'obtenir le meilleur rapport qualité-prix pour les requêtes et les charges de travail prêtes à l'emploi (OOB) d'Apache Iceberg.

Correctif 194 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.148169 — TRAILING Track, version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiées le 5 novembre 2025
- 1.0.138443 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 18 octobre 2025
- 1.0.129791 — CURRENT Track : version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 8 octobre 2025

Nouvelles fonctionnalités et améliorations de ce correctif

- Amazon Redshift n’échouera plus une requête qui accède à une relation gouvernée par AWS Lake Formation où le champ `AuthorizedColumns` contient une barre oblique inverse.
- Ajout de la prise en charge de l’option NULL AS dans la commande COPY pour les colonnes SUPER, vous permettant de spécifier une chaîne personnalisée pour représenter les valeurs NULL.
- Ajout de la prise en charge des parties de date ISOWEEK et ISOYEAR dans les fonctions EXTRACT et DATE_PART lorsqu’elles sont utilisées avec des dates et des horodatages.
- Correction de la navigation PartiQL sur les variables groupées afin de garantir une analyse et une évaluation correctes de l’accès aux champs imbriqués dans les requêtes GROUP BY.
- Ajout de la prise en charge de l’affichage des contraintes de clé primaire et de clé étrangère à l’aide de la commande SHOW CONSTRAINTS.
- Ajout de la prise en charge des vues matérialisées locales créées à partir de vues matérialisées de partage de données.

- Améliore les performances des requêtes qui extraient des données de différentes tables et invoquent des fonctions Lambda définies par l'utilisateur dans des conditions de jointure.
- Ajout de la prise en charge des machines virtuelles sur les machines virtuelles de partage de données
- La commande DROP DATABASE utilise désormais un outil de travail en arrière-plan pour supprimer les répertoires du catalogue des nœuds principaux après la validation. L'utilisation d'une application de travail permet d'éviter les rares bogues liés au nettoyage du répertoire du catalogue.

Correctif 193 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.136890 — TRAILING Track, version du cluster provisionné Amazon Redshift et version du groupe de travail Amazon Redshift Serverless, publiées le 17 octobre 2025
- 1.0.127211 — CURRENT Track : version du cluster provisionné par Amazon Redshift et version du groupe de travail Amazon Redshift Serverless — Publiée le 30 septembre 2025

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajout de la prise en charge de la création de tables à l'aide de CREATE TABLE LIKE pour cloner une table parent à partir de bases de données distantes (à la fois au sein du même cluster et entre différents clusters).
- Ajout d'une GeomFromGeoJSON surcharge ST_ qui crée une géométrie à partir du type de données SUPER au format GeoJSON, avec prise en charge des géométries allant jusqu'à 1 Mo.
- Modification de l'option de secours par défaut en cas de mauvaise configuration dans la gestion automatique de la charge de travail (WLM). L'option de secours par défaut est désormais la gestion automatique de la charge de travail au lieu de la gestion manuelle de la charge de travail.
- Mise à jour du calcul du fuseau horaire en adoptant les derniers correctifs de la base de données des fuseaux horaires de l'IANA. Cette modification modifie le fonctionnement des conversions de date et d'heure pour certains fuseaux horaires et certaines périodes. Pour plus d'informations, consultez Amazon Redshift utilise la base de données de fuseaux horaires de l'IANA à jour.
- Ajout de la prise en charge du format de données multidimensionnelles (MDDL). Les clés de tri MDDL trient les données de manière dynamique en fonction des filtres de requête réels, accélérant ainsi les performances des requêtes. Pour plus d'informations, consultez Format de données multidimensionnelles dans le Guide du développeur de base de données Amazon Redshift.

Correctif 192 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.124422 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 22 septembre 2025
- 1.0.122914 : version précédente du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 16 septembre 2025
- 1.0.121035 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 22 août 2025
- 1.0.119650 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 7 août 2025
- 1.0.118447 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 24 juillet 2025

Nouvelles fonctionnalités et améliorations de ce correctif

- Résout un problème lorsque JOIN sur une colonne assemblée insensible à la casse et une colonne de chaîne constante sélectionne une fonction de hachage non correspondante.

Correctif 191 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.117891 : version précédente du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 29 juillet 2025
- 1.0.117891 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 22 juillet 2025
- 1.0.117458 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 15 juillet 2025
- 1.0.116415 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 26 juin 2025
- 1.0.116263 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 25 juin 2025

- 1.0.115865 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 18 juin 2025

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajoute la prise en charge de l'opération UNNEST dans la clause FROM de l'instruction SELECT, permettant aux clients de convertir les éléments du tableau en lignes individuelles.
- Améliore la gestion des erreurs pour la syntaxe de désimbrication PartiQL lors de l'utilisation du type de données SUPER dans les expressions de table communes (CTE) et les CTE récursives, en particulier lors de la résolution d'alias de table portant des noms identiques.
- Améliore les performances de l'analyse automatique en ajoutant la prise en charge de l'analyse automatique incrémentielle pour les tables volumineuses.
- Amazon Redshift prend désormais en charge l'actualisation en cascade des vues matérialisées (VM) imbriquées.
- Amazon Redshift prend désormais en charge l'actualisation automatique des vues matérialisées (VM) définies sur les tables Apache Iceberg.
- Ajoute la prise en charge des intégrations zéro ETL Amazon RDS pour Oracle à Amazon Redshift.
- Ajoute la prise en charge des intégrations zéro ETL Amazon RDS pour PostgreSQL à Amazon Redshift.

Patch 190 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.115140 : version précédente du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 16 juin 2025
- 1.0.115564 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 14 juin 2025
- 1.0.113436 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 15 mai 2025
- 1.0.112895 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 7 mai 2025

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajoute des modèles améliorés pour le AI-driven dimensionnement et les optimisations d'Amazon Redshift Serverless.
- Prend en charge la copie automatique lors de l’utilisation d’Amazon Redshift avec le routage VPC amélioré activé.
- Prend en charge plusieurs opérations d’optimisation automatique des tables à exécuter simultanément sur différentes tables.
- Corrige un problème rare lié à l’ingestion en streaming, dans lequel les requêtes d’actualisation automatique en file d’attente déclenchent des requêtes UNDO qui sont également mises en file d’attente, ce qui entraîne des conflits de verrouillage.
- Prend en charge les intégrations Oracle Database@AWS sans ETL avec Amazon Redshift.

Correctif 189 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.112790 : version précédente du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 14 mai 2025
- 1.0.112790 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 6 mai 2025
- 1.0.112086 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 29 avril 2025
- 1.0.111040 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 16 avril 2025
- 1.0.109768 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 22 mars 2025
- 1.0.109284 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 13 mars 2025
- 1.0.108971 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 7 mars 2025

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajoute la prise en charge de la mise à l'échelle de la simultanéité pour les requêtes d'écriture utilisant les types de données SUPER, GEOMETRY et GEOGRAPHY.
- Résout un problème qui permettait de définir les colonnes SUPER, GEOMETRY ou GEOGRAPHY en tant que colonnes DISTKEY ou SORTKEY lors de la création d'une table avec CREATE TABLE AS.
- Ajoute la prise en charge de la fonction TRY_CAST.
- Permet d'exécuter plusieurs commandes de suppression simultanément sur différentes tables.

Correctif 188 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.109616 : version précédente du groupe de travail d'Amazon Redshift sans serveur — Publiée le 27 mars 2025
- 1.0.109616 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 24 mars 2025
- 1.0.108470 : version précédente du groupe de travail d'Amazon Redshift sans serveur — Publiée le 13 mars 2025
- 1.0.108470 : version actuelle du groupe de travail d'Amazon Redshift sans serveur — Publiée le 11 mars 2025
- 1.0.108950 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 10 mars 2025
- 1.0.108790 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 9 mars 2025
- 1.0.108470 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 4 mars 2025
- 1.0.107910 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 20 février 2025
- 1.0.107360 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 13 février 2025
- 1.0.106767 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 5 février 2025

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajoute la prise en charge du montage automatique d'un catalogue de tableaux Amazon S3, ce qui vous permet d'exécuter plus facilement des requêtes sur les tables Apache Iceberg gérées dans les tableaux Amazon S3. Consultez Prérequis pour la gestion des espaces de noms Amazon Redshift dans le AWS Glue Data Catalog dans le Guide du développeur AWS Lake Formation pour connaître les autorisations requises.
- Vous pouvez désormais contourner le contrôle de masquage des données et ajouter une table avec une pièce jointe de masquage dynamique des données (DDM) à une unité de partage des données.
- Interdit l'utilisation de références de corrélation qui ignorent un bloc de requête, également appelées « références de corrélation de niveau non hiérarchique ». Pour plus d'informations, consultez Modèles de sous-requêtes corrélées non pris en charge dans le Guide du développeur de base de données Amazon Redshift.
- Ajoute la prise en charge des requêtes de type de données SUPER corrélées avec partage de données et notation en 3 parties.
- Ajoute la prise en charge du mot clé SQL EXCLUDE.
- Ajoute la prise en charge du nouveau mot clé SQL GROUP BY ALL.
- Améliore les performances des files d'attente de gestion de la charge de travail (WLM) configurées avec des rôles, ce qui réduit les conflits de verrouillage.
- Ajoute la prise en charge des vues matérialisées actualisées automatiquement sur les tables sans ETL lorsque le mode historique est activé.
- Ajoute la prise en charge des caractères null incorporés dans les chaînes lors de la réplication sans ETL.
- Améliore les modèles pour une mise à l'échelle et des optimisations basées sur l'IA.
- Ajoute la colonne `username` à la vue `sys_query_history`.

Correctif 187 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.107351 : version précédente du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 13 février 2025
- 1.0.106452 : version précédente du cluster alloué Amazon Redshift — Publiée le 5 février 2025

- 1.0.106980 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 3 février 2025
- 1.0.106452 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 24 janvier 2025
- 1.0.106073 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 21 janvier 2025
- 1.0.105722 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 10 janvier 2025
- 1.0.105373 : version actuelle du cluster alloué Amazon Redshift et version du groupe de travail Amazon Redshift sans serveur — Publiée le 8 janvier 2025
- 1.0.104930 : version du groupe de travail Amazon Redshift sans serveur – Publiée le 20 décembre 2024

Nouvelles fonctionnalités et améliorations de ce correctif

- Introduit deux nouvelles fonctions spatiales H3 (H3_center et H3_boundary).
- Active le cache disque dynamique sur les clusters de mise à l'échelle de la simultanéité.
- Corrige une inefficacité de l'utilisation de la mémoire lors de l'ingestion de tables triées susceptible d'avoir un impact sur les performances.
- Résout un problème selon lequel certaines requêtes comportant une sous-requête dans la clause SELECT, par exemple `SELECT ARRAY_FLATTEN((SELECT FROM ...))`, déclenchaient incorrectement une erreur XCHECK `size >= min_partiql_size` dans des scénarios spécifiques impliquant une seule valeur SUPER.
- Résout un problème où les expressions SUPER non nullables (`json_serialize()`, `json_size()`, `json_typeof()is_object()`, et plusieurs autres) produisaient parfois des résultats erronés lorsqu'elles étaient combinées avec des expressions d'arguments telles que `CASE ... END` ou `COALESCE()`.
- Résout un problème où SELECT dans les vues à liaison tardive provoquait une erreur après avoir activé la sécurité au niveau des lignes sur la vue.
- Résout un problème où le CDC sur une intégration zéro ETL entraînait une consommation UC élevée du nœud principal.
- Permet aux intégrations zéro ETL d'interroger des tables dans tous les états, y compris lors des mises à jour.

- Ajoute la possibilité aux intégrations sans ETL de tronquer les fichiers volumineux texts/strings pour les mapper à la taille maximale des varchars sur Amazon Redshift.
- Permet aux intégrations sans ETL de remplacer les UTF-8 caractères non valides par un caractère spécifique de votre choix.
- Résout un problème relatif à l'« intervalle d'actualisation » pour l'intégration zéro ETL avec Amazon RDS for MySQL.
- Ajoute la prise en charge du type de JSON/JSONB données pour l'intégration Zero-ETL avec Aurora PostgreSQL.
- Résout un problème où les requêtes contenant des expressions avec `IS [NOT] {TRUE|FALSE|UNKNOWN}` pouvaient rencontrer une erreur d'assertion.
- Résout un problème où les fonctions `json_extract_path_text()` et `json_extract_array_element_text()` produisaient une chaîne vide `''` au lieu de `NULL` ou vice versa dans des cas tels que l'accès à un élément ou à un attribut de tableau inexistant, à la valeur JSON `'null'` ou à une chaîne JSON vide.
- Améliore les performances des INSERT/COPY instructions lors de transactions simultanées écrites dans la même table en leur permettant de partager un verrou et de progresser jusqu'à ce qu'elles aient besoin d'écrire des données dans la table.

Correctif 186 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.82096 : version de suivi précédente — Publiée le 10 janvier 2025
- 1.0.82000 — Version sans serveur d'Amazon Redshift — Publiée le 10 janvier 2025
- 1.0.81981 — Version actuelle du titre — Sortie le 10 janvier 2025
- 1.0.81475 : version de suivi précédente — Publiée le 6 janvier 2025
- 1.0.81473 — Version sans serveur d'Amazon Redshift — Publiée le 6 janvier 2025
- 1.0.81462 — Version actuelle du titre — Sortie le 6 janvier 2025
- 1.0.80643 : version de suivi précédente – Publiée le 17 décembre 2024
- 1.0.80583 — Version sans serveur d'Amazon Redshift — Publiée le 17 décembre 2024
- 1.0.80560 — Version actuelle du titre — Sortie le 17 décembre 2024
- 1.0.80498 — Version sans serveur d'Amazon Redshift — Publiée le 13 décembre 2024

- 1.0.80491 — Version actuelle du titre — Sortie le 13 décembre 2024
- 1.0.80036 — Version sans serveur d'Amazon Redshift — Publiée le 6 décembre 2024
- 1.0.80009 — Version actuelle du titre — Sortie le 6 décembre 2024
- 1.0.79372 : version d’Amazon Redshift sans serveur – Publiée le 26 novembre 2024
- 1.0.79237 : version d’Amazon Redshift sans serveur – Publiée le 24 novembre 2024
- 1.0.79229 : version de suivi actuelle – Publiée le 24 novembre 2024
- 1.0.79003 : version d’Amazon Redshift sans serveur – Publiée le 19 novembre 2024
- 1.0.78987 : version de suivi actuelle – Publiée le 19 novembre 2024
- 1.0.78890 : version d’Amazon Redshift sans serveur – Publiée le 18 novembre 2024
- 1.0.78881 : version de suivi actuelle – Publiée le 18 novembre 2024
- 1.0.78646 : version d’Amazon Redshift sans serveur – Publiée le 14 novembre 2024
- 1.0.78641 : version de suivi actuelle – Publiée le 14 novembre 2024
- 1.0.78178 : version d’Amazon Redshift sans serveur – Publiée le 12 novembre 2024
- 1.0.78160 : version de suivi actuelle – Publiée le 12 novembre 2024
- 1.0.77809 : version d’Amazon Redshift sans serveur – Publiée le 31 octobre 2024
- 1.0.77777 : version de suivi actuelle – Publiée le 31 octobre 2024
- 1.0.77292 : version d’Amazon Redshift sans serveur – Publiée le 24 octobre 2024
- 1.0.77272 : version de suivi actuelle – Publiée le 24 octobre 2024
- 1.0.77040 : version d’Amazon Redshift sans serveur – Publiée le 22 octobre 2024
- 1.0.77028 : version de suivi actuelle – Publiée le 22 octobre 2024

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajoute la prise en charge de l’actualisation automatique et incrémentielle des vues matérialisées sur les tables issues d’intégrations zéro ETL à Amazon Aurora MySQL, Amazon Aurora PostgreSQL, Amazon RDS for MySQL et Amazon DynamoDB.
- Améliore la façon dont Amazon Redshift réécrit les requêtes avec des sous-requêtes à une seule ligne corrélées, telles que `SELECT … WHERE key = (SELECT … correlated subquery)`. Notez que ces requêtes ne sont valides que si la sous-requête génère une seule ligne. En raison de l’amélioration de la réécriture, certaines requêtes qui ne respectent pas cette condition peuvent désormais échouer avec une erreur ERROR: single-row subquery returns more than one row

dans les cas où elles étaient précédemment autorisées. Pour éviter cela, il peut être nécessaire de corriger ces sous-requêtes afin de garantir qu'elles renvoient une seule ligne, par exemple en ajoutant un agrégat MIN() ou MAX().

- Ajoute un identifiant SQL « KAFKA » dans Amazon Redshift pour prendre en charge le streaming depuis des sources Kafka externes vers Amazon Redshift avec ingestion en streaming directe. Ces sources incluent des sources Kafka externes telles que Confluent Managed Cloud et Apache Kafka.
- Prend en charge les écritures multi-entrepôts grâce au partage de données afin que vous puissiez mettre à l'échelle vos charges de travail d'écriture et améliorer les performances des charges de travail d'extraction, de transformation et de chargement (ETL) en utilisant différents entrepôts de différents types et tailles, en fonction de vos besoins en matière de charge de travail.
- Vous pouvez désormais exécuter des requêtes `SELECT` sur des tables Apache Iceberg gérées dans des tableaux Amazon S3à l'aide d'Amazon Redshift. Pour plus d'informations, consultez Accès aux tableaux Amazon S3 avec Amazon Redshift dans le Guide de l'utilisateur Amazon Simple Storage Service.
- Ajoute la prise en charge les requêtes d'écriture entre bases de données, afin que vous puissiez écrire sur plusieurs bases de données au sein d'un cluster Amazon Redshift. Pour plus d'informations, consultez la section Cross-database Requêtes.

Correctif 185 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.79878 : version de suivi précédente – Publiée le 3 décembre 2024
- 1.0.79868 — Version sans serveur d'Amazon Redshift — Publiée le 3 décembre 2024
- 1.0.79845 — Version actuelle du titre — Sortie le 3 décembre 2024
- 1.0.78946 : version de suivi actuelle – Publiée le 19 novembre 2024
- 1.0.78354 : version de suivi actuelle – Publiée le 12 novembre 2024
- 1.0.78130 : version d'Amazon Redshift sans serveur – Publiée le 12 novembre 2024
- 1.0.78125 : version de suivi actuelle – Publiée le 12 novembre 2024
- 1.0.78016 : version d'Amazon Redshift sans serveur – Publiée le 5 novembre 2024
- 1.0.78014 : version de suivi actuelle – Publiée le 5 novembre 2024
- 1.0.77707 : version d'Amazon Redshift sans serveur – Publiée le 4 novembre 2024

- 1.0.77687 : version de suivi actuelle – Publiée le 4 novembre 2024
- 1.0.77467 : version d'Amazon Redshift sans serveur – Publiée le 4 novembre 2024
- 1.0.77433 : version de suivi actuelle – Publiée le 4 novembre 2024
- 1.0.77467 : version d'Amazon Redshift sans serveur – Publiée le 29 octobre 2024
- 1.0.77433 : version de suivi actuelle – Publiée le 29 octobre 2024
- 1.0.76991 : version d'Amazon Redshift sans serveur – Publiée le 21 octobre 2024
- 1.0.76913 : version de suivi actuelle – Publiée le 21 octobre 2024
- 1.0.76645 : version d'Amazon Redshift sans serveur – Publiée le 14 octobre 2024
- 1.0.76642 : version de suivi actuelle – Publiée le 14 octobre 2024
- 1.0.76242 : version d'Amazon Redshift sans serveur – Publiée le 10 octobre 2024
- 1.0.76230 : version de suivi actuelle – Publiée le 10 octobre 2024

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajoute la prise en charge de l'actualisation incrémentielle des vues matérialisées (VM) créées sur des tables de lacs de données.
- Permet de modifier la clé de distribution et la clé de tri pour les vues matérialisées.
- Ajoute la prise en charge de l'intégration du machine learning (ML) d'Amazon Redshift à Amazon Bedrock afin de tirer parti des grands modèles de langage (LLM) à partir de simples commandes SQL ainsi que des données d'Amazon Redshift.
- Corrige un bogue qui permettait le traitement de shapefiles vides dans les données spatiales Amazon Redshift sans générer d'erreurs.
- Corrige un bogue qui permettait aux types de données varbit et varbinary d'ingérer une valeur de chaîne vide sous la forme "", plutôt que NULL, dans une intégration zéro ETL.
- Corrige un problème lié à un cache de résultats, à cause duquel les requêtes entre bases de données renvoyaient des résultats périmés dans le cadre d'une intégration zéro ETL.
- Optimise le processus de resynchronisation avec intégration zéro ETL, réduisant ainsi les temps de resynchronisation.
- Améliore le temps d'amorçage sans ETL après les opérations de restauration et de maintenance du système. Le système peut désormais récupérer le CDC après la dernière opération de requête, au lieu de pouvoir le récupérer jusqu'au dernier point CDC disponible.

- Améliore l’observabilité pour une intégration zéro ETL avec une nouvelle table système, `sys_integration_table_activity`. Cette table suit les insertions, les mises à jour et les suppressions de tables d’intégration zéro ETL.
- Améliore l’expérience de création automatique de rôles fédérés. Les administrateurs Amazon Redshift ont désormais davantage de contrôle sur la création automatique de rôles fédérés lors de la connexion des utilisateurs fédérés. Vous pouvez désormais activer, désactiver, appliquer des filtres et configurer les paramètres de création automatique pour chaque fournisseur d’identité.
- Les utilisateurs d’IAM Identity Center peuvent exécuter COPY, UNLOAD et CREATE LIBRARY avec les informations d’identification IAM Identity Center à l’aide des autorisations d’accès S3.
- Auto-copy (COPY JOB), qui permet l'ingestion continue de fichiers depuis Amazon S3, est désormais disponible pour tous.

Correctif 184 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.77706 : version de suivi actuelle – Publiée le 12 novembre 2024
- 1.0.76832 : version de suivi précédente – Publiée le 17 octobre 2024
- 1.0.76169 : version d’Amazon Redshift sans serveur – Publiée le 10 octobre 2024
- 1.0.76142 : version de suivi actuelle – Publiée le 10 octobre 2024
- 1.0.75677 : version d’Amazon Redshift sans serveur – Publiée le 27 septembre 2024
- 1.0.75672 : version de suivi actuelle – Publiée le 27 septembre 2024
- 1.0.75504 : version d’Amazon Redshift sans serveur – Publiée le 23 septembre 2024
- 1.0.75449 : version de suivi actuelle – Publiée le 24 septembre 2024
- 1.0.74765 : version d’Amazon Redshift sans serveur – Publiée le 12 septembre 2024
- 1.0.74754 : version de suivi actuelle – Publiée le 12 septembre 2024

Nouvelles fonctionnalités et améliorations de ce correctif

- Les vues matérialisées en streaming (VM) Amazon Redshift destinées à l’ingestion de données en streaming ont augmenté la taille des colonnes VARBYTE à plus de 1 024 000 octets. Amazon Redshift peut désormais ingérer des enregistrements d’Amazon Kinesis Data Streams jusqu’à 1 048 576 octets, soit 1 Mio. Redshift peut ingérer des enregistrements d’Amazon Managed Streaming pour Apache Kafka jusqu’à 16 777 216 octets, soit 16 Mio. Si vous utilisez

la commande ATA SQL `ALTER TABLE <target_tbl> APPEND FROM <streaming_mv>`, supprimez et recréez votre <target_tbl> pour obtenir les plus grandes tailles de colonne VARBYTE correspondantes.

- Les partages de données Amazon Redshift peuvent désormais AWS Glue Data Catalog inclure des tables et des vues de lacs de données Amazon S3 qui font référence à des tables régies par Lake Formation.
- Ajoute la prise en charge de l'actualisation automatique et incrémentielle des vues matérialisées sur les tables grâce à l'intégration zéro ETL avec DynamoDB.
- Permet de configurer « l'intervalle d'actualisation » sur les tables d'intégration zéro ETL afin de spécifier le taux de rafraîchissement de la réplication sur Amazon Redshift. Vous pouvez le définir au moment de créer une base de données pour une nouvelle intégration ou de modifier la base de données d'une intégration existante.
- Ajoute la prise en charge de l'authentification MTLS (Mutual Transport Layer Security) lors de l'ingestion en streaming par Amazon Redshift pour Amazon Managed Streaming pour Apache Kafka.
- Ajoute la prise en charge du hachage de requête, un identifiant unique pour une requête SQL basé sur la représentation textuelle de la requête et les valeurs de ses paramètres. Il peut être utilisé pour identifier, regrouper et analyser des requêtes similaires. Le hachage de la requête peut désormais être trouvé dans la vue SYS_QUERY_HISTORY, avec l'ajout de deux nouvelles colonnes :
  - `user_query_hash` : le hachage tel qu'il a été soumis par l'utilisateur, y compris les littéraux de requête.
  - `generic_query_hash` : le hachage tel qu'il a été soumis par l'utilisateur sans aucun littéral de requête.
- Résout le blocage du système dans un cas rare où une intégration zéro ETL exécutait une réplication et un scan CDC, en effectuant des requêtes de table avec le cache de résultats.
- Résout un problème de gestion de la charge de travail (WLM) où une requête de fonction Python définie par l'utilisateur préemptait les autres requêtes lorsque les ressources de gestion de la charge de travail pour les requêtes de fonction Python définie par l'utilisateur n'étaient pas disponibles.
- Résolution d'un problème où la gestion de la charge de travail (WLM) ne parvenait pas à acheminer les requêtes vers la file d'attente mappée à un rôle utilisateur nouvellement créé.
- Améliore l'utilisation du disque pour les petits consommateurs de partage de données qui interrogent de grandes tables de producteurs.

- Améliore les performances des instructions INSERT pour les clusters alloués redimensionnés élastiquement à une taille supérieure.

Correctif 183 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.75655 : version de suivi précédente – Publiée le 30 septembre 2024
- 1.0.75388 : version d’Amazon Redshift sans serveur – Publiée le 25 septembre 2024
- 1.0.75379 : version de suivi actuelle – Publiée le 25 septembre 2024
- 1.0.74967 : version d’Amazon Redshift sans serveur – Publiée le 17 septembre 2024
- 1.0.74927 : version de suivi actuelle – Publiée le 17 septembre 2024
- 1.0.74518 : version d’Amazon Redshift sans serveur – Publiée le 11 septembre 2024
- 1.0.74503 : version de suivi actuelle – Publiée le 11 septembre 2024
- 1.0.74223 : version d’Amazon Redshift sans serveur – Publiée le 5 septembre 2024
- 1.0.74159 : version de suivi actuelle – Publiée le 5 septembre 2024
- 1.0.74126 : version d’Amazon Redshift sans serveur – Publiée le 30 août 2024
- 1.0.74097 : version de suivi actuelle – Publiée le 30 août 2024
- 1.0.73016 : version d’Amazon Redshift sans serveur – Publiée le 8 août 2024
- 1.0.72982 : version de suivi actuelle – Publiée le 8 août 2024

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajoute la prise en charge la découverte des autorisations étendues via SVV_DATABASE_PRIVILEGES et SVV_SCHEMA_PRIVILEGES. Introduit également la colonne privilege_scope dans SVV_DATABASE_PRIVILEGES et SVV_SCHEMA_PRIVILEGES.
- Améliore les performances des requêtes qui exécutent des opérations d’agrégation distinctes lorsque le regroupement de colonnes comporte un faible nombre de valeurs distinctes (NDV).
- Améliore les performances des INSERT/COPY instructions pour les entrepôts de données provisionnés redimensionnés élastiquement par deux fois ou plus.
- Prend en charge les variables de contexte de session dans le cadre d’une politique de masquage dynamique des données.

- Ajoute la prise en charge des sous-requêtes et des vues en tant que source de l'instruction MERGE.
- Prend en charge les procédures stockées contenant une instruction MERGE sur le mise à l'échelle de la simultanéité alloué et pour le calcul de mise à l'échelle automatique sans serveur.
- Améliore les performances des requêtes grâce à une meilleure prévision des ressources dans la gestion de la charge de travail pour les commandes COPY et pour les entrepôts redimensionnés.
- Améliore la résilience face aux erreurs de mémoire insuffisante dans les clusters dont la mémoire disponible est limitée
- Ajoute la prise en charge des caractères non ASCII en tant que délimiteurs de champs à la commande COPY.
- Permet d'ingérer des données codées dans le jeu de ISO-8859-1 caractères à l'aide de la commande COPY.
- Supprime l'obligation de spécifier CLUSTER_ARN dans la définition du schéma externe MSK si vous spécifiez un URI.
- Prend en charge l'application de filtres d'analyse par plage lors des scans sur les tables d'intégration zéro ETL.
- Prend en charge l'ajout de clés de tri aux tables d'intégration zéro ETL.
- Prend en charge les options de base de données telles que `serializable` et `collation` à spécifier avec l'instruction CREATE DATABASE lors de la création d'une base de données d'intégration zéro ETL.
- Correction du problème qui provoquait le redémarrage du cluster lorsque le filtre de données dépassait 2 Ko dans le cadre d'une intégration zéro ETL.

Correctif 182 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.73589 : version de suivi précédente – Publiée le 22 août 2024
- 1.0.73359 : version d'Amazon Redshift sans serveur – Publiée le 15 août 2024
- 1.0.73348 : version de suivi actuelle – Publiée le 15 août 2024
- 1.0.72917 : version d'Amazon Redshift sans serveur – Publiée le 12 août 2024
- 1.0.72899 : version de suivi actuelle – Publiée le 12 août 2024
- 1.0.72528 : version d'Amazon Redshift sans serveur – Publiée le 7 août 2024

- 1.0.72503 : version de suivi actuelle – Publiée le 8 août 2024
- 1.0.72239 : version d'Amazon Redshift sans serveur – Publiée le 1 août 2024
- 1.0.71714 : version d'Amazon Redshift sans serveur – Publiée le 24 juillet 2024
- 1.0.71629 : version de suivi actuelle – Publiée le 24 juillet 2024
- 1.0.70953 : version d'Amazon Redshift sans serveur – Publiée le 11 juillet 2024
- 1.0.70890 : version de suivi actuelle – Publiée le 11 juillet 2024
- 1.0.70716 : version d'Amazon Redshift sans serveur – Publiée le 8 juillet 2024
- 1.0.70695 : version de suivi actuelle – Publiée le 8 juillet 2024
- 1.0.69945 : version d'Amazon Redshift sans serveur – Publiée le 27 juin 2024
- 1.0.69938 : version de suivi actuelle – Publiée le 27 juin 2024

Nouvelles fonctionnalités et améliorations de ce correctif

- Met à jour LISTAGG, MEDIAN, PERCENTILE_CONT et PERCENTILE_DISC pour ne plus nécessiter de tables définies par l'utilisateur. Les requêtes qui font référence à des tables de catalogue ou qui ne font référence à aucune table peuvent également utiliser ces fonctions.
- Réduit le temps de planification des requêtes pour le partage de données et les requêtes de lecture en consolidant les tables temporaires entre plusieurs requêtes au cours d'une même session, pour les charges de travail à forte simultanéité.
- Fournit la disponibilité générale de l'intégration de Redshift machine learning (ML) à Amazon SageMaker AI Jumpstart, pour apporter vos propres modèles en langage étendu.
- Introduit la prise en charge du type de données d'entrée et de sortie SUPER dans le machine learning Redshift.
- Active la prise en charge d'une instruction UPDATE avec une clause JOIN lorsque la table cible est protégée par une politique de masquage dynamique des données et référencée dans la clause JOIN.
- Permet d'interroger une base de données zéro ETL sur Redshift, même après la suppression de l'intégration de la source.
- Corrige une erreur de réplication susceptible d'entraîner l'échec de l'intégration zéro ETL. Cela rend l'intégration plus résiliente.
- Permet aux utilisateurs autres que celui qui a créé une intégration zéro ETL d'interroger les données, après avoir obtenu les autorisations GRANT.

- Résout un problème de manque de mémoire susceptible de provoquer le redémarrage du cluster dans un cluster alloué Amazon Redshift avec l'intégration zéro ETL activée.
- Permet de créer une intégration RDS for MySQL Zero-ETL avec Redshift, à partir d'un cluster de base de données RDS source. Multi-AZ Un Multi-AZ cluster de base de données est un mode de déploiement semi-synchrone à haute disponibilité d'Amazon RDS avec deux instances de base de données répliques lisibles.
- Permet à un utilisateur de se connecter à un cluster Amazon MSK depuis un client consommateur de streaming Amazon Redshift en spécifiant l'URI de l'agent du cluster Amazon MSK dans la définition du schéma externe nécessaire pour associer une vue matérialisée de streaming Amazon Redshift à une rubrique Amazon MSK. Cette fonctionnalité élimine le besoin d'obtenir le nom du nœud du courtier Amazon MSK bootstrap en appelant l' GetBootStrapBroker API du cluster Amazon MSK via une passerelle Internet.
- Résout le problème lié à la reprise des instances Amazon Redshift sans serveur, permettant à un utilisateur de base de données existant de reprendre une instance sans serveur lorsqu'il se connecte à des bases de données dans Amazon Redshift Query Editor V2, à l'aide de la méthode d'authentification IAM Identity Center.
- Optimise la réplication CDC et réduit l'utilisation des ressources sur le calcul Redshift en passant à la partition basée sur des tables.
- Améliore les performances des requêtes grâce à une meilleure prévision des ressources dans la gestion de la charge de travail (WLM).
- Corrige les requêtes échouant sur les clusters de mise à l'échelle de la simultanéité avec le message suivant : plus de files d'attente de gestion de la charge de travail pour le redémarrage.
- Résout un problème de gestion de la charge de travail (WLM) où Amazon Redshift revient à la gestion manuelle de la charge de travail lorsque les clients essaient d'appliquer une configuration de gestion de la charge de travail non valide.
- Permet aux consommateurs du partage de données d'exécuter des requêtes de lecture même lorsque le producteur est en panne en raison d'une maintenance planifiée ou d'une interruption imprévue.
- Résout un problème rare de redémarrage de cluster qui se produit lorsque la fonction ANY_VALUE est utilisée dans des requêtes agrégeant des données, par exemple la fonction d'agrégation COUNT(DISTINCT).

Correctif 181 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.72031 : version de suivi actuelle – Publiée le 1er août 2024
- 1.0.71912 : version de suivi précédente – Publiée le 1er août 2024
- 1.0.70665 : version d’Amazon Redshift sans serveur – Publiée le 8 juillet 2024
- 1.0.70634 : version de suivi actuelle – Publiée le 8 juillet 2024
- 1.0.69954 : version d’Amazon Redshift sans serveur – Publiée le 26 juin 2024
- 1.0.69952 : version de suivi actuelle – Publiée le 26 juin 2024
- 1.0.69497 : version d’Amazon Redshift sans serveur – Publiée le 18 juin 2024
- 1.0.69451 : version de suivi actuelle – Publiée le 18 juin 2024
- 1.0.69076 : version d’Amazon Redshift sans serveur – Publiée le 14 juin 2024
- 1.0.69065 : version de suivi actuelle – Publiée le 14 juin 2024
- 1.0.68555 : version Amazon Redshift sans serveur – Publiée le 31 mai 2024
- 1.0.68540 : version de suivi actuelle – Publiée le 31 mai 2024
- 1.0.68328 : version Amazon Redshift sans serveur – Publiée le 23 mai 2024
- 1.0.68205 : version de suivi actuelle – Publiée le 23 mai 2024
- 1.0.67796 : version Amazon Redshift sans serveur – Publiée le 15 mai 2024
- 1.0.67788 : version de suivi actuelle – Publiée le 15 mai 2024
- 1.0.67308 : version Amazon Redshift sans serveur – Publiée le 1 mai 2024
- 1.0.67305 : version de suivi actuelle – Publiée le 1 mai 2024

Nouvelles fonctionnalités et améliorations de ce correctif

- Introduit la prise en charge des fonctions « lower_attribute_names() » et « upper_attribute_names() » qui modifient le cas des noms d’attributs pour les valeurs d’objets SUPER.
- Résout un problème dans CREATE TABLE LIKE lors de l’utilisation d’une colonne d’identité. Auparavant, la nouvelle table héritait de l’identifiant de la table source. Cela posait des problèmes si la table source était supprimée ultérieurement, car l’identifiant devenait invalide dans la nouvelle table.
- Résout un problème empêchant l’affichage de certaines tables externes dans SVV_ALL_TABLES.

- Améliore le temps d'amorçage du cluster et accélère l'initialisation des requêtes pour les charges de travail à simultanéité élevée.
- Résout un problème lié à une requête fédérée qui provoquait des erreurs lors de la transmission des fonctions split_part() à la source fédérée vers RDS et Aurora MySQL
- Prend en charge les modifications de clé de distribution initiées par l'utilisateur via les commandes ALTER TABLE...ALTER DISTSTYLE KEY DISTKEY sur les clusters de mise à l'échelle de la simultanéité alloués et pour le calcul de mise à l'échelle automatique sans serveur.
- Prend en charge les vues matérialisées actualisées manuellement qui impliquent l'agrégation sur la mise à l'échelle de la simultanéité allouée et pour le calcul de mise à l'échelle automatique sans serveur.
- Ajoute la prise en charge de l'intégration zéro ETL pour gérer les enregistrements d'une taille maximale de 16 Mo et pour la prise en charge de valeurs SUPER jusqu'à 16 Mo.
- Améliore les messages d'erreur lors de la synchronisation initiale dans une intégration zéro ETL à partir d'Aurora MySQL en fournissant des détails supplémentaires tels que le schéma et le nom de la table.
- Introduit la prise en charge du balisage avec Amazon Redshift ML CREATE MODEL. Grâce à cette amélioration, vous pouvez désormais étiqueter les ressources Amazon SageMaker AI utilisées par Amazon Redshift ML. Le balisage vous aide à gérer, identifier, organiser, rechercher et filtrer des ressources.
- Améliore les performances des requêtes impliquant des fonctions Lambda définies par l'utilisateur (UDF) en optimisant le traitement des données avec le AWS Lambda.
- Réduit l'utilisation de la mémoire lors de l'ingestion de données dans des tables triées de clusters sans serveur et redimensionnés de manière élastique.
- Ajoute la prise en charge des nouvelles lignes (\n) dans la colonne `query_text` dans la vue SYS_QUERY_HISTORY et pour la colonne `text` dans la vue SYS_QUERY_TEXT.

Correctif 180 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.68520 : version de suivi précédente – Publiée le 28 mai 2024
- 1.0.67699 : version de suivi précédente – Publiée le 15 mai 2024
- 1.0.66960 : version de suivi précédente – Publiée le 21 avril 2024
- 1.0.66954 : version de suivi actuelle – Publiée le 21 avril 2024

- 1.0.66276 : version de suivi actuelle – Publiée le 12 avril 2024
- 1.0.66290 : version Amazon Redshift sans serveur – Publiée le 10 avril 2024
- 1.0.63590 : version de suivi actuelle – Publiée le 19 février 2024
- 1.0.63567 : version Amazon Redshift sans serveur – Publiée le 16 février 2024
- 1.0.63282 : version Amazon Redshift sans serveur – Publiée le 13 février 2024
- 1.0.63269 : version de suivi actuelle – Publiée le 13 février 2024
- 1.0.63215 : version Amazon Redshift sans serveur – Publiée le 12 février 2024
- 1.0.63205 : version de suivi actuelle – Publiée le 12 février 2024
- 1.0.63030 : version Amazon Redshift sans serveur – Publiée le 7 février 2024
- 1.0.62913 : version de suivi actuelle – Publiée le 7 février 2024
- 1.0.62922 : version Amazon Redshift sans serveur – Publiée le 5 février 2024
- 1.0.62878 : version de suivi actuelle – Publiée le 5 février 2024
- 1.0.62698 — Version sans serveur d'Amazon Redshift — Publiée le 31 janvier 2024
- 1.0.62614 — Version actuelle du titre — Sortie le 31 janvier 2024
- 1.0.61687 – Version Amazon Redshift sans serveur – Publiée le 5 janvier 2024
- 1.0.61678 – Version de suivi actuelle — Publiée le 5 janvier 2024
- 1.0.61567 – Version d’Amazon Redshift sans serveur – Publiée le 31 décembre 2023
- 1.0.61559 – Version de suivi actuelle – Publiée le 31 décembre 2023
- 1.0.61430 – Version d’Amazon Redshift sans serveur – Publiée le 29 décembre 2023
- 1.0.61395 – Version de suivi actuelle – Publiée le 29 décembre 2023

Nouvelles fonctionnalités et améliorations de ce correctif

- Modifie CURRENT_USER pour ne plus tronquer à 64 caractères le nom d’utilisateur renvoyé.
- Permet d’appliquer des politiques de masquage des données aux vues standard et à liaison tardive.
- Permet d’appliquer un masquage dynamique des données (DDM) aux attributs scalaires des colonnes de type de données SUPER.
- Ajoute la fonction SQL OBJECT_TRANSFORM. Pour plus d’informations, consultez Fonction OBJECT_TRANSFORM dans le Guide du développeur de base de données Amazon Redshift.
- Permet d'appliquer un contrôle d'accès AWS Lake Formation précis à vos données imbriquées et d'effectuer des requêtes à l'aide des analyses des lacs de données Amazon Redshift.

- Ajoute le type de données INTERVAL.
- Ajoute CONTINUE_HANDLER, qui est un type de gestionnaire d'exceptions qui contrôle le flux d'une procédure stockée. En l'utilisant, vous pouvez intercepter et gérer les exceptions sans mettre fin au bloc d'instructions existant.
- Permet de définir des autorisations sur un champ d'application (schéma ou base de données) en plus des objets individuels. Cela permet aux utilisateurs et aux rôles d'obtenir une autorisation sur tous les objets actuels et futurs relevant du champ d'application.
- Permet de créer une base de données à partir d'une unité de partage des données avec des autorisations permettant aux administrateurs côté client d'accorder des autorisations individuelles sur des objets de base de données partagés à des utilisateurs et à des rôles côté consommateur.
- Ajoute la prise en charge du type de données de retour SUPER à partir de modèles BYOM distants. Cela élargit la gamme des modèles d' SageMaker IA acceptés pour inclure ceux dont les formats de retour sont plus complexes.
- Modifie les fonctions externes pour maintenant convertir implicitement les nombres avec ou sans parties fractionnaires dans le type de données numériques de la colonne. Pour les colonnes int2, int4 et int8, les nombres contenant des chiffres fractionnaires sont acceptés par troncation, sauf si le nombre est hors plage. Pour les colonnes float4 et float8, les nombres sont acceptés sans chiffres fractionnaires.
- Ajoute trois fonctions spatiales qui fonctionnent avec le système de grille d'indexation géospatiale hiérarchique H3 : H3_FromLongLat, H3_ et H3_Polyfill. FromPoint

Correctif 179 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.62317 — Version sans serveur d'Amazon Redshift — Publiée le 29 janvier 2024
- 1.0.62312 : version de suivi précédente — Publiée le 29 janvier 2024
- 1.0.61631 – Version Amazon Redshift sans serveur – Publiée le 5 janvier 2024
- 1.0.61626 – Version de suivi actuelle — Publiée le 5 janvier 2024
- 1.0.61191 – Version de suivi actuelle – Publiée le 16 décembre 2023
- 1.0.61150 – Version d'Amazon Redshift sans serveur – Publiée le 16 décembre 2023
- 1.0.60982 – Version d'Amazon Redshift sans serveur – Publiée le 13 décembre 2023
- 1.0.60854 – Version de suivi actuelle – Publiée le 10 décembre 2023
- 1.0.60354 – Version d'Amazon Redshift sans serveur – Publiée le 22 novembre 2023

- 1.0.60353 – Version de piste actuelle – Publiée le 21 novembre 2023
- 1.0.60293 – Version d'Amazon Redshift sans serveur – Publiée le 21 novembre 2023
- 1.0.60292 – Version de piste actuelle – Publiée le 22 novembre 2023
- 1.0.60161 – Version d'Amazon Redshift sans serveur – Publiée le 18 novembre 2023
- 1.0.60140 – Version de piste actuelle – Publiée le 18 novembre 2023
- 1.0.60139 – Version d'Amazon Redshift sans serveur – Publiée le 18 novembre 2023
- 1.0.59947 – Version d'Amazon Redshift sans serveur – Publiée le 16 novembre 2023
- 1.0.59945 – Version de piste actuelle – Publiée le 16 novembre 2023
- 1.0.59118 – Version d'Amazon Redshift sans serveur – Publiée le 9 novembre 2023
- 1.0.59117 – Version de piste actuelle – Publiée le 9 novembre 2023

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajoute une prise en charge afin que les utilisateurs fédérés disposant des autorisations appropriées puissent consulter les vues système de masquage dynamique des données et de sécurité au niveau des lignes, y compris :
  - SVV_ATTACHED_MASKING_POLICY
  - SVV_MASKING_POLICY
  - SVV_RLS_ATTACHED_POLICY
  - SVV_RLS_POLICY
  - SVV_RLS_RELATION
- Ajoute une fonctionnalité permettant qu'une requête contenant uniquement des fonctions scalaires dans la clause FROM entraîne désormais une erreur.
- Ajoute des instructions CREATE TABLE AS (CTAS) avec une fonctionnalité de tables cible permanentes pour les clusters de mise à l'échelle de la simultanéité. Les clusters de mise à l'échelle de la simultanéité prennent désormais en charge un plus grand nombre de requêtes.
- Ajoute les tables système suivantes pour suivre le statut de redistribution des tables après l'exécution d'un redimensionnement classique sur des clusters RA3 :
  - La table système SYS_RESTORE_STATE indique la progression de la redistribution au niveau de la table.
  - La table système SYS_RESTORE_LOG indique l'historique du débit de redistribution des données.

- Améliore la réduction de l'asymétrie des tranches sur les tables EVEN après l'exécution du redimensionnement classique sur les types de nœuds RA3. Cela s'applique également aux clusters du patch 178 ayant effectué un redimensionnement classique.
- Ajoute la prise en charge de UNLOAD avec EXTENSION sur les clusters de mise à l'échelle de la simultanéité.
- Améliore les performances pour les requêtes contenant des UDF λ HashJoins et des NestLoop jointures.
- Améliore les performances d'Elastic Resize sur les types de nœuds RA3.
- Améliore les performances des requêtes de partage des données.
- Améliore les performances des requêtes d'analyse lancées manuellement dans des clusters provisionnés redimensionnés élastiquement et des groupes de travail sans serveur.
- Améliore les performances des requêtes WLM automatiques grâce à une meilleure prévision des ressources dans la gestion de la charge de travail.
- Supprime la fonctionnalité de lancement des clusters dans des VPC de location dédiée. Cette modification n'affecte pas la location des instances EC2 du VPC. Vous pouvez modifier la location par défaut de votre VPC à l'aide `modify-vpc-tenancy` AWS CLI de la commande.
- L'actualisation manuelle des vues matérialisées est désormais prise en charge sur les clusters de mise à l'échelle de la simultanéité provisionnés et pour le calcul de mise à l'échelle automatique sans serveur.
- Ajoute la prise en charge des littéraux INTERVAL à la fonction EXTRACT. Par exemple, `EXTRACT('hours' from Interval '50 hours')` renvoie 2, car 50 heures sont interprétées comme 2 jours et 2 heures, et que la composante horaire de 2 est extraite.

Correctif 178 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.63327 : version de suivi actuelle – Publiée le 9 février 2024
- 1.0.63313 : version de suivi précédente – Publiée le 9 février 2024
- 1.0.60977 – Version de piste de fin – Publiée le 15 décembre 2023
- 1.0.59596 – Version de piste actuelle – Publiée le 9 novembre 2023
- 1.0.58593 – Version d'Amazon Redshift sans serveur – Publiée le 23 octobre 2023
- 1.0.58558 – Version de suivi actuelle – Publiée le 23 octobre 2023

- 1.0.57864 – Version de suivi actuelle – Publiée le 12 octobre 2023
- 1.0.57850 – Version d'Amazon Redshift sans serveur – Publiée le 12 octobre 2023
- 1.0.56952 – Version de piste actuelle – Publiée le 25 septembre 2023
- 1.0.56970 – Version d'Amazon Redshift sans serveur – Publiée le 25 septembre 2023

Nouvelles fonctionnalités et améliorations de ce correctif

- Amazon Redshift a désormais amélioré les performances des requêtes de partage de données en accélérant l'actualisation des métadonnées sur les instances client alors que des modifications de données se produisent simultanément sur l'instance du producteur.
- Prend en charge l'actualisation automatique et incrémentielle des vues matérialisées sur les instances de consommateurs de partage de données Amazon Redshift lorsque les tables de base de la vue matérialisée font référence aux données partagées.
- Prend en charge le stockage d'objets volumineux d'une taille maximale de 16 Mo dans le type de données SUPER. Lors de l'ingestion à partir de fichiers source JSON, PARQUET, TEXT et CSV, vous pouvez charger des données semi-structurées ou des documents sous forme de valeurs dans le type de données SUPER, jusqu'à 16 Mo.
- Prend en charge le redimensionnement élastique pour la mise à l'échelle vers et depuis un cluster Amazon Redshift RA3 à nœud unique.
- Single-node Les clusters Amazon Redshift RA3 peuvent désormais bénéficier d'améliorations de chiffrement, réduisant ainsi le temps de chiffrement global et améliorant la disponibilité de l'entrepôt de données pendant le processus de chiffrement.
- Améliore la prise en charge des requêtes lors de la désimbrication et du dépivotement des données stockées dans le type de données SUPER.
- Améliore les performances d'actualisation des vues matérialisées avec les types de données SUPER.
- Prend en charge l'agrégation des littéraux INTERVAL avec la fonction ANY_VALUE.
- L'ingestion en streaming prend désormais en charge la nouvelle commande SQL suivante pour purger les données de streaming : `DELETE FROM streaming_materialized_views WHERE <where filter clause>`.
- La fonction DECODE remplace une valeur spécifique par une autre valeur spécifique ou une valeur par défaut, selon le résultat d'une condition d'égalité. DECODE nécessite désormais les trois paramètres suivants :

  - expression
  - search
  - result
- Ajoute une fonctionnalité aux procédures stockées pour permettre la détection du dépassement de données, des erreurs de conversion des types de données et de les gérer au sein d'un bloc de gestion des exceptions.
- Vous recevrez désormais une erreur lorsque vous interrogerez les relations de sécurité au niveau des lignes ou les relations protégées par le masquage dynamique des données si vous modifiez enable_case_sensitive_identifier pour qu'il soit différent du paramètre par défaut de la session. En outre, la configuration suivante est bloquée lorsque des politiques de sécurité au niveau des lignes ou de masquage dynamique des données sont appliquées dans votre cluster provisionné ou dans votre espace de noms sans serveur :

  ```
  ALTER USER <current_user> SET case-sensitive identifier.
  ```
- La commande MERGE prend désormais en charge une syntaxe simplifiée qui ne nécessite que la table cible et la table source. Pour en savoir plus, consultez MERGE dans le Guide du développeur de base de données Amazon Redshift.
- Permet d'associer des politiques de masquage dynamique des données identiques à plusieurs utilisateurs ou rôles avec la même priorité ou sans spécifier de priorité.
- Vous pouvez désormais spécifier COLLATION lors de l'ajout d'une nouvelle colonne via ALTER TABLE ADD COLUMN.
- Résout un problème qui retarde l'application des règles QMR sur les clusters de mise à l'échelle simultanée et Amazon Redshift sans serveur.
- Amazon Redshift Federated Query a étendu la prise en charge de la poussée pour le fuseau horaire avec horodatage sur Amazon RDS for PostgreSQL et Amazon Aurora PostgreSQL.
- Vous pouvez désormais utiliser les noms de bases de données Amazon RDS for MySQL et Aurora MySQL commençant par des chiffres avec des requêtes fédérées.
- Ajoute la vue SYS_ANALYZE_HISTORY, qui contient les détails des enregistrements des opérations ANALYZE.
- Ajoute la vue SYS_ANALYZE_COMPRESSION_HISTORY, qui contient les détails des enregistrements pour les opérations d'analyse de compression pendant les commandes COPY ou ANALYZE COMPRESSION.
- Ajoute la vue SYS_SESSION_HISTORY, qui contient les détails des enregistrements relatifs aux sessions actives, historiques et redémarrées.

- Ajoute la vue SYS_TRANSACTION_HISTORY, qui contient les détails des enregistrements relatifs à l'analyse au niveau des transactions, qui fournissent le temps passé à la validation, les données, le nombre de blocs validés et le niveau d'isolement.
- Ajoute la vue SVV_REDSHIFT_SCHEMA_QUOTA, qui contient les enregistrements relatifs aux quotas et à l'utilisation actuelle du disque pour chaque schéma d'une base de données.
- Ajoute la vue SYS_PROCEDURE_CALL, qui contient les enregistrements relatifs aux appels de procédure stockée, notamment l'heure de début, l'heure de fin, le statut de l'appel de procédure stockée et la hiérarchie des appels pour les appels de procédure stockée imbriqués.
- Ajoute la vue SYS_CROSS_REGION_DATASHARING_USAGE, qui contient les enregistrements relatifs au suivi de l'utilisation du partage de données entre régions.
- Ajoute la vue SYS_PROCEDURE_MESSAGES, qui contient les enregistrements relatifs aux informations de suivi relatives aux messages de procédure stockée journalisés.
- Ajoute la vue SYS_UDF_LOG, qui contient les enregistrements relatifs au suivi des messages du journal système provenant d'appels de fonctions définis par l'utilisateur, d'erreurs, d'avertissements ou de traces, le cas échéant.
- Ajoute les nouvelles colonnes IS_RECURSIVE, IS_NESTED, S3LIST_TIME et GET_PARTITION_TIME à SYS_EXTERNAL_QUERY_DETAIL.
- Ajoute MaxRPU, un nouveau paramètre de contrôle des coûts de calcul pour Redshift Serverless. Avec MaxRPU, vous avez la possibilité de spécifier un seuil de calcul supérieur pour contrôler les coûts des entrepôts des données à différents moments, en sélectionnant le niveau de calcul maximal que Redshift Serverless peut mettre à l'échelle par groupe de travail.
- Corrige la sortie du littéral INTERVAL avec des chaînes d'intervalles numériques. Par exemple, un intervalle qui indique `INTERVAL '1' YEAR` renvoie maintenant `1 YEAR` au lieu de `"00:00:00`. En outre, la sortie du littéral INTERVAL est tronquée au plus petit composant INTERVAL spécifié. Par exemple, `INTERVAL '1 day 1 hour 1 minute 1.123 seconds' HOUR TO MINUTE` devient `1 day 01:01:00`.

Correctif 177 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.57922 – Version de piste de fin – Publiée le 12 octobre 2023
- 1.0.57799 – Version d'Amazon Redshift sans serveur – Publiée le 10 octobre 2023
- 1.0.57798 – Version de suivi actuelle – Publiée le 10 octobre 2023

- 1.0.57085 – Version de piste de fin – Publiée le 26 septembre 2023
- 1.0.56899 – Version d'Amazon Redshift sans serveur – Publiée le 21 septembre 2023
- 1.0.56754 – Version de piste actuelle – Publiée le 21 septembre 2023
- 1.0.56242 – Version de piste actuelle – Publiée le 11 septembre 2023
- 1.0.55539 – Version d'Amazon Redshift sans serveur – Publiée le 28 août 2023
- 1.0.55524 – Version de piste actuelle – Publiée le 28 août 2023
- 1.0.54899 – Version de suivi actuelle – Publiée le 15 août 2023
- 1.0.54899 – Version de piste actuelle – Publiée le 14 août 2023
- 1.0.54899 – Version de suivi actuelle – Publiée le 15 août 2023
- 1.0.54239 – Version de suivi actuelle – Publiée le 3 août 2023
- 1.0.54321 – Version d'Amazon Redshift sans serveur – Publiée le 3 août 2023

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajout de la vue SYS_MV_STATE, qui contient une ligne pour chaque transition d'état d'une vue matérialisée. SYS_MV_STATE peut être utilisé pour la surveillance de l'actualisation des vues matérialisées pour les instances provisionnées d'Amazon Redshift sans serveur et d'Amazon Redshift.
- Ajout de la vue SYS_USERLOG, qui enregistre les détails concernant les modifications apportées à un utilisateur de base de données pour les actions de création, de suppression, de modification (changement de nom/propriétés) d'un utilisateur.
- Ajoute la vue SYS_COPY_REPLACEMENTS, qui affiche un journal qui enregistre les cas où des UTF-8 caractères non valides ont été remplacés par la commande COPY avec l'option ACCEPTINVCHARS.
- Ajout de la vue SYS_SPATIAL_SIMPLIFY, qui contient des informations sur les objets de géométrie spatiale simplifiée avec la commande COPY.
- Ajout de la vue SYS_VACUUM_HISTORY, que vous pouvez utiliser pour afficher les détails et les résultats des opérations VACUUM.
- Ajout de la vue SYS_SCHEMA_QUOTA_VIOLATIONS pour enregistrer l'occurrence, l'horodatage, l'ID de transaction (XID) et d'autres informations utiles en cas de dépassement d'un quota de schéma.
- Ajout de la vue SYS_RESTORE_STATE, que vous pouvez utiliser pour surveiller la progression de la redistribution de chaque table du cluster lors d'un redimensionnement classique asynchrone.

- Ajout de la vue SYS_EXTERNAL_QUERY_ERROR, qui renvoie des informations sur les erreurs d'analyse de Redshift Spectrum.
- Ajout du paramètre de balise à la commande CREATE MODEL, ce qui vous permet désormais de suivre les coûts d'entraînement avec les tâches d'entraînement Autopilot.
- Ajout des noms de domaine personnalisés (CNAME) pour les clusters Amazon Redshift.
- Ajout de la prise en charge préliminaire d'Apache Iceberg, ce qui permet aux clients d'exécuter des requêtes analytiques sur des tables Apache Iceberg depuis Amazon Redshift.
- Ajout de la prise en charge de l'utilisation de rôles utilisateur avec les groupes de paramètres de la gestion de la charge de travail (WLM).
- Prend en charge le montage automatique de AWS Glue Data Catalog, ce qui permet aux clients d'exécuter plus facilement des requêtes dans leurs lacs de données.
- Ajout d'une fonctionnalité selon laquelle l'utilisation de fonctions de regroupement sans clause GROUP BY ou l'utilisation d'opérations de regroupement dans une clause WHERE génère une erreur.
- Ajout d'une fonctionnalité aux procédures stockées pour permettre la détection des erreurs de division par zéro et de les gérer au sein d'un bloc de gestion des exceptions.
- Correction d'un bogue qui empêchait les requêtes d'utiliser la mise à l'échelle de la simultanéité pour écrire des données dans des tables lorsque la table source était une table de partage de données.
- Correction du problème lié à l'identifiant sensible à la casse documenté dans la rubrique enable_case_sensitive_identifier, qui est désormais compatible avec les instructions MERGE.
- Correction du bogue qui faisait qu'une requête au niveau de la fonction pg_get_late_binding_view_cols () pouvait parfois être ignorée. Vous pouvez maintenant toujours annuler ces requêtes.
- Amélioration des performances pour les requêtes de partage de données s'exécutant au niveau des consommateurs lors de l'exécution de tâches de vidage (VACUUM) au niveau du producteur.
- Amélioration des performances pour les requêtes de partage de données et les requêtes de mise à l'échelle de la simultanéité, en particulier dans le cas des modifications de données simultanées au niveau du producteur ou lors du déchargement sur une instance de mise à l'échelle de la simultanéité rattachée au consommateur.

Correctif 176 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.56738 – Version de piste de fin – Publiée le 21 septembre 2023
- 1.0.55837 – Version de piste de fin – Publiée le 11 septembre 2023
- 1.0.54776 – Version de suivi actuelle – Publiée le 15 août 2023
- 1.0.54052 – Version de suivi actuelle – Publiée le 26 juillet 2023
- 1.0.53642 – Version d'Amazon Redshift sans serveur – Publiée le 20 juillet 2023
- 1.0.53301 – Version de suivi actuelle – Publiée le 20 juillet 2023
- 1.0.52943 – Version d'Amazon Redshift sans serveur – Publiée le 7 juillet 2023
- 1.0.52931 – Version de suivi actuelle – Publiée le 7 juillet 2023
- 1.0.52194 – Version d'Amazon Redshift sans serveur – Publiée le 21 juin 2023
- 1.0.51986 – Version de suivi actuelle – Publiée le 16 juin 2023
- 1.0.51594 – Version de suivi actuelle – Publiée le 9 juin 2023

Nouvelles fonctionnalités et améliorations de ce correctif

- Amélioration de la gestion des erreurs lors de l'écriture de GROUP BY () pour un jeu de regroupement vide. Cela a été ignoré précédemment et renvoie maintenant une erreur d'analyse.
- Améliorations des performances pour l'actualisation de manière incrémentielle des vues matérialisées avec des colonnes SUPER.
- ALTER TABLE <target_tbl> APPEND FROM <streaming_mv> : la commande SQL (ATA) permet désormais de déplacer tous les enregistrements d'une vue matérialisée en streaming en tant que source, en plus des tables en tant que source, vers une table cible. La prise en charge d'ATA sur les vues matérialisées en streaming permet aux utilisateurs de purger rapidement tous les enregistrements d'une vue matérialisée en streaming en les déplaçant vers une autre table pour gérer la croissance des données.
- TRUNCATE <streaming_mv> : la commande SQL permet désormais de tronquer tous les enregistrements d'une vue matérialisée en streaming, en plus des tables. TRUNCATE supprime tous les enregistrements dans la vue matérialisée en streaming, tout en laissant la structure de la vue matérialisée en streaming intacte. L'exécution de TRUNCATE sur des vues matérialisées en streaming permet aux clients de purger rapidement tous les enregistrements d'une vue matérialisée en streaming afin de gérer la croissance des données.
- Ajout d'une fonctionnalité pour la clause QUALIFY à la commande SELECT.
- Le machine learning de Redshift prend en charge les prévisions de séries chronologiques grâce à l'intégration à Amazon Forecast.

- AWS Glue Data Catalog le montage automatique est pris en charge pour simplifier l'interrogation d'un lac de données sans étapes supplémentaires pour créer des références de schéma externes.
- La modification d'une politique RLS est désormais prise en charge. Pour plus de détails, consultez ALTER RLS POLICY dans la documentation.
- Les fonctions UDF Lambda prennent désormais en charge le paramètre de volatilité de la fonction STABLE dans l'instruction CREATE FUNCTION. Lorsque le paramètre STABLE est utilisé dans l'instruction CREATE FUNCTION et que l'UDF Lambda est appelée plusieurs fois, avec les mêmes arguments, le nombre attendu d'invocations de fonction UDF Lambda diminue. La catégorie de volatilité de la fonction STABLE est expliquée plus en détail dans les paramètres CREATE FUNCTION.
- Plusieurs améliorations des performances de la fonction UDF Lambda. Plus précisément, amélioration de la prise en charge par lots d'enregistrements lors de l'interrogation d'une table protégée par une politique de sécurité au niveau des lignes (RLS).
- Réduction du temps de chiffrement global pour les clusters Amazon Redshift RA3 et amélioration de la disponibilité de l'entrepôt des données pendant le chiffrement. Pour plus d'informations, consultez Chiffrement de base de données Amazon Redshift.
- Une nouvelle vue système SYS_MV_REFRESH_HISTORY a été ajoutée à Redshift. La vue SYS_MV_REFRESH_HISTORY contient une ligne pour l'activité d'actualisation des vues matérialisées. À l'aide de SYS_MV_REFRESH_HISTORY, vous pouvez consulter l'historique d'actualisation des vues matérialisées. SYS_MV_REFRESH_HISTORY est visible par tous les utilisateurs. Les super-utilisateurs peuvent voir toutes les lignes, tandis que les utilisateurs standard peuvent voir uniquement leurs propres données.

  Une nouvelle colonne SPILLED_BLOCK_LOCAL_DISK a été ajoutée à la vue système SYS_QUERY_DETAIL. La nouvelle colonne SPILLED_BLOCK_LOCAL_DISK aide les clients à déterminer les blocs déversés sur le disque local. Vous pouvez utiliser SYS_QUERY_DETAIL pour afficher les détails des requêtes au niveau d'une étape. SYS_QUERY_DETAIL est visible par tous les utilisateurs. Les super-utilisateurs peuvent voir toutes les lignes, tandis que les utilisateurs standard peuvent voir uniquement les métadonnées auxquelles ils ont accès.
- Une nouvelle vue système, SYS_QUERY_TEXT, a été ajoutée à Amazon Redshift sans serveur et Amazon Redshift a été provisionné. La vue SYS_QUERY_TEXT est similaire à SVL_STATEMENTTEXT pour les clusters provisionnés. Utilisez la colonne `sequence` de la vue SYS_QUERY_TEXT pour obtenir le texte complet de l'instruction SQL.

Correctif 175 d’Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.53064 – Version de suivi actuelle – Publiée le 7 juillet 2023
- 1.0.51973 – Version de suivi actuelle – Publiée le 16 juin 2023
- 1.0.51781 – Version de suivi actuelle – Publiée le 10 juin 2023
- 1.0.51314 – Version Amazon Redshift sans serveur – Publiée le 3 juin 2023
- 1.0.51304 – Version de suivi actuelle – Publiée le 2 juin 2023
- 1.0.50708 – Version de suivi actuelle – Publiée le 19 mai 2023
- 1.0.50300 – Version de suivi actuelle – Publiée le 8 mai 2023
- 1.0.49710 – Version Amazon Redshift sans serveur – Publiée le 28 avril 2023
- 1.0.49676 – Version de suivi actuelle – Publiée le 28 avril 2023

Nouvelles fonctionnalités et améliorations de ce correctif

- Correctifs de bogues mineurs.
- L'ingestion de streaming par Amazon Redshift prend désormais en charge l'ingestion de streaming entre régions lorsque votre source Amazon Kinesis Data Streams (KDS) ou le sujet Amazon Managed Streaming for Apache Kafka (MSK) peuvent être situés dans AWS une région différente de celle AWS où se trouve votre entrepôt de données Amazon Redshift. La documentation disponible dans la rubrique Mise en route de l’ingestion en streaming à partir d’ Amazon Kinesis Data Streams a été révisée et explique comment le mot clé REGION est utilisé.
- Ajustement de l’heure d’été en Égypte.
- Amélioration des délais globaux de chiffrement des clusters RA3.

Correctif 174 d’Amazon Redshift

1.0.51296 – Publiée le 2 juin 2023

Mise à jour de la piste de fin. Aucune note de mise à jour.

1.0.50468 – Publié le 9 mai 2022

Publication de maintenance. Aucune note de mise à jour.

1.0.49780, 1.0.49868 et 1.0.49997 – Publiés le 28 avril 2023

Notes de mise à jour pour cette version :

- Amélioration de la prise en charge du traitement par lots pour les fonctions UDF Lambda.
- Traitement par lots incrémentiel pour les fonctions UDF Lambda.
- Nouvelle commande SQL MERGE pour appliquer les modifications de données source aux tables Amazon Redshift.
- Nouvelle fonctionnalité de masquage dynamique des données pour simplifier le processus de protection des données sensibles dans un entrepôt des données Amazon Redshift.
- Nouveau contrôle d'accès centralisé pour le partage de données avec Lake Formation qui permet de gérer les autorisations accordées, de consulter les contrôles d'accès et d'auditer les autorisations sur les tables et les vues des partages de données Amazon Redshift à l'aide des API Lake Formation et de la console. AWS
- Ajustement de l’heure d’été en Égypte.

1.0.49087 - Publiée le 12 avril 2023

Publication de maintenance. Aucune note de mise à jour.

1.0.48805 - Publiée le 5 avril 2023

Notes de mise à jour pour cette version :

- Amazon Redshift a introduit des améliorations de performances supplémentaires pour les requêtes riches en chaînes de caractères à l’aide de BYTEDICT, un nouvel encodage de compression dans Amazon Redshift qui accélère le traitement des données basées sur les chaînes de caractères de 5 à 63 fois par rapport aux encodages de compression alternatifs tels que LZO ou ZSTD. Pour plus d’informations sur cette fonctionnalité, consultez Encodages de compression dans le Guide du développeur de base de données Amazon Redshift.

1.0.48004 – Publiée le 17 mars 2023

Publication de maintenance. Aucune note de mise à jour.

1.0.47470 – Publiée le 11 mars 2023

Notes de mise à jour pour cette version :

- Améliore les performances des requêtes sur `pg_catalog.svv_table_info` Ajoute également une nouvelle colonne `create_time`. Lors de la création d'un tableau, cette colonne stocke le date/time tampon en UTC.
- Ajout du soutien pour la spécification du délai d’attente au niveau de la session sur les requêtes fédérées.

Correctif 173 d’Amazon Redshift

1.0.48714 – Publié le 28 avril 2023

Notes de mise à jour pour cette version :

- Ajustement de l’heure d’été en Égypte.

1.0.49074 - Publiée le 12 avril 2023

Notes de mise à jour pour cette version :

- Mise à jour de la configuration du fuseau horaire en fonction de la version 2022g de la bibliothèque IANA.

1.0.48766 – Publiée le 5 avril 2023

Publication de maintenance. Aucune note de mise à jour.

1.0.48714 – Publiée le 5 avril 2023

Publication de maintenance. Aucune note de mise à jour.

1.0.48022 – Publiée le 17 mars 2023

Publication de maintenance. Aucune note de mise à jour.

1.0.47357 – Publiée le 7 mars 2023

Publication de maintenance. Aucune note de mise à jour.

1.0.46987 – Publié le 24 février 2023

Publication de maintenance. Aucune note de mise à jour.

1.0.46806 – Publié le 18 février 2023

Publication de maintenance. Aucune note de mise à jour.

1.0.46607 – Publié le 13 février 2023

Notes de mise à jour pour cette version :

- Nous convertissons désormais automatiquement les tables dont les clés de tri entrelacées sont définies manuellement en clés de tri composées si leur style de distribution a été défini sur DISTSTYLE KEY, afin d'améliorer les performances de ces tables. Cela se fait au moment de la restauration d'un instantané dans Amazon Redshift sans serveur.

1.0.45698 – Publié le 20 janvier 2023

Notes de mise à jour pour cette version :

- Ajoute un paramètre d'extension de fichier à la commande UNLOAD, de sorte que des extensions de fichier soient automatiquement ajoutées aux noms de fichiers.
- Supporte la protection RLS-protected des objets par défaut lors de leur ajout à un partage de données ou s'ils font déjà partie d'un partage de données. Les administrateurs peuvent désormais désactiver RLS pour les unités de partage des données afin de permettre aux consommateurs d'accéder à l'objet protégé.
- Ajoute de nouvelles tables système pour la surveillance : `SVV_ML_MODEL_INFO`, `SVV_MV_DEPENDENCY` et `SYS_LOAD_DETAIL`. Ajoute également les colonnes `data_skewness` et `time_skewness` à la table système `SYS_QUERY_DETAIL`.

Correctif 172 d'Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.46534 – Publié le 18 février 2023
- 1.0.46523 – Publié le 13 février 2023
- 1.0.46206 – Publié le 1er février 2023
- 1.0.45603 – Publié le 20 janvier 2023
- 1.0.44924 – Publié le 19 décembre 2022
- 1.0.44903 – Publié le 18 décembre 2022
- 1.0.44540 – Publié le 13 décembre 2022
- 1.0.44126 – Publié le 23 novembre 2022
- 1.0.43980 – Publié le 17 novembre 2022

Nouvelles fonctionnalités et améliorations de ce correctif

- Les tables créées par CTAS sont AUTO par défaut.
- Ajoute la prise en charge de la sécurité au niveau des lignes (RLS) sur les vues matérialisées.
- Augmente le délai d'expiration de S3 pour améliorer le partage de données entre régions.
- Ajoute une nouvelle fonction spatiale `ST_GeomFromGeohash`.
- Améliore la sélection automatique de la clé de distribution à partir de clés primaires composites afin d'améliorer les performances dès le départ.
- Ajoute la clé primaire automatique à la clé de distribution pour les tables dotées de clés primaires composites afin d'améliorer les performances dès le départ.
- Améliore le dimensionnement de la simultanéité pour permettre à un plus grand nombre de requêtes d'être mises à l'échelle même en cas de modification des données.
- Améliore les performances des requêtes de partage des données.
- Ajoute des métriques de probabilité de machine learning pour les modèles de classification.
- Ajoute de nouvelles tables système pour la surveillance : `SVV_USER_INFO`, `SVV_MV_INFO`, `SYS_CONNECTION_LOG`, `SYS_DATASHARE_USAGE_PRODUCER`, `SYS_DATASHARE_USAGE_CONSUMER` et `SYS_DATASHARE_CHANGE_LOG`.
- Ajoute une prise en charge de l'interrogation des colonnes VARBYTE dans les tables externes pour les types de fichiers Parquet et ORC.

Correctif 171 d’Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.43931 – Publié le 16 novembre 2022
- 1.0.43551 – Publié le 5 novembre 2022
- 1.0.43331 – Publié le 29 septembre 2022
- 1.0.43029 – Publié le 26 septembre 2022

Nouvelles fonctionnalités et améliorations de ce correctif

- Support CONNECT BY : ajoute la prise en charge de la construction CONNECT BY SQL, qui vous permet d’interroger de manière récursive les données hiérarchiques de votre entrepôt des données en fonction de la relation parent-enfant au sein de ce jeu de données.

Correctif 170 d’Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.43922 – Publié le 21 novembre 2022
- 1.0.43573 – Publié le 7 novembre 2022
- 1.0.41881 – Publié le 20 septembre 2022
- 1.0.41465 — Publié le 7 septembre 2022
- 1.0.40325 – Publié le 27 juillet 2022

Nouvelles fonctionnalités et améliorations de ce correctif

- ST_ GeomfromGeo JSON : construit un objet de géométrie spatiale Amazon Redshift à partir de VARCHAR dans une représentation GeoJSON.

Correctif 169 d’Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.41050 – Publié le 7 septembre 2022

- 1.0.40083 – publiée le 16 juillet 2022
- 1.0.39734 – publiée le 7 juillet 2022
- 1.0.39380 – publiée le 23 juillet 2022
- 1.0.39251 – publiée le 15 juin 2022
- 1.0.39009 – publiée le 8 juin 2022

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajoute un rôle en tant que paramètre pour la commande Alter Default Privileges afin de prendre en charge le contrôle Role-based d'accès.
- Ajoute le paramètre ACCEPTINVCHARS pour prendre en charge le remplacement des UTF-8 caractères non valides lors de la copie à partir de fichiers Parquet et ORC.
- Ajoute la fonction OBJECT(k,v) pour créer des objets SUPER à partir de paires clé-valeur.

Correctif 168 d’Amazon Redshift

Versions de cluster dans ce correctif :

- 1.0.38698 – publiée le 25 mai 2022
- 1.0.38551 – publiée le 20 mai 2022
- 1.0.38463 – publiée le 18 mai 2022
- 1.0.38361 – publiée le 13 mai 2022
- 1.0.38199 – publiée le 9 mai 2022
- 1.0.38112 – Publiée le 6 mail 2022
- 1.0.37684 - Publiée le 20 avril 2022

Nouvelles fonctionnalités et améliorations de ce correctif

- Ajoute la prise en charge du type de modèle Linear Learner dans Amazon Redshift ML.
- Ajoute l’option SNAPSHOT au niveau d’isolation des transactions SQL.
- Ajoute `farmhashFingerprint64` en tant que nouvel algorithme de hachage pour les données `VARBYTE` et `VARCHAR`.
- Prend en charge la fonction AVG lors de l’actualisation incrémentielle des vues matérialisées.

- Prend en charge les sous-requêtes corrélées sur les tables externes dans Redshift Spectrum.
- Pour améliorer les performances des requêtes prêtes à l'emploi, Amazon Redshift choisit automatiquement une clé primaire à colonne unique pour des tables spécifiques en tant que clé de distribution.

Changements de comportement dans Amazon Redshift

Alors qu'Amazon Redshift continue d'évoluer et de s'améliorer, certains changements de comportement sont introduits afin d'améliorer les performances, la sécurité et l'expérience utilisateur. Cette page constitue une ressource complète qui vous permet de rester informé de ces mises à jour critiques, de prendre des mesures et d'éviter d'éventuelles perturbations de vos charges de travail.

Changements de comportement à venir

Ce qui suit décrit les changements de comportement à venir.

Rubriques

- Amazon Redshift prend des instantanés automatisés des clusters de producteurs de partage de données interrompus à compter du 30 septembre 2026
- Le type de données SUPER prend en charge les chaînes individuelles plus grandes à partir du patch 206
- AWS KMS application des autorisations clés pour les API Amazon Redshift sans serveur après le 17 août 2026
- Amazon Redshift impose le verrouillage des utilisateurs après plusieurs tentatives de connexion infructueuses, à commencer par le patch 208
- Modèle de facturation amélioré pour les instantanés manuels sur les instances Amazon Redshift Serverless et Amazon Redshift RG à compter du 8 juin 2026
- Les tables Iceberg DELETE on Lake Formation nécessitent l'autorisation DELETE à compter du patch 202
- Amazon Redshift Serverless préserve les intégrations d'événements sans ETL et S3 lors de la restauration de snapshots à partir du correctif 202
- Fin du support pour le pilote ODBC 1.x Amazon Redshift le 31 décembre 2026
- Les fonctions scalaires Python définies par l'utilisateur ne seront plus prises en charge après le 30 juin 2026
- Modification du Auto-REFRESH comportement de la vue matérialisée (MV) après le 27 février 2026
- Amazon Redshift ne prendra pas en charge les fonctions permettant d'accéder aux informations des consommateurs via l'unité de partage des données après le 16 février 2026

- Modifications apportées à la version du protocole TLS (Minimum Transport Layer Security) à compter du 31 octobre 2026
- Amazon Redshift ne prendra pas en charge la création de nouvelles fonctions scalaires Python définies par l'utilisateur après le 30 octobre 2025

Amazon Redshift prend des instantanés automatisés des clusters de producteurs de partage de données interrompus à compter du 30 septembre 2026

À compter du 30 septembre 2026, Amazon Redshift prend des instantanés automatisés d'un cluster de producteurs de partage de données suspendu. Comme les consommateurs peuvent écrire à un producteur suspendu, ces instantanés capturent ces écritures de partage de données et fournissent un point de récupération.

Cela peut vous affecter si vous interrompez les clusters de producteurs de partage de données.

Auparavant, Amazon Redshift ne prenait pas d'instantanés automatisés de ces clusters pendant leur pause. Le dernier instantané automatique disponible pour la restauration était donc celui pris lors de la suspension du cluster. Les instantanés automatisés continuent désormais d'être créés pendant toute la période de pause.

Ces instantanés suivent le calendrier et la période de conservation des instantanés automatisés existants du cluster, et aucune action n'est requise. Pour un cluster suspendu qui n'est pas un producteur de partage de données, Amazon Redshift ne prend pas de snapshots automatisés pendant que le cluster est suspendu.

Pour plus d'informations, consultez Instantanés automatiques.

Le type de données SUPER prend en charge les chaînes individuelles plus grandes à partir du patch 206

À partir du correctif 206, Amazon Redshift prend en charge les chaînes individuelles jusqu'à 16 000 000 octets dans le type de données SUPER (utilisé pour stocker des données semi-structurées). Cette limite s'applique également aux opérations de chaîne en mémoire. Pour utiliser cette fonctionnalité, créez un groupe de paramètres de base de données et définissez le `enable_large_strings_opt_in` paramètre sur`Yes`. Attachez ensuite le groupe de paramètres à votre entrepôt de données. Pour les clusters provisionnés, vous devez redémarrer le cluster pour appliquer la modification des paramètres.

Cette modification peut vous affecter si vous utilisez les types de données SUPER pour stocker des documents JSON volumineux. Cela peut également vous affecter si vos charges de travail reposent sur des vues `VARCHAR(MAX)` in, des fonctions définies par l'utilisateur (UDF) ou des procédures stockées qui traitent des chaînes de plus de 65 535 octets.

Lorsque vous définissez sur`Yes`, `enable_large_strings_opt_in` les opérations en mémoire sont résolues `VARCHAR(MAX)` sur`VARCHAR(16000000)`. Ces opérations incluent les vues`CAST`, les UDF et les procédures stockées. Ils peuvent ensuite traiter des chaînes de plus de 65 535 octets. Cette modification n'affecte pas le stockage persistant pour les colonnes VARCHAR. `CREATE TABLE`avec `VARCHAR(MAX)` continue à créer des `VARCHAR(65535)` colonnes. Lorsque vous définissez le paramètre surNo, Amazon Redshift préserve le comportement existant de votre entrepôt de données. Pour vérifier l'état actuel de votre entrepôt de données, exécutez`SELECT is_large_string_enabled();`.

Lorsque vous réglez `enable_large_strings_opt_in` sur `Yes` :

- `COPY`et les colonnes `INSERT` INTO SUPER prennent en charge des tailles supérieures à la limite précédente de 65 535 octets. Les fonctions de chaîne telles que `JSON_PARSE`, `JSON_SERIALIZE`, et prennent `LISTAGG` également en charge ces tailles plus grandes.
- Les vues, UDF et procédures stockées existantes restent limitées à 65 535 octets jusqu'à ce que vous les recréiez.
- Si une vue existante l'utilise `VARCHAR(MAX)` et que d'autres objets (tels que d'autres vues) en dépendent, `CREATE OR REPLACE VIEW` échoue. L'erreur est « Impossible de modifier le type de données de la colonne de vue ». Pour mettre à jour la vue, supprimez les objets dépendants, supprimez et recréez la vue, puis recréez les objets dépendants. Vous pouvez remplacer les vues qui utilisent des objets dépendants `VARCHAR(MAX)` et qui ne possèdent aucun objet dépendant sans ces étapes supplémentaires.
- Maintenez ce paramètre aligné entre les entrepôts de données du producteur et du consommateur qui partagent les données.

Lorsque vous réglez `enable_large_strings_opt_in` sur `No` :

- Vous ne pouvez pas `COPY` placer des `INSERT` chaînes de plus de 65 535 octets dans des colonnes SUPER. Vous pouvez toujours lire les chaînes existantes via SUPER. Toutefois, le transfert vers `VARCHAR(MAX)` tronque la valeur à 65 535 octets.
- Les fonctions de chaîne telles que `JSON_PARSE`, `JSON_SERIALIZE`, et ne `LISTAGG` peuvent pas traiter les valeurs VARCHAR supérieures à 65 535 octets.

- Vous ne pouvez pas interroger les vues, les procédures stockées et les UDF qui traitent des chaînes littérales de plus de 65 535 octets.
- Si vous avez créé une vue `VARCHAR(MAX)` alors que le paramètre était défini sur`Yes`, et que d'autres objets (tels que d'autres vues) en dépendent, cela `CREATE OR REPLACE VIEW` échoue avec la même erreur « Impossible de modifier le type de données de la colonne de vue ». Suivez les mêmes étapes de correction décrites dans la liste précédente.
- Une restauration instantanée entre instances peut ne pas ingérer de longues chaînes. Cet échec se produit lorsque le snapshot contient des chaînes de plus de 65 535 octets dans une colonne SUPER. Cela se produit lorsque vous restaurez cet instantané sur un cluster sur lequel ce paramètre est défini sur`No`.

Pour plus d'informations sur les versions des correctifs, consultez[Versions de cluster pour Amazon Redshift](#).

AWS KMS application des autorisations clés pour les API Amazon Redshift sans serveur après le 17 août 2026

Amazon Redshift Serverless effectue désormais une nouvelle vérification d'autorisation qui oblige le principal IAM qui appelle certaines API Amazon Redshift Serverless à obtenir des AWS KMS autorisations explicites sur la clé gérée par le client qui chiffre l'espace de noms cible. Auparavant, Amazon Redshift effectuait AWS KMS des opérations en votre nom à l'aide du rôle de service Amazon Redshift sans vérifier si le principal IAM appelant était lui-même autorisé à utiliser cette clé.

Une fois le nouveau contrôle d'autorisation activé, les appels d'API des principaux ne disposant pas des AWS KMS autorisations requises échoueront avec un `ValidationException` : Cela peut `"Insufficient KMS permissions."` vous affecter si vous avez chiffré les espaces de noms Amazon Redshift Serverless à l'aide d'une clé gérée par le client et que vous utilisez les principaux IAM pour appeler les API concernées répertoriées ci-dessous.

Pour éviter toute interruption, vérifiez quels principaux IAM de vos comptes appellent les API répertoriées ci-dessous par rapport aux espaces de noms chiffrés à l'aide d'une clé gérée par le client, et assurez-vous que ces principaux disposent des AWS KMS autorisations requises sur la clé. Vous pouvez accorder ces autorisations par le biais d'une politique AWS KMS clé, d'une stratégie basée sur l'identité IAM ou d'une subvention. AWS KMS

Cette modification n'affecte pas les espaces de noms chiffrés avec la clé AWS détenue par défaut. Si vos responsables IAM disposent déjà des AWS KMS autorisations requises répertoriées ci-dessous, aucune action n'est nécessaire.

Les API concernées et les autorisations requises sur la clé gérée par le client de l'espace de noms sont répertoriées ci-dessous :

- `CreateWorkgroup`,`RestoreFromSnapshot`, `RestoreFromRecoveryPoint` — exiger `kms:Encryptkms:GenerateDataKey`,`kms:CreateGrant`, et`kms:Decrypt`.
- `RestoreTableFromSnapshot`, `RestoreTableFromRecoveryPoint` — exiger`kms:Decrypt`.

Pour plus d'informations, consultez la section Contrôle de l'accès aux AWS KMS clés dans le Guide du AWS Key Management Service développeur. Pour plus d'informations sur le chiffrement des bases de données Amazon Redshift, consultez. Chiffrement de base de données Amazon Redshift

Amazon Redshift impose le verrouillage des utilisateurs après plusieurs tentatives de connexion infructueuses, à commencer par le patch 208

À partir d'Amazon Redshift Patch 208, afin d'améliorer le niveau de sécurité de votre entrepôt de données, Amazon Redshift verrouille automatiquement un utilisateur de base de données lorsque celui-ci dépasse le nombre configuré de tentatives de connexion infructueuses consécutives. La fonctionnalité est activée par défaut avec un seuil de 5 tentatives infructueuses (configurable de 2 à 50) et s'applique à la fois aux clusters provisionnés et aux groupes de travail sans serveur.

Cela peut vous affecter si vous vous connectez à l'aide de connexions à la base de données (basées sur un mot de passe). Une fois verrouillée, les tentatives de connexion sont rejetées, même avec le mot de passe correct, jusqu'à ce qu'un administrateur ou un superutilisateur le déverrouille. Les identités fédérées qui s'authentifient via IAM ou AWS IAM Identity Center ne sont pas concernées, car elles utilisent des jetons éphémères plutôt que des mots de passe statiques.

Pour gérer ce comportement, procédez comme suit :

- Définissez le seuil avec `ALTER SYSTEM SET max_failed_login_attempts TO` *`value`*`;` (2 à 50, 5 par défaut).
- Vérifiez l'état de verrouillage de tous les utilisateurs avec`SHOW USER LOCKOUT;`.
- Déverrouillez l'utilisateur avec`ALTER USER` *`username`* `LOGIN PASSWORD '`*`password`*`';`, ce qui réinitialise également le compteur de tentatives infructueuses.

Pour plus d'informations, consultez SHOW USER LOCKOUT, ALTER USER et max_failed_login_attempts.

Modèle de facturation amélioré pour les instantanés manuels sur les instances Amazon Redshift Serverless et Amazon Redshift RG à compter du 8 juin 2026

À compter du 8 juin 2026, Amazon Redshift annonce un modèle de facturation amélioré pour les instantanés manuels sur les instances Amazon Redshift Serverless et Amazon Redshift RG. Grâce à cette amélioration, les instantanés manuels sont désormais mesurés en fonction de blocs de données uniques stockés dans tous les instantanés manuels actifs de votre compte. Les blocs de données partagés qui apparaissent dans plusieurs instantanés ne sont comptabilisés qu'une seule fois et sont facturés aux tarifs des instantanés manuels en vigueur dans votre région.

Cela peut vous affecter si vous utilisez des instantanés manuels sur des groupes de travail Amazon Redshift Serverless ou des clusters Amazon Redshift RG. Cela se traduit par une réduction des coûts liés aux instantanés manuels pour les clients qui gèrent plusieurs instantanés.

Aucune action n’est requise. Le modèle de facturation amélioré s'applique automatiquement aux instantanés manuels existants et nouveaux.

Pour plus d'informations sur la tarification des instantanés, consultez la tarification d'Amazon Redshift.

Les tables Iceberg DELETE on Lake Formation nécessitent l'autorisation DELETE à compter du patch 202

À partir d'Amazon Redshift Patch 202, les opérations DELETE d'Iceberg sur les tables gérées par Lake Formation (LF) nécessitent l'autorisation DELETE Lake Formation. Les opérations UPDATE et MERGE nécessitent à la fois les autorisations INSERT et DELETE. Toutes les opérations DML d'Iceberg nécessitent l'autorisation ALTER.

Cela peut vous affecter si vous effectuez des opérations DELETE, UPDATE ou MERGE sur des tables Iceberg gérées par AWS Lake Formation.

Auparavant, les principaux ne disposant que de l'autorisation INSERT (et non de l'autorisation DELETE) pouvaient effectuer des opérations de suppression sur les tables LF-managed Iceberg. À partir du patch 202, les opérations DELETE nécessitent l'autorisation DELETE Lake Formation.

Les principaux qui s'appuient uniquement sur l'autorisation INSERT pour effectuer des suppressions recevront une erreur d'autorisation jusqu'à ce que l'autorisation DELETE soit explicitement accordée. Les tables S3 ne sont pas concernées par cette modification.

Pour continuer à effectuer des opérations DELETE après cette modification, passez en revue les autorisations que vous avez accordées à Lake Formation pour les tables Iceberg et assurez-vous que l'autorisation DELETE Lake Formation a été accordée aux principaux responsables des opérations de suppression. Vous pouvez vérifier les autorisations existantes à l'aide de la console AWS Lake Formation ou de la `aws lakeformation list-permissions` AWS CLI commande.

Si vous devez revenir temporairement au comportement précédent, contactez le AWS Support pour désactiver cette modification sur votre cluster sans avoir à déployer de code.

Pour plus d'informations sur les versions des correctifs, consultezVersions de cluster pour Amazon Redshift.

Amazon Redshift Serverless préserve les intégrations d'événements sans ETL et S3 lors de la restauration de snapshots à partir du correctif 202

À partir d'Amazon Redshift Patch 202, lorsque vous restaurez un espace de noms Amazon Redshift Serverless à partir d'un instantané ou d'un point de restauration vers le même espace de noms sans serveur, les intégrations d'événements Zero-ETL et S3 associées à l'espace de noms et au point sont automatiquement maintenues. snapshot/recovery Aucune action supplémentaire n'est requise.

Cela peut vous affecter si vous restaurez un instantané ou un point de restauration dans des espaces de noms Amazon Redshift Serverless sur lesquels des intégrations d'événements Zéro ETL ou S3 sont configurées.

Auparavant, la restauration d'un instantané ou d'un point de restauration dans un espace de noms sans serveur marquait les intégrations d'événements Zero-ETL et S3 associées comme ayant échoué, vous deviez les recréer manuellement une fois la restauration terminée. À partir du correctif 202, ces intégrations sont maintenues par défaut et reprennent leurs activités une fois la restauration terminée.

Cette fonctionnalité s'applique à Amazon Redshift Serverless uniquement en cas de restauration dans le même espace de noms sans serveur. La restauration d'un instantané dans un espace de noms différent ne permet pas de maintenir les intégrations. Les restaurations de snapshots sur des clusters provisionnés ne permettent pas de maintenir des intégrations d'événements S3 ou ETL nuls.

Pour refuser la maintenance des intégrations lors d'une restauration, décochez la case Maintenir les intégrations sur la page de restauration du. Console de gestion AWSSi vous utilisez le AWS CLI, définissez le `--no-maintain-integration` paramètre lorsque vous appelez l'opération d'API restore-from-snapshot ou restore-from-recovery-point. Lorsque vous vous désinscrivez, les intégrations entrent dans l'`FAILED`état après la restauration. Vous pouvez ensuite supprimer les intégrations qui ont échoué et les recréer.

Pour plus d'informations sur les versions des correctifs, consultezVersions de cluster pour Amazon Redshift.

Fin du support pour le pilote ODBC 1.x Amazon Redshift le 31 décembre 2026

À compter du 31 décembre 2026, Amazon Redshift cessera de prendre en charge le pilote ODBC 1.x. Sur la base des commentaires des clients, nous avons prolongé la date initiale de fin du support du 30 septembre 2026 au 31 décembre 2026, afin de prolonger le délai de migration. Cela s’applique à la fois aux clusters alloués par Amazon Redshift et aux groupes de travail sans serveur.

Cela peut vous affecter si vous utilisez une version quelconque du pilote ODBC 1.x pour vous connecter à Amazon Redshift. Pour vérifier si vous utilisez un pilote ODBC 1.x, exécutez la requête suivante :

```
SELECT *
FROM SYS_CONNECTION_LOG
WHERE
(driver_version ilike 'Amazon Redshift ODBC Driver 1%'
OR driver_version ilike 'Redshift ODBC Driver 01%'
OR driver_version ilike 'Redshift ODBC Driver 1,%'
)
OR
(application_name ilike 'Amazon Redshift ODBC Driver 1%');
```

Pour continuer à bénéficier du support technique pour vos connexions au pilote ODBC Amazon Redshift, veuillez migrer vers le dernier pilote ODBC Amazon Redshift 2.x avant le 30 décembre 2026.

Avant de migrer vers le pilote ODBC 2.x dans un environnement de production, nous vous recommandons de procéder à une validation de principe approfondie afin de vérifier que le nouveau pilote répond à toutes vos exigences fonctionnelles.

Nous vous recommandons d'utiliser la dernière version du pilote ODBC 2.x Amazon Redshift et de définir la ApplicationNamepropriété pour identifier votre application lors de la connexion à Amazon Redshift.

Les fonctions scalaires Python définies par l'utilisateur ne seront plus prises en charge après le 30 juin 2026

Amazon Redshift ne prendra plus en charge les fonctions scalaires Python définies par l'utilisateur après le 30 juin 2026. En guise d'alternative, nous vous recommandons d'utiliser les fonctions Lambda définies par l'utilisateur.

Les fonctions Lambda définies par l'utilisateur présentent les avantages suivants par rapport aux fonctions Python :

- Les fonctions Lambda définies par l'utilisateur peuvent se connecter à des services externes et à des API à partir de la logique des fonctions définies par l'utilisateur.
- Les fonctions Lambda définies par l'utilisateur utilisent des ressources de calcul Lambda. Les fonctions Lambda définies par l'utilisateur gourmandes en calcul ou en mémoire n'ont aucun impact sur les performances des requêtes d'Amazon Redshift ni sur la simultanéité des ressources.
- Les fonctions Lambda définies par l'utilisateur prennent en charge l'exécution de code Python. Les fonctions Lambda définies par l'utilisateur prennent en charge plusieurs environnements d'exécution Python en fonction de cas d'utilisation spécifiques. Pour plus d'informations, consultez Création avec Python dans le Guide du développeur AWS Lambda .
- Vous pouvez isoler l'exécution de code personnalisé dans une limite de service distincte. Cela simplifie la maintenance, la surveillance, la budgétisation et la gestion des autorisations.

Pour plus d'informations sur la création et l'utilisation des fonctions Lambda définies par l'utilisateur, consultez la section Fonctions scalaires Lambda définies par l'utilisateur dans le Guide du développeur de base de données Amazon Redshift. Pour plus d'informations sur la conversion des fonctions Python définies par l'utilisateur existantes en fonctions Lambda définies par l'utilisateur, consultez le billet de blog.

Modification du Auto-REFRESH comportement de la vue matérialisée (MV) après le 27 février 2026

À compter du 27 février 2026, les requêtes Auto REFRESH pour les vues matérialisées Amazon Redshift sont exécutées en tant que requêtes utilisateur plutôt que sous forme de processus

autonomes en arrière-plan. Par conséquent, les requêtes Auto REFRESH sont désormais exécutées avec la même priorité que les autres requêtes utilisateur.

Cette modification améliore la fraîcheur des vues matérialisées grâce à l'activation de l'actualisation automatique, ce qui les aide à rester mieux informées des dernières modifications apportées à leurs tables de base par rapport au comportement précédent.

Remarque : La fonctionnalité de modification du comportement MV Auto REFRESH n'est activée que pour les clusters provisionnés Amazon Redshift sur la version ACTUELLE du correctif P198 et versions ultérieures. Il est actuellement désactivé sur Serverless.

Amazon Redshift ne prendra pas en charge les fonctions permettant d’accéder aux informations des consommateurs via l’unité de partage des données après le 16 février 2026

À compter du 16 février 2026, Amazon Redshift ne prendra plus en charge l’utilisation de `user_is_member_of` et des fonctions associées permettant d’accéder aux informations relatives aux utilisateurs, aux rôles ou aux groupes des consommateurs via l’unité de partage des données.

Modifications apportées à la version du protocole TLS (Minimum Transport Layer Security) à compter du 31 octobre 2026

À compter du 31 octobre 2026, Amazon Redshift appliquera une version TLS (Transport Layer Security) minimale de 1.2. Les connexions entrantes qui utilisent les versions 1.0 ou 1.1 du protocole TLS (Transport Layer Security) seront rejetées. Cela s’applique à la fois aux clusters alloués par Amazon Redshift et aux groupes de travail sans serveur. Les entrepôts de données Amazon Redshift n’utilisant pas le protocole TLS ne seront pas affectés par cette modification.

Cette mise à jour peut vous affecter si vous utilisez les versions TLS 1.0 ou 1.1 pour vous connecter à Amazon Redshift.

Pour vérifier la version de TLS que vous utilisez actuellement, vous pouvez :

Pour un cluster alloué Amazon Redshift : consultez la colonne sslversion dans la table système STL_CONNECTION_LOG [1].

Pour un groupe de travail Amazon Redshift sans serveur : consultez la colonne ssl_version dans la table système SYS_CONNECTION_LOG [2].

Pour conserver un accès ininterrompu à votre entrepôt de données Amazon Redshift après cette modification, veuillez suivre les étapes ci-dessous :

1. Mettez à jour votre client pour prendre en charge le protocole TLS 1.2 ou une version ultérieure
2. Installer la dernière version de pilote avec prise en charge du protocole TLS 1.2+

Dans la mesure du possible, nous vous recommandons d'utiliser la dernière version du pilote Amazon Redshift [3].

[1] https://docs.aws.amazon.com/redshift/latest/dg/r_STL_CONNECTION_LOG.html

[2] https://docs.aws.amazon.com/redshift/latest/dg/SYS_CONNECTION_LOG.html

[3] https://docs.aws.amazon.com/redshift/latest/mgmt/configuring-connections.html

Amazon Redshift ne prendra pas en charge la création de nouvelles fonctions scalaires Python définies par l'utilisateur après le 30 octobre 2025

Amazon Redshift ne prendra plus en charge la création de nouvelles fonctions Python définies par l'utilisateur après le 30 octobre 2025. Les fonctions Python définies par l'utilisateur existantes continueront de fonctionner normalement. Nous vous recommandons fortement de migrer vos fonctions Python définies par l'utilisateur existantes vers des fonctions Lambda définies par l'utilisateur avant cette date.

Les fonctions Lambda définies par l'utilisateur présentent les avantages suivants par rapport aux fonctions Python :

- Les fonctions Lambda définies par l'utilisateur peuvent se connecter à des services externes et à des API à partir de la logique des fonctions définies par l'utilisateur.
- Les fonctions Lambda définies par l'utilisateur utilisent des ressources de calcul Lambda. Les fonctions Lambda définies par l'utilisateur gourmandes en calcul ou en mémoire n'ont aucun impact sur les performances des requêtes d'Amazon Redshift ni sur la simultanéité des ressources.
- Les fonctions Lambda définies par l'utilisateur prennent en charge l'exécution de code Python. Les fonctions Lambda définies par l'utilisateur prennent en charge plusieurs environnements d'exécution Python en fonction de cas d'utilisation spécifiques. Pour plus d'informations, consultez Création avec Python dans le Guide du développeur AWS Lambda .
- Vous pouvez isoler l'exécution de code personnalisé dans une limite de service distincte. Cela simplifie la maintenance, la surveillance, la budgétisation et la gestion des autorisations.

Pour plus d'informations sur la création et l'utilisation des fonctions Lambda définies par l'utilisateur, consultez la section Fonctions scalaires Lambda définies par l'utilisateur dans le Guide du développeur de base de données Amazon Redshift. Pour plus d'informations sur la conversion des fonctions Python définies par l'utilisateur existantes en fonctions Lambda définies par l'utilisateur, consultez le billet de blog.

Changements de comportement récents

Rubriques

- Amazon Redshift utilise la base de données de fuseaux horaires IANA à jour après le 26 août 2025
- Les modifications apportées aux unités de traitement Redshift (RPU) Amazon Redshift sans serveur entreront en vigueur après le 15 août 2025
- Modifications apportées à la journalisation des audits de base de données en vigueur après le 10 août 2025
- Modifications apportées au point de terminaison du cloud privé virtuel pour les groupes de travail sans serveur à compter du 27 juin 2025
- Les modifications apportées à la surveillance des requêtes entreront en vigueur après le 2 mai 2025
- Changements de sécurité en vigueur après le 10 janvier 2025

Amazon Redshift utilise la base de données de fuseaux horaires IANA à jour après le 26 août 2025

À compter du 26 août 2025, Amazon Redshift calcule les fuseaux horaires en adoptant les derniers correctifs de la base de données des fuseaux horaires de l'IANA. Cette modification modifie le fonctionnement des conversions de date et d'heure pour certains fuseaux horaires et certaines périodes. Cette mise à jour concerne les conversions de fuseaux horaires explicites, telles que celles effectuées avec la fonction CONVERT_TIMEZONE ou les commandes TIMEZONE et AT TIME ZONE, ainsi que les conversions implicites qui se produisent lors des opérations de changement de type, en particulier entre les formats TIMESTAMP et TIMESTAMPTZ.

Voici une liste des mises à jour pour les combinaisons de fuseaux horaires et de périodes :

- Les fuseaux horaires respectent désormais correctement l'heure d'été (DST) après 2038. Auparavant, aucun fuseau horaire n'était observé après 2038.

- Le fuseau horaire `America/Toronto`, et les fuseaux horaires qui y sont liés, changent pour l'heure d'été en 1947-1950 à 2 heures du matin, heure locale, au lieu de minuit.
- Amazon Redshift reflète désormais correctement l'heure moyenne locale (LMT) pour les périodes avant la standardisation pour tous les fuseaux horaires. Cette période est spécifique à un fuseau horaire, la plupart des fuseaux horaires passant à la normalisation avant le milieu du XIXe siècle.
- `EET`, `CET`, `WET` et `MET` sont désormais traités comme des fuseaux horaires normaux plutôt que comme des abréviations.
- Les noms de fuseaux horaires suivants n'existent plus dans Amazon Redshift :
  - `Asia/Riyadh87`
  - `Asia/Riyadh88`
  - `Asia/Riyadh89`
  - `Mideast/Riyadh87`
  - `Mideast/Riyadh88`
  - `Mideast/Riyadh89`
  - `US/Pacific-New`

Pour plus d'informations sur la base de données des fuseaux horaires de l'IANA, consultez Base de données des fuseaux horaires sur le site Web de la base de données des fuseaux horaires de l'IANA.

Les modifications apportées aux unités de traitement Redshift (RPU) Amazon Redshift sans serveur entreront en vigueur après le 15 août 2025

À compter du 15 août 2025, le quota de AWS comptes pour les unités de traitement Redshift de base (RPU) Amazon Redshift sans serveur est égal à 3 200 RPU ou à 1,5 fois le maximum des RPU de base agrégées des six mois précédents.

Modifications apportées à la journalisation des audits de base de données en vigueur après le 10 août 2025

À compter du 10 août 2025, Amazon Redshift apporte une modification à la journalisation des audits de base de données, ce qui nécessite votre intervention. Amazon Redshift enregistre les informations relatives aux connexions et aux activités des utilisateurs dans votre base de données dans des compartiments Amazon S3 et. CloudWatch Après le 10 août 2025, Amazon Redshift cessera de consigner les audits de base de données dans vos compartiments Amazon S3 dotés d'une stratégie

de compartiment spécifiant un utilisateur Redshift IAM. Nous vous recommandons de mettre à jour vos politiques pour utiliser le Redshift à la SERVICE-PRINCIPAL place, dans le cadre des politiques du compartiment S3 pour la journalisation des audits. Pour plus d'informations sur la journalisation, consultez Autorisations du compartiment pour la journalisation des audits Amazon Redshift.

Pour éviter toute interruption de journalisation, passez en revue et mettez à jour vos stratégies relatives aux compartiments S3 afin d'accorder l'accès au principal de service Redshift dans la région associée avant le 10 août 2025. Pour plus d'informations sur la journalisation des audits de base de données, consultez Fichiers journaux dans Amazon S3.

Pour toute question ou préoccupation, contactez le AWS support via le lien suivant : AWS Support.

Modifications apportées au point de terminaison du cloud privé virtuel pour les groupes de travail sans serveur à compter du 27 juin 2025

À compter du 27 juin 2025, Amazon Redshift apporte une modification à la prise en charge des points de terminaison du cloud privé virtuel (VPCE) pour les groupes de travail sans serveur. Avant cette date, Amazon Redshift se déploie avec des points de terminaison dans une seule zone de disponibilité (AZ) lors de la création du groupe de travail, et étend la prise en charge des points de terminaison du cloud privé virtuel (VPCE) jusqu'à trois zones de disponibilité au fil du temps. Après cette date, Amazon Redshift déploie les points de terminaison du cloud privé virtuel (VPCE) dans un maximum de trois des zones de disponibilité spécifiées lors de la création du groupe de travail.

Pour plus d'informations, consultez Considérations relatives à l'utilisation d'Amazon Redshift sans serveur.

Pour toute question ou préoccupation, contactez le AWS support via le lien suivant : AWS Support.

Rubriques

- Les modifications apportées à la surveillance des requêtes entreront en vigueur après le 2 mai 2025
- Changements de sécurité en vigueur après le 10 janvier 2025

Les modifications apportées à la surveillance des requêtes entreront en vigueur après le 2 mai 2025

À compter du 2 mai 2025, nous ne proposerons plus les métriques Temps UC de la requête (`max_query_cpu_time`) et Utilisation UC de la requête (`max_query_cpu_percentage`)

dans l'onglet Limites de requête pour les groupes de travail Redshift sans serveur existants et nouvellement créés. Après cette date, nous supprimerons automatiquement toutes les limites de requête basées sur ces métriques dans tous les groupes de travail Redshift sans serveur.

Les limites de requête sont conçues pour intercepter les requêtes intempestives. Cependant, le temps UC de la requête (`max_query_cpu_time`) et l'utilisation UC de la requête (`max_query_cpu_percentage`) peuvent varier au cours de la durée de vie de la requête et ne constituent donc pas une méthode toujours efficace pour intercepter les requêtes intempestives. Pour détecter les requêtes intempestives, nous vous recommandons de tirer parti des métriques de surveillance des requêtes qui fournissent des informations cohérentes et exploitables. Voici quelques exemples :

- Durée d'exécution des requêtes (`max_query_execution_time`) : pour garantir que les requêtes sont terminées dans les délais prévus.
- Nombre de lignes renvoyées (`max_scan_row_count`) : pour surveiller l'échelle des données traitées.
- Durée de la file d'attente des requêtes (`max_query_queue_time`) : pour identifier les requêtes qui passent du temps à dans la file d'attente.

Pour obtenir la liste complète des métriques prises en charge, consultez Métriques de surveillance des requêtes pour Amazon Redshift sans serveur.

Changements de sécurité en vigueur après le 10 janvier 2025

Chez Amazon Web Services (AWS), la sécurité est notre priorité principale. À cette fin, nous renforçons encore le niveau de sécurité des environnements Amazon Redshift en introduisant des paramètres de sécurité améliorés qui vous aident à respecter les bonnes pratiques en matière de sécurité des données sans nécessiter de configuration supplémentaire et à réduire le risque de mauvaise configuration. Pour éviter toute interruption potentielle, passez en revue les configurations, les scripts et les outils de création de clusters alloués et de groupes de travail sans serveur afin d'apporter les modifications nécessaires et les aligner sur les nouveaux paramètres par défaut avant la date d'entrée en vigueur.

Accès public désactivé par défaut

Après le 10 janvier 2025, l'accessibilité publique sera désactivée par défaut pour tous les clusters alloués nouvellement créés et pour les clusters restaurés à partir d'instantanés. Dans cette version,

par défaut, les connexions aux clusters ne seront autorisées qu'à partir d'applications clientes au sein d'un même cloud privé virtuel (VPC). Pour accéder à votre entrepôt de données depuis les applications d'un autre VPC, configurez l'accès inter-VPC. Cette modification se reflétera dans les opérations d'API `CreateCluster` et `RestoreFromClusterSnapshot`, ainsi que dans les commandes SDK et AWS CLI correspondantes. Si vous créez un cluster alloué à partir de la console Amazon Redshift, l'accès public au cluster est désactivé par défaut.

Si vous avez toujours besoin d'un accès public, vous devrez remplacer la valeur par défaut et définir le paramètre `PubliclyAccessible` sur true lorsque vous exécutez des opérations d'API `CreateCluster` ou `RestoreFromClusterSnapshot`. Dans le cas d'un cluster publiquement accessible, nous vous recommandons d'utiliser des groupes de sécurité ou des listes de contrôle d'accès (ACL) réseau pour restreindre l'accès. Pour plus d'informations, consultez Groupes de sécurité VPC et Configuration des paramètres de communication des groupes de sécurité pour un cluster Amazon Redshift ou un groupe de travail Amazon Redshift sans serveur.

Chiffrement par défaut

Après le 10 janvier 2025, Amazon Redshift améliorera encore la sécurité des données et des clusters en activant le chiffrement comme paramètre par défaut pour tous les clusters alloués Amazon Redshift nouvellement créés. Cela ne s'applique pas aux clusters restaurés à partir d'instantanés.

Avec cette modification, la possibilité de déchiffrer les clusters ne sera plus disponible lors de l'utilisation de l'API Console de gestion AWS AWS CLI, ou pour créer un cluster provisionné sans spécifier de clé KMS. Le cluster sera automatiquement chiffré avec un Clé détenue par AWS.

Cette mise à jour peut avoir un impact sur vous si vous créez des clusters non chiffrés à l'aide de scripts automatisés ou si vous exploitez le partage de données avec des clusters non chiffrés. Pour garantir une transition fluide, mettez à jour vos scripts qui créent des clusters non chiffrés. En outre, si vous créez régulièrement de nouveaux clusters de consommateurs non chiffrés et que vous les utilisez pour le partage de données, revoyez vos configurations pour vous assurer que les clusters de producteurs et de consommateurs sont tous deux chiffrés, afin d'éviter toute interruption de vos activités de partage de données. Pour plus d'informations, consultez Chiffrement de base de données Amazon Redshift.

Application des connexions SSL

Après le 10 janvier 2025, Amazon Redshift appliquera les connexions SSL par défaut pour les clients se connectant à des clusters alloués et restaurés récemment créés. Cette modification par défaut s'appliquera également aux groupes de travail sans serveur.

Avec cette modification, un nouveau groupe de paramètres par défaut nommé `default.redshift-2.0` sera introduit pour tous les clusters nouvellement créés ou restaurés, le paramètre `require_ssl` étant défini sur `true` par défaut. Tout nouveau cluster créé sans groupe de paramètres spécifié utilisera automatiquement le groupe de paramètres `default.redshift-2.0`. Lors de la création d'un cluster via la console Amazon Redshift, le nouveau groupe de paramètres `default.redshift-2.0` est automatiquement sélectionné. Cette modification se reflétera également dans les opérations de `RestoreFromClusterSnapshot` l'API `CreateCluster` et dans le SDK et AWS CLI les commandes correspondants. Si vous utilisez des groupes de paramètres existants ou personnalisés, Amazon Redshift continuera à respecter la valeur `require_ssl` spécifiée dans votre groupe de paramètres. Vous avez toujours la possibilité de modifier la valeur `require_ssl` de vos groupes de paramètres personnalisés selon vos besoins.

Pour les utilisateurs d'Amazon Redshift sans serveur, la valeur par défaut de `require_ssl` dans les `config-parameters` sera remplacée par `true`. Toute demande de création de nouveaux groupes de travail avec la valeur `require_ssl` définie sur `false` sera rejetée. Vous pouvez modifier la valeur `require_ssl` sur `false` après la création du groupe de travail. Pour plus d'informations, consultez Configuration des options de sécurité des connexions.

Notez que vous aurez toujours la possibilité de modifier les paramètres du cluster ou du groupe de travail pour modifier le comportement par défaut, si cela s'avère nécessaire pour vos cas d'utilisation spécifiques.

Exemples de code pour Amazon Redshift à l'aide de AWS Kits SDK

Les exemples de code suivants montrent comment utiliser Amazon Redshift avec un kit de développement AWS logiciel (SDK).

Les principes de base sont des exemples de code qui vous montrent comment effectuer les opérations essentielles au sein d'un service.

Les actions sont des extraits de code de programmes plus larges et doivent être exécutées dans leur contexte. Alors que les actions vous indiquent comment appeler des fonctions de service individuelles, vous pouvez les voir en contexte dans leurs scénarios associés.

Les scénarios sont des exemples de code qui vous montrent comment accomplir des tâches spécifiques en appelant plusieurs fonctions au sein d'un même service ou combinés à d'autres Services AWS.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezL'utilisation de ce service avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit de développement logiciel (SDK).

Exemples de code

- Exemples de base pour l'utilisation d'Amazon Redshift AWS Kits SDK
  - Bonjour Amazon Redshift
  - Découvrez les bases d'Amazon Redshift grâce à AWS Kit SDK
  - Actions pour Amazon Redshift utilisant AWS Kits SDK
    - À utiliser CreateClusteravec un AWS SDK ou CLI
    - À utiliser DeleteClusteravec un AWS SDK ou CLI
    - À utiliser DescribeClustersavec un AWS SDK ou CLI
    - À utiliser DescribeStatementavec un AWS Kit SDK
    - À utiliser ExecuteStatementavec un AWS Kit SDK
    - À utiliser GetStatementResultavec un AWS Kit SDK
    - À utiliser ListDatabasesavec un AWS Kit SDK

    - À utiliser ModifyClusteravec un AWS SDK ou CLI
- Scénarios d'utilisation d'Amazon Redshift AWS Kits SDK
    - Créer un outil de suivi des éléments Amazon Redshift.
    - Commencez avec les entrepôts de données sans serveur à l'aide de la CLI
    - Commencer à utiliser des clusters d'entrepôts de données provisionnés

Exemples de base pour l'utilisation d'Amazon Redshift AWS Kits SDK

Les exemples de code suivants montrent les bases de l'utilisation d'Amazon Redshift avec des kits AWS SDK.

Exemples

- Bonjour Amazon Redshift
- Découvrez les bases d'Amazon Redshift grâce à AWS Kit SDK
- Actions pour Amazon Redshift utilisant AWS Kits SDK
    - À utiliser CreateClusteravec un AWS SDK ou CLI
    - À utiliser DeleteClusteravec un AWS SDK ou CLI
    - À utiliser DescribeClustersavec un AWS SDK ou CLI
    - À utiliser DescribeStatementavec un AWS Kit SDK
    - À utiliser ExecuteStatementavec un AWS Kit SDK
    - À utiliser GetStatementResultavec un AWS Kit SDK
    - À utiliser ListDatabasesavec un AWS Kit SDK
    - À utiliser ModifyClusteravec un AWS SDK ou CLI

Bonjour Amazon Redshift

Les exemples de code suivants montrent comment démarrer avec Amazon Redshift.

.NET

SDK pour .NET (v4)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Main method to run the Hello Amazon Redshift example.
    /// </summary>
    /// <param name="args">Command line arguments (not used).</param>
    public static async Task Main(string[] args)
    {
        var redshiftClient = new AmazonRedshiftClient();

        Console.WriteLine("Hello, Amazon Redshift! Let's list available
clusters:");

        var clusters = new List<Cluster>();

        try
        {
            // Use pagination to retrieve all clusters.
            var clustersPaginator =
redshiftClient.Paginators.DescribeClusters(new DescribeClustersRequest());

            await foreach (var response in clustersPaginator.Responses)
            {
                if (response.Clusters != null)
                    clusters.AddRange(response.Clusters);
            }

            Console.WriteLine($"{clusters.Count} cluster(s) retrieved.");

            foreach (var cluster in clusters)
            {
                Console.WriteLine($"\t{cluster.ClusterIdentifier} (Status:
{cluster.ClusterStatus})");
            }
```

```
        }
        catch (AmazonRedshiftException ex)
        {
            Console.WriteLine($"Couldn't list clusters. Here's why:
 {ex.Message}");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred: {ex.Message}");
        }
    }
```

- Pour plus de détails sur l'API, voir DescribeClustersla section Référence des AWS SDK pour .NET API.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
package main

import (
 "context"
 "fmt"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/redshift"
)

// main uses the AWS SDK for Go V2 to create a Redshift client
// and list up to 10 clusters in your account.
// This example uses the default settings specified in your shared credentials
```

```
// and config files.
func main() {
 ctx := context.Background()
 sdkConfig, err := config.LoadDefaultConfig(ctx)
 if err != nil {
  fmt.Println("Couldn't load default configuration. Have you set up your AWS
 account?")
  fmt.Println(err)
  return
 }
 redshiftClient := redshift.NewFromConfig(sdkConfig)
 count := 20
 fmt.Printf("Let's list up to %v clusters for your account.\n", count)
 result, err := redshiftClient.DescribeClusters(ctx,
 &redshift.DescribeClustersInput{
  MaxRecords: aws.Int32(int32(count)),
 })
 if err != nil {
  fmt.Printf("Couldn't list clusters for your account. Here's why: %v\n", err)
  return
 }
 if len(result.Clusters) == 0 {
  fmt.Println("You don't have any clusters!")
  return
 }
 for _, cluster := range result.Clusters {
  fmt.Printf("\t%v : %v\n", *cluster.ClusterIdentifier, *cluster.ClusterStatus)
 }
}
```

- Pour plus de détails sur l'API, voir DescribeClusterslа section Référence des AWS SDK pour Go API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.redshift.RedshiftClient;
import
 software.amazon.awssdk.services.redshift.paginators.DescribeClustersIterable;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class HelloRedshift {
    public static void main(String[] args) {
        Region region = Region.US_EAST_1;
        RedshiftClient redshiftClient = RedshiftClient.builder()
            .region(region)
            .build();

        listClustersPaginator(redshiftClient);
    }

    public static void listClustersPaginator(RedshiftClient redshiftClient) {
        DescribeClustersIterable clustersIterable =
 redshiftClient.describeClustersPaginator();
        clustersIterable.stream()
            .flatMap(r -> r.clusters().stream())
            .forEach(cluster -> System.out
                .println(" Cluster identifier: " + cluster.clusterIdentifier() +
 " status = " + cluster.clusterStatus()));
```

```
    }
}
```

- Pour plus de détails sur l'API, voir DescribeClustersla section Référence des AWS SDK for Java 2.x API.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import boto3


def hello_redshift(redshift_client):
    """
    Use the AWS SDK for Python (Boto3) to create an Amazon Redshift client and
 list
    the clusters in your account. This list might be empty if you haven't created
    any clusters.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param redshift_client: A Boto3 Redshift Client object.
    """
    print("Hello, Redshift! Let's list your clusters:")
    paginator = redshift_client.get_paginator("describe_clusters")
    clusters = []
    for page in paginator.paginate():
        clusters.extend(page["Clusters"])

    print(f"{len(clusters)} cluster(s) were found.")

    for cluster in clusters:
        print(f"  {cluster['ClusterIdentifier']}")
```

```
if __name__ == "__main__":
    hello_redshift(boto3.client("redshift"))
```

- Pour plus de détails sur l'API, consultez DescribeClustersle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezL'utilisation de ce service avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Découvrez les bases d'Amazon Redshift grâce à AWS Kit SDK

Les exemples de code suivants montrent comment :

- créer un cluster Redshift ;
- Répertoriez les bases de données du cluster.
- Créez une table intitulée Films.
- Renseignez la table Films.
- Interrogez la table Films par année.
- Modifiez le cluster Redshift.
- Supprimez le cluster Amazon Redshift.

.NET

SDK pour .NET (v4)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez une classe d'enveloppe Redshift pour gérer les opérations.

```
/// <summary>
```

```
/// Wrapper class for Amazon Redshift operations.
/// </summary>
public class RedshiftWrapper
{
    private readonly IAmazonRedshift _redshiftClient;
    private readonly IAmazonRedshiftDataAPIService _redshiftDataClient;

    /// <summary>
    /// Constructor for RedshiftWrapper.
    /// </summary>
    /// <param name="redshiftClient">Amazon Redshift client.</param>
    /// <param name="redshiftDataClient">Amazon Redshift Data API client.</param>
    public RedshiftWrapper(IAmazonRedshift redshiftClient,
 IAmazonRedshiftDataAPIService redshiftDataClient)
    {
        _redshiftClient = redshiftClient;
        _redshiftDataClient = redshiftDataClient;
    }

    /// <summary>
    /// Create a new Amazon Redshift cluster.
    /// </summary>
    /// <param name="clusterIdentifier">The identifier for the cluster.</param>
    /// <param name="databaseName">The name of the database.</param>
    /// <param name="masterUsername">The master username.</param>
    /// <param name="masterUserPassword">The master user password.</param>
    /// <param name="nodeType">The node type for the cluster.</param>
    /// <returns>The cluster that was created.</returns>
    public async Task<Cluster> CreateClusterAsync(string clusterIdentifier,
 string databaseName,
        string masterUsername, string masterUserPassword, string nodeType =
 "ra3.large")
    {
        try
        {
            var request = new CreateClusterRequest
            {
                ClusterIdentifier = clusterIdentifier,
                DBName = databaseName,
                MasterUsername = masterUsername,
                MasterUserPassword = masterUserPassword,
                NodeType = nodeType,
                NumberOfNodes = 1,
                ClusterType = "single-node"
```

```
            };

            var response = await _redshiftClient.CreateClusterAsync(request);
            Console.WriteLine($"Created cluster {clusterIdentifier}");
            return response.Cluster;
        }
        catch (ClusterAlreadyExistsException ex)
        {
            Console.WriteLine($"Cluster already exists: {ex.Message}");
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't create cluster. Here's why:
{ex.Message}");
            throw;
        }
    }

    /// <summary>
    /// Describe Amazon Redshift clusters.
    /// </summary>
    /// <param name="clusterIdentifier">Optional cluster identifier to describe a
specific cluster.</param>
    /// <returns>A list of clusters.</returns>
    public async Task<List<Cluster>> DescribeClustersAsync(string?
clusterIdentifier = null)
    {
        try
        {
            var clusters = new List<Cluster>();
            var request = new DescribeClustersRequest();
            if (!string.IsNullOrEmpty(clusterIdentifier))
            {
                request.ClusterIdentifier = clusterIdentifier;
            }

            var clustersPaginator =
_redshiftClient.Paginators.DescribeClusters(request);
            await foreach (var response in clustersPaginator.Responses)
            {
                if (response.Clusters != null)
                    clusters.AddRange(response.Clusters);
            }
```

```
            Console.WriteLine($"{clusters.Count} cluster(s) retrieved.");
            foreach (var cluster in clusters)
            {
                Console.WriteLine($"\t{cluster.ClusterIdentifier} (Status:
{cluster.ClusterStatus})");
            }

            return clusters;
        }
        catch (ClusterNotFoundException ex)
        {
            Console.WriteLine($"Cluster {clusterIdentifier} not found:
{ex.Message}");
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't describe clusters. Here's why:
{ex.Message}");
            throw;
        }
    }

    /// <summary>
    /// Modify an Amazon Redshift cluster.
    /// </summary>
    /// <param name="clusterIdentifier">The identifier for the cluster.</param>
    /// <param name="preferredMaintenanceWindow">The preferred maintenance
window.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> ModifyClusterAsync(string clusterIdentifier, string
preferredMaintenanceWindow)
    {
        try
        {
            var request = new ModifyClusterRequest
            {
                ClusterIdentifier = clusterIdentifier,
                PreferredMaintenanceWindow = preferredMaintenanceWindow
            };

            var response = await _redshiftClient.ModifyClusterAsync(request);
```

```
            Console.WriteLine($"The modified cluster was successfully modified
and has {response.Cluster.PreferredMaintenanceWindow} as the maintenance
window");
            return true;
        }
        catch (ClusterNotFoundException ex)
        {
            Console.WriteLine($"Cluster {clusterIdentifier} not found:
{ex.Message}");
            return false;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't modify cluster. Here's why:
{ex.Message}");
            return false;
        }
    }

    /// <summary>
    /// Delete an Amazon Redshift cluster without a final snapshot.
    /// </summary>
    /// <param name="clusterIdentifier">The identifier for the cluster.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteClusterWithoutSnapshotAsync(string
clusterIdentifier)
    {
        try
        {
            var request = new DeleteClusterRequest
            {
                ClusterIdentifier = clusterIdentifier,
                SkipFinalClusterSnapshot = true
            };

            var response = await _redshiftClient.DeleteClusterAsync(request);
            Console.WriteLine($"The {clusterIdentifier} was deleted");
            return true;
        }
        catch (ClusterNotFoundException ex)
        {
            Console.WriteLine($"Cluster not found: {ex.Message}");
            return false;
        }
```

```
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't delete cluster. Here's why:
{ex.Message}");
            return false;
        }
    }

    /// <summary>
    /// List databases in a Redshift cluster.
    /// </summary>
    /// <param name="clusterIdentifier">The cluster identifier.</param>
    /// <param name="dbUser">The database user.</param>
    /// <param name="dbUser">The database name for authentication.</param>
    /// <returns>A list of database names.</returns>
    public async Task<List<string>> ListDatabasesAsync(string clusterIdentifier,
string dbUser, string databaseName)
    {
        try
        {
            var request = new ListDatabasesRequest
            {
                ClusterIdentifier = clusterIdentifier,
                DbUser = dbUser,
                Database = databaseName
            };

            var response = await _redshiftDataClient.ListDatabasesAsync(request);
            var databases = new List<string>();

            foreach (var database in response.Databases)
            {
                Console.WriteLine($"The database name is : {database}");
                databases.Add(database);
            }

            return databases;
        }
        catch (Amazon.RedshiftDataAPIService.Model.ValidationException ex)
        {
            Console.WriteLine($"Validation error: {ex.Message}");
            throw;
        }
        catch (Exception ex)
```

```
        {
            Console.WriteLine($"Couldn't list databases. Here's why:
{ex.Message}");
            throw;
        }
    }

    /// <summary>
    /// Create a table in the Redshift database.
    /// </summary>
    /// <param name="clusterIdentifier">The cluster identifier.</param>
    /// <param name="database">The database name.</param>
    /// <param name="dbUser">The database user.</param>
    /// <returns>The statement ID.</returns>
    public async Task<string> CreateTableAsync(string clusterIdentifier, string
database, string dbUser)
    {
        try
        {
            var sqlStatement = @"
                CREATE TABLE Movies (
                    id INTEGER PRIMARY KEY,
                    title VARCHAR(250) NOT NULL,
                    year INTEGER NOT NULL
                )";

            var request = new ExecuteStatementRequest
            {
                ClusterIdentifier = clusterIdentifier,
                Database = database,
                DbUser = dbUser,
                Sql = sqlStatement
            };

            var response = await
_redshiftDataClient.ExecuteStatementAsync(request);
            await WaitForStatementToCompleteAsync(response.Id);
            Console.WriteLine("Table created: Movies");
            return response.Id;
        }
        catch (Amazon.RedshiftDataAPIService.Model.ValidationException ex)
        {
            Console.WriteLine($"Validation error: {ex.Message}");
            throw;
```

```
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't create table. Here's why:
{ex.Message}");
            throw;
        }
    }

    /// <summary>
    /// Insert a record into the Movies table using parameterized query.
    /// </summary>
    /// <param name="clusterIdentifier">The cluster identifier.</param>
    /// <param name="database">The database name.</param>
    /// <param name="dbUser">The database user.</param>
    /// <param name="id">The movie ID.</param>
    /// <param name="title">The movie title.</param>
    /// <param name="year">The movie year.</param>
    /// <returns>The statement ID.</returns>
    public async Task<string> InsertMovieAsync(string clusterIdentifier, string
database, string dbUser,
        int id, string title, int year)
    {
        try
        {
            var sqlStatement = "INSERT INTO Movies (id, title, year) VALUES
(:id, :title, :year)";

            var request = new ExecuteStatementRequest
            {
                ClusterIdentifier = clusterIdentifier,
                Database = database,
                DbUser = dbUser,
                Sql = sqlStatement,
                Parameters = new List<SqlParameter>
                {
                    new SqlParameter { Name = "id", Value = id.ToString() },
                    new SqlParameter { Name = "title", Value = title },
                    new SqlParameter { Name = "year", Value = year.ToString() }
                }
            };

            var response = await
_redshiftDataClient.ExecuteStatementAsync(request);
```

```
            await WaitForStatementToCompleteAsync(response.Id);
            Console.WriteLine($"Inserted: {title} ({year})");
            return response.Id;
        }
        catch (Amazon.RedshiftDataAPIService.Model.ValidationException ex)
        {
            Console.WriteLine($"Validation error: {ex.Message}");
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't insert movie. Here's why:
{ex.Message}");
            throw;
        }
    }

    /// <summary>
    /// Query movies by year using parameterized query.
    /// </summary>
    /// <param name="clusterIdentifier">The cluster identifier.</param>
    /// <param name="database">The database name.</param>
    /// <param name="dbUser">The database user.</param>
    /// <param name="year">The year to query.</param>
    /// <returns>A list of movie titles.</returns>
    public async Task<List<string>> QueryMoviesByYearAsync(string
clusterIdentifier, string database,
        string dbUser, int year)
    {
        try
        {
            var sqlStatement = "SELECT title FROM Movies WHERE year = :year";

            var request = new ExecuteStatementRequest
            {
                ClusterIdentifier = clusterIdentifier,
                Database = database,
                DbUser = dbUser,
                Sql = sqlStatement,
                Parameters = new List<SqlParameter>
                {
                    new SqlParameter { Name = "year", Value = year.ToString() }
                }
            };
```

```
            var response = await
_redshiftDataClient.ExecuteStatementAsync(request);
            Console.WriteLine($"The identifier of the statement is
{response.Id}");

            await WaitForStatementToCompleteAsync(response.Id);

            var results = await GetStatementResultAsync(response.Id);
            var movieTitles = new List<string>();

            foreach (var row in results)
            {
                if (row.Count > 0)
                {
                    var title = row[0].StringValue;
                    Console.WriteLine($"The Movie title field is {title}");
                    movieTitles.Add(title);
                }
            }

            return movieTitles;
        }
        catch (Amazon.RedshiftDataAPIService.Model.ValidationException ex)
        {
            Console.WriteLine($"Validation error: {ex.Message}");
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't query movies. Here's why:
{ex.Message}");
            throw;
        }
    }

    /// <summary>
    /// Describe a statement execution.
    /// </summary>
    /// <param name="statementId">The statement ID.</param>
    /// <returns>The statement description.</returns>
    public async Task<DescribeStatementResponse> DescribeStatementAsync(string
statementId)
    {
```

```
        try
        {
            var request = new DescribeStatementRequest
            {
                Id = statementId
            };

            var response = await
_redshiftDataClient.DescribeStatementAsync(request);
            return response;
        }
        catch (Amazon.RedshiftDataAPIService.Model.ResourceNotFoundException ex)
        {
            Console.WriteLine($"Statement not found: {ex.Message}");
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't describe statement. Here's why:
{ex.Message}");
            throw;
        }
    }

    /// <summary>
    /// Get the results of a statement execution.
    /// </summary>
    /// <param name="statementId">The statement ID.</param>
    /// <returns>A list of result rows.</returns>
    public async Task<List<List<Field>>> GetStatementResultAsync(string
statementId)
    {
        try
        {
            var request = new GetStatementResultRequest
            {
                Id = statementId
            };

            var response = await
_redshiftDataClient.GetStatementResultAsync(request);
            return response.Records;
        }
        catch (Amazon.RedshiftDataAPIService.Model.ResourceNotFoundException ex)
```

```
        {
            Console.WriteLine($"Statement not found: {ex.Message}");
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't get statement result. Here's why:
{ex.Message}");
            throw;
        }
    }

    /// <summary>
    /// Wait for a statement to complete execution.
    /// </summary>
    /// <param name="statementId">The statement ID.</param>
    /// <returns>A task representing the asynchronous operation.</returns>
    private async Task WaitForStatementToCompleteAsync(string statementId)
    {
        var status = StatusString.SUBMITTED;
        DescribeStatementResponse? response = null;

        while (status == StatusString.SUBMITTED || status == StatusString.PICKED
|| status == StatusString.STARTED)
        {
            await Task.Delay(1000); // Wait 1 second
            response = await DescribeStatementAsync(statementId);
            status = response.Status;
            Console.WriteLine($"...{status}");
        }

        if (status == StatusString.FINISHED)
        {
            Console.WriteLine("The statement is finished!");
        }
        else
        {
            var errorMessage = response?.Error ?? "Unknown error";
            Console.WriteLine($"The statement failed with status: {status}");
            Console.WriteLine($"Error message: {errorMessage}");
        }
    }

    /// <summary>
```

```
    /// Wait for a cluster to become available.
    /// </summary>
    /// <param name="clusterIdentifier">The cluster identifier.</param>
    /// <returns>A task representing the asynchronous operation.</returns>
    public async Task WaitForClusterAvailableAsync(string clusterIdentifier)
    {
        Console.WriteLine($"Wait until {clusterIdentifier} is available. This may
 take a few minutes.");

        var startTime = DateTime.Now;
        var clusters = await DescribeClustersAsync(clusterIdentifier);

        while (clusters[0].ClusterStatus != "available")
        {
            var elapsed = DateTime.Now - startTime;
            Console.WriteLine($"Elapsed Time: {elapsed:mm\\:ss} - Waiting for
 cluster...");

            await Task.Delay(5000); // Wait 5 seconds
            clusters = await DescribeClustersAsync(clusterIdentifier);
        }

        var totalElapsed = DateTime.Now - startTime;
        Console.WriteLine($"Cluster is available! Total Elapsed Time:
 {totalElapsed:mm\\:ss}");
    }
}
```

Exécutez un scénario interactif illustrant les principes de base de Redshift.

```
/// <summary>
/// Amazon Redshift Getting Started Scenario.
/// </summary>
public class RedshiftBasics
{
    public static bool IsInteractive = true;
    public static RedshiftWrapper? Wrapper = null;
    public static ILogger logger = null!;
    private static readonly string _moviesFilePath = "../../../../../../
resources/sample_files/movies.json";

    /// <summary>
```

```
    /// Main method for the Amazon Redshift Getting Started scenario.
    /// </summary>
    /// <param name="args">Command line arguments.</param>
    public static async Task Main(string[] args)
    {
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonRedshift>()
                    .AddAWSService<IAmazonRedshiftDataAPIService>()
                    .AddTransient<RedshiftWrapper>()
            )
            .Build();

        logger = LoggerFactory.Create(builder => { builder.AddConsole(); })
            .CreateLogger<RedshiftBasics>();

        Wrapper = host.Services.GetRequiredService<RedshiftWrapper>();

        await RunScenarioAsync();
    }

    /// <summary>
    /// Run the complete Amazon Redshift scenario.
    /// </summary>
    public static async Task RunScenarioAsync()
    {
        // Set all variables to default values
        string userName = "awsuser";
        string userPassword = "AwsUser1000";
        string clusterIdentifier = "redshift-cluster-movies";
        var databaseName = "dev";
        int recordCount = 50;
        int year = 2013;
        try
        {
            Console.WriteLine(

"================================================================================");
            Console.WriteLine("Welcome to the Amazon Redshift SDK Getting Started
scenario.");
            Console.WriteLine(
                "This .NET program demonstrates how to interact with Amazon
Redshift by using the AWS SDK for .NET.");
            Console.WriteLine("Let's get started...");
```

```
            Console.WriteLine(

 "================================================================================");

            // Step 1: Get user credentials (if interactive)
            if (IsInteractive)
            {
                Console.WriteLine("Please enter a user name for the cluster
 (default is awsuser):");
                var userInput = Console.ReadLine();
                if (!string.IsNullOrEmpty(userInput))
                    userName = userInput;


 Console.WriteLine("================================================================================
                Console.WriteLine("Please enter a user password for the cluster
 (default is AwsUser1000):");
                var passwordInput = Console.ReadLine();
                if (!string.IsNullOrEmpty(passwordInput))
                    userPassword = passwordInput;


 Console.WriteLine("================================================================================

                // Step 2: Get cluster identifier
                Console.WriteLine("Enter a cluster id value (default is redshift-
cluster-movies):");
                var clusterInput = Console.ReadLine();
                if (!string.IsNullOrEmpty(clusterInput))
                    clusterIdentifier = clusterInput;
            }
            else
            {
                Console.WriteLine($"Using default values: userName={userName},
 clusterIdentifier={clusterIdentifier}");
            }

            // Step 3: Create Redshift cluster
            await Wrapper!.CreateClusterAsync(clusterIdentifier, databaseName,
 userName, userPassword);

 Console.WriteLine("================================================================================

            // Step 4: Wait for cluster to become available
```

```
Console.WriteLine("==========================================================================
            await Wrapper.WaitForClusterAvailableAsync(clusterIdentifier);

Console.WriteLine("==========================================================================

            // Step 5: List databases

Console.WriteLine("==========================================================================
            Console.WriteLine($" When you created {clusterIdentifier}, the dev
database is created by default and used in this scenario.");
            Console.WriteLine(" To create a custom database, you need to have a
CREATEDB privilege.");
            Console.WriteLine(" For more information, see the documentation here:
https://docs.aws.amazon.com/redshift/latest/dg/r_CREATE_DATABASE.html.");
            if (IsInteractive)
            {
                Console.WriteLine("Press Enter to continue...");
                Console.ReadLine();
            }

Console.WriteLine("==========================================================================


Console.WriteLine("==========================================================================
            Console.WriteLine($"List databases in {clusterIdentifier}");
            if (IsInteractive)
            {
                Console.WriteLine("Press Enter to continue...");
                Console.ReadLine();
            }
            await Wrapper.ListDatabasesAsync(clusterIdentifier, userName,
databaseName);

Console.WriteLine("==========================================================================

            // Step 6: Create Movies table

Console.WriteLine("==========================================================================
            Console.WriteLine("Now you will create a table named Movies.");
            if (IsInteractive)
            {
                Console.WriteLine("Press Enter to continue...");
                Console.ReadLine();
```

```
            }
            await Wrapper.CreateTableAsync(clusterIdentifier, databaseName,
userName);

Console.WriteLine("=============================================================================

            // Step 7: Populate the Movies table

Console.WriteLine("=============================================================================
            Console.WriteLine("Populate the Movies table using the Movies.json
file.");

            if (IsInteractive)
            {
                Console.WriteLine("Specify the number of records you would like
to add to the Movies Table.");
                Console.WriteLine("Please enter a value between 50 and 200.");
                Console.Write("Enter a value: ");

                var recordCountInput = Console.ReadLine();
                if (int.TryParse(recordCountInput, out var inputCount) &&
inputCount is >= 50 and <= 200)
                {
                    recordCount = inputCount;
                }
                else
                {
                    Console.WriteLine($"Invalid input. Using default value of
{recordCount}.");
                }
            }
            else
            {
                Console.WriteLine($"Using default record count: {recordCount}");
            }

            await PopulateMoviesTableAsync(clusterIdentifier, databaseName,
userName, recordCount);
            Console.WriteLine($"{recordCount} records were added to the Movies
table.");

Console.WriteLine("=============================================================================

            // Step 8 & 9: Query movies by year
```

```
 Console.WriteLine("=================================================================
            Console.WriteLine("Query the Movies table by year. Enter a value
 between 2012-2014.");

            if (IsInteractive)
            {
                Console.Write("Enter a year: ");
                var yearInput = Console.ReadLine();
                if (int.TryParse(yearInput, out var inputYear) && inputYear is >=
 2012 and <= 2014)
                {
                    year = inputYear;
                }
                else
                {
                    Console.WriteLine($"Invalid input. Using default value of
 {year}.");
                }
            }
            else
            {
                Console.WriteLine($"Using default year: {year}");
            }

            await Wrapper.QueryMoviesByYearAsync(clusterIdentifier, databaseName,
 userName, year);

 Console.WriteLine("=================================================================

            // Step 10: Modify the cluster

 Console.WriteLine("=================================================================
            Console.WriteLine("Now you will modify the Redshift cluster.");
            if (IsInteractive)
            {
                Console.WriteLine("Press Enter to continue...");
                Console.ReadLine();
            }
            await Wrapper.ModifyClusterAsync(clusterIdentifier, "wed:07:30-
wed:08:00");

 Console.WriteLine("=================================================================
```

```
            // Step 11 & 12: Delete cluster confirmation

Console.WriteLine("================================================================================
            if (IsInteractive)
            {
                Console.WriteLine("Would you like to delete the Amazon Redshift
cluster? (y/n)");
                var deleteResponse = Console.ReadLine();
                if (deleteResponse?.ToLower() == "y")
                {
                    await
Wrapper.DeleteClusterWithoutSnapshotAsync(clusterIdentifier);
                }
            }
            else
            {
                Console.WriteLine("Deleting the Amazon Redshift cluster...");
                await
Wrapper.DeleteClusterWithoutSnapshotAsync(clusterIdentifier);
            }

Console.WriteLine("================================================================================


Console.WriteLine("================================================================================
            Console.WriteLine("This concludes the Amazon Redshift SDK Getting
Started scenario.");

Console.WriteLine("================================================================================
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred during the scenario:
{ex.Message}");
            Console.WriteLine("Deleting the Amazon Redshift cluster...");
            await Wrapper!.DeleteClusterWithoutSnapshotAsync(clusterIdentifier);
            throw;
        }
    }

    /// <summary>
    /// Populate the Movies table with data from the JSON file.
    /// </summary>
    /// <param name="clusterIdentifier">The cluster identifier.</param>
```

```
    /// <param name="database">The database name.</param>
    /// <param name="dbUser">The database user.</param>
    /// <param name="recordCount">Number of records to insert.</param>
    private static async Task PopulateMoviesTableAsync(string clusterIdentifier,
string database, string dbUser, int recordCount)
    {
        if (!File.Exists(_moviesFilePath))
        {
            throw new FileNotFoundException($"Required movies data file not found
at: {_moviesFilePath}");
        }

        var jsonContent = await File.ReadAllTextAsync(_moviesFilePath);
        var options = new JsonSerializerOptions
        {
            PropertyNameCaseInsensitive = true
        };
        var movies = JsonSerializer.Deserialize<List<Movie>>(jsonContent,
options);

        if (movies == null || movies.Count == 0)
        {
            throw new InvalidOperationException("Failed to parse movies JSON file
or file is empty.");
        }

        var insertCount = Math.Min(recordCount, movies.Count);

        for (int i = 0; i < insertCount; i++)
        {
            var movie = movies[i];
            await Wrapper!.InsertMovieAsync(clusterIdentifier, database, dbUser,
i, movie.Title, movie.Year);
        }
    }

    /// <summary>
    /// Movie data model.
    /// </summary>
    private class Movie
    {
        public string Title { get; set; } = string.Empty;
        public int Year { get; set; }
    }
```

```
}
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK pour .NET .
  - CreateCluster
  - DescribeClusters
  - DescribeStatement
  - ExecuteStatement
  - GetStatementResult
  - ListDatabasesPaginator
  - ModifyCluster

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
package scenarios

import (
 "context"
 "encoding/json"
 "errors"
 "fmt"
 "log"
 "math/rand"
 "strings"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 redshift_types "github.com/aws/aws-sdk-go-v2/service/redshift/types"
```

```
 redshiftdata_types "github.com/aws/aws-sdk-go-v2/service/redshiftdata/types"
 "github.com/aws/aws-sdk-go-v2/service/secretsmanager"
 "github.com/awsdocs/aws-doc-sdk-examples/gov2/demotools"
 "github.com/awsdocs/aws-doc-sdk-examples/gov2/redshift/actions"

 "github.com/aws/aws-sdk-go-v2/service/redshift"
 "github.com/aws/aws-sdk-go-v2/service/redshiftdata"
)

// IScenarioHelper abstracts input and wait functions from a scenario so that
 they
// can be mocked for unit testing.
type IScenarioHelper interface {
 GetName() string
}

const rMax = 100000

type ScenarioHelper struct {
 Prefix string
 Random *rand.Rand
}

// GetName returns a unique name formed of a prefix and a random number.
func (helper ScenarioHelper) GetName() string {
 return fmt.Sprintf("%v%v", helper.Prefix, helper.Random.Intn(rMax))
}

// RedshiftBasicsScenario separates the steps of this scenario into individual
 functions so that
// they are simpler to read and understand.
type RedshiftBasicsScenario struct {
 sdkConfig         aws.Config
 helper            IScenarioHelper
 questioner        demotools.IQuestioner
 pauser            demotools.IPausable
 filesystem        demotools.IFileSystem
 redshiftActor     *actions.RedshiftActions
 redshiftDataActor *actions.RedshiftDataActions
 secretsmanager    *SecretsManager
}

// SecretsManager is used to retrieve username and password information from a
 secure service.
```

```
type SecretsManager struct {
 SecretsManagerClient *secretsmanager.Client
}

// RedshiftBasics constructs a new Redshift Basics runner.
func RedshiftBasics(sdkConfig aws.Config, questioner demotools.IQuestioner,
 pauser demotools.IPausable, filesystem demotools.IFileSystem, helper
 IScenarioHelper) RedshiftBasicsScenario {
 scenario := RedshiftBasicsScenario{
  sdkConfig:         sdkConfig,
  helper:            helper,
  questioner:        questioner,
  pauser:            pauser,
  filesystem:        filesystem,
  secretsmanager:    &SecretsManager{SecretsManagerClient:
 secretsmanager.NewFromConfig(sdkConfig)},
  redshiftActor:     &actions.RedshiftActions{RedshiftClient:
 redshift.NewFromConfig(sdkConfig)},
  redshiftDataActor: &actions.RedshiftDataActions{RedshiftDataClient:
 redshiftdata.NewFromConfig(sdkConfig)},
 }
 return scenario
}


// Movie makes it easier to use Movie objects given in json format.
type Movie struct {
 ID    int    `json:"id"`
 Title string `json:"title"`
 Year  int    `json:"year"`
}


// User makes it easier to get the User data back from SecretsManager and use it
 later.
type User struct {
 Username string `json:"userName"`
 Password string `json:"userPassword"`
}

// Run runs the RedshiftBasics interactive example that shows you how to use
 Amazon
// Redshift and how to interact with its common endpoints.
//
```

```
// 0. Retrieve username and password information to access Redshift.
// 1. Create a cluster.
// 2. Wait for the cluster to become available.
// 3. List the available databases in the region.
// 4. Create a table named "Movies" in the "dev" database.
// 5. Populate the movies table from the "movies.json" file.
// 6. Query the movies table by year.
// 7. Modify the cluster's maintenance window.
// 8. Optionally clean up all resources created during this demo.
//
// This example creates an Amazon Redshift service client from the specified
 sdkConfig so that
// you can replace it with a mocked or stubbed config for unit testing.
//
// It uses a questioner from the `demotools` package to get input during the
 example.
// This package can be found in the ..\..\demotools folder of this repo.
func (runner *RedshiftBasicsScenario) Run(ctx context.Context) {

 user := User{}
 secretId := "s3express/basics/secrets"
 clusterId := "demo-cluster-1"
 maintenanceWindow := "wed:07:30-wed:08:00"
 databaseName := "dev"
 tableName := "Movies"
 fileName := "Movies.json"
 nodeType := "ra3.xlplus"
 clusterType := "single-node"

 defer func() {
  if r := recover(); r != nil {
   log.Println("Something went wrong with the demo.")
   _, isMock := runner.questioner.(*demotools.MockQuestioner)
   if isMock || runner.questioner.AskBool("Do you want to see the full error
 message (y/n)?", "y") {
    log.Println(r)
   }
   runner.cleanUpResources(ctx, clusterId, databaseName, tableName,
 user.Username, runner.questioner)
  }
 }()

 // Retrieve the userName and userPassword from SecretsManager
```

```
 output, err := runner.secretsmanager.SecretsManagerClient.GetSecretValue(ctx,
 &secretsmanager.GetSecretValueInput{
  SecretId: aws.String(secretId),
 })
 if err != nil {
  log.Printf("There was a problem getting the secret value: %s", err)
  log.Printf("Please make sure to create a secret named 's3express/basics/
secrets' with keys of 'userName' and 'userPassword'.")
  panic(err)
 }

 err = json.Unmarshal([]byte(*output.SecretString), &user)
 if err != nil {
  log.Printf("There was a problem parsing the secret value from JSON: %s", err)
  panic(err)
 }

 // Create the Redshift cluster
 _, err = runner.redshiftActor.CreateCluster(ctx, clusterId, user.Username,
 user.Password, nodeType, clusterType, true)
 if err != nil {
  var clusterAlreadyExistsFault *redshift_types.ClusterAlreadyExistsFault
  if errors.As(err, &clusterAlreadyExistsFault) {
   log.Println("Cluster already exists. Continuing.")
  } else {
   log.Println("Error creating cluster.")
   panic(err)
  }
 }

 // Wait for the cluster to become available
 waiter :=
 redshift.NewClusterAvailableWaiter(runner.redshiftActor.RedshiftClient)
 err = waiter.Wait(ctx, &redshift.DescribeClustersInput{
  ClusterIdentifier: aws.String(clusterId),
 }, 5*time.Minute)
 if err != nil {
  log.Println("An error occurred waiting for the cluster.")
  panic(err)
 }

 // Get some info about the cluster
 describeOutput, err := runner.redshiftActor.DescribeClusters(ctx, clusterId)
 if err != nil {
```

```
 log.Println("Something went wrong trying to get information about the
cluster.")
 panic(err)
}
log.Println("Here's some information about the cluster.")
log.Printf("The cluster's status is %s",
*describeOutput.Clusters[0].ClusterStatus)
log.Printf("The cluster was created at %s",
*describeOutput.Clusters[0].ClusterCreateTime)

// List databases
log.Println("List databases in", clusterId)
runner.questioner.Ask("Press Enter to continue...")
err = runner.redshiftDataActor.ListDatabases(ctx, clusterId, databaseName,
user.Username)
if err != nil {
 log.Printf("Failed to list databases: %v\n", err)
 panic(err)
}

// Create the "Movies" table
log.Println("Now you will create a table named " + tableName + ".")
runner.questioner.Ask("Press Enter to continue...")
err = nil
result, err := runner.redshiftDataActor.CreateTable(ctx, clusterId,
databaseName, tableName, user.Username, runner.pauser, []string{"title
VARCHAR(256)", "year INT"})
if err != nil {
 log.Printf("Failed to create table: %v\n", err)
 panic(err)
}

describeInput := redshiftdata.DescribeStatementInput{
 Id: result.Id,
}
query := actions.RedshiftQuery{
 Context: ctx,
 Input:   describeInput,
 Result:  result,
}
err = runner.redshiftDataActor.WaitForQueryStatus(query, runner.pauser, true)
if err != nil {
 log.Printf("Failed to execute query: %v\n", err)
 panic(err)
```

```
 }
 log.Printf("Successfully executed query\n")

 // Populate the "Movies" table
 runner.PopulateMoviesTable(ctx, clusterId, databaseName, tableName,
 user.Username, fileName)

 // Query the "Movies" table by year
 log.Println("Query the Movies table by year.")
 year := runner.questioner.AskInt(
  fmt.Sprintf("Enter a value between %v and %v:", 2012, 2014),
  demotools.InIntRange{Lower: 2012, Upper: 2014})
 runner.QueryMoviesByYear(ctx, clusterId, databaseName, tableName, user.Username,
 year)

 // Modify the cluster's maintenance window
 runner.redshiftActor.ModifyCluster(ctx, clusterId, maintenanceWindow)

 // Delete the Redshift cluster if confirmed
 runner.cleanUpResources(ctx, clusterId, databaseName, tableName, user.Username,
 runner.questioner)

 log.Println("Thanks for watching!")
}

// cleanUpResources asks the user if they would like to delete each resource
 created during the scenario, from most
// impactful to least impactful. If any choice to delete is made, further
 deletion attempts are skipped.
func (runner *RedshiftBasicsScenario) cleanUpResources(ctx context.Context,
 clusterId string, databaseName string, tableName string, userName string,
 questioner demotools.IQuestioner) {
 deleted := false
 var err error = nil
 if questioner.AskBool("Do you want to delete the entire cluster? This will clean
 up all resources. (y/n)", "y") {
  deleted, err = runner.redshiftActor.DeleteCluster(ctx, clusterId)
  if err != nil {
   log.Printf("Error deleting cluster: %v", err)
  }
 }
 if !deleted && questioner.AskBool("Do you want to delete the dev table? This
 will clean up all inserted records but keep your cluster intact. (y/n)", "y") {
```

```
  deleted, err = runner.redshiftDataActor.DeleteTable(ctx, clusterId,
 databaseName, tableName, userName)
  if err != nil {
   log.Printf("Error deleting movies table: %v", err)
  }
 }
 if !deleted && questioner.AskBool("Do you want to delete all rows in the Movies
 table? This will clean up all inserted records but keep your cluster and table
 intact. (y/n)", "y") {
  deleted, err = runner.redshiftDataActor.DeleteDataRows(ctx, clusterId,
 databaseName, tableName, userName, runner.pauser)
  if err != nil {
   log.Printf("Error deleting data rows: %v", err)
  }
 }
 if !deleted {
  log.Print("Please manually delete any unwanted resources.")
 }
}


// loadMoviesFromJSON takes the <fileName> file and populates a slice of Movie
 objects.
func (runner *RedshiftBasicsScenario) loadMoviesFromJSON(fileName string,
 filesystem demotools.IFileSystem) ([]Movie, error) {
 file, err := filesystem.OpenFile("../../resources/sample_files/" + fileName)
 if err != nil {
  return nil, err
 }
 defer filesystem.CloseFile(file)

 var movies []Movie
 err = json.NewDecoder(file).Decode(&movies)
 if err != nil {
  return nil, err
 }

 return movies, nil
}



// PopulateMoviesTable reads data from the <fileName> file and inserts records
 into the "Movies" table.
```

```
func (runner *RedshiftBasicsScenario) PopulateMoviesTable(ctx context.Context,
 clusterId string, databaseName string, tableName string, userName string,
 fileName string) {
 log.Println("Populate the " + tableName + " table using the " + fileName + "
 file.")
 numRecords := runner.questioner.AskInt(
  fmt.Sprintf("Enter a value between %v and %v:", 10, 100),
  demotools.InIntRange{Lower: 10, Upper: 100})

 movies, err := runner.loadMoviesFromJSON(fileName, runner.filesystem)
 if err != nil {
  log.Printf("Failed to load movies from JSON: %v\n", err)
  panic(err)
 }

 var sqlStatements []string

 for i, movie := range movies {
  if i >= numRecords {
   break
  }

  sqlStatement := fmt.Sprintf(`INSERT INTO %s (title, year) VALUES ('%s', %d);`,
   tableName,
   strings.Replace(movie.Title, "'", "''", -1), // Double any single quotes to
escape them
   movie.Year)

  sqlStatements = append(sqlStatements, sqlStatement)
 }

 input := &redshiftdata.BatchExecuteStatementInput{
  ClusterIdentifier: aws.String(clusterId),
  Database:          aws.String(databaseName),
  DbUser:            aws.String(userName),
  Sqls:              sqlStatements,
 }

 result, err := runner.redshiftDataActor.ExecuteBatchStatement(ctx, *input)
 if err != nil {
  log.Printf("Failed to execute batch statement: %v\n", err)
  panic(err)
 }
```

```
 describeInput := redshiftdata.DescribeStatementInput{
  Id: result.Id,
 }

 query := actions.RedshiftQuery{
  Context: ctx,
  Result:  result,
  Input:   describeInput,
 }
 err = runner.redshiftDataActor.WaitForQueryStatus(query, runner.pauser, true)
 if err != nil {
  log.Printf("Failed to execute batch insert query: %v\n", err)
  return
 }
 log.Printf("Successfully executed batch statement\n")

 log.Printf("%d records were added to the Movies table.\n", numRecords)
}



// QueryMoviesByYear retrieves only movies from the "Movies" table which match
 the given year.
func (runner *RedshiftBasicsScenario) QueryMoviesByYear(ctx context.Context,
 clusterId string, databaseName string, tableName string, userName string, year
 int) {

 sqlStatement := fmt.Sprintf(`SELECT title FROM %s WHERE year = %d;`, tableName,
 year)

 input := &redshiftdata.ExecuteStatementInput{
  ClusterIdentifier: aws.String(clusterId),
  Database:          aws.String(databaseName),
  DbUser:            aws.String(userName),
  Sql:               aws.String(sqlStatement),
 }

 result, err := runner.redshiftDataActor.ExecuteStatement(ctx, *input)
 if err != nil {
  log.Printf("Failed to query movies: %v\n", err)
  panic(err)
 }

 log.Println("The identifier of the statement is ", *result.Id)
```

```
 describeInput := redshiftdata.DescribeStatementInput{
  Id: result.Id,
 }

 query := actions.RedshiftQuery{
  Context: ctx,
  Input:   describeInput,
  Result:  result,
 }
 err = runner.redshiftDataActor.WaitForQueryStatus(query, runner.pauser, true)
 if err != nil {
  log.Printf("Failed to execute query: %v\n", err)
  panic(err)
 }
 log.Printf("Successfully executed query\n")

 getResultOutput, err := runner.redshiftDataActor.GetStatementResult(ctx,
 *result.Id)
 if err != nil {
  log.Printf("Failed to query movies: %v\n", err)
  panic(err)
 }
 for _, row := range getResultOutput.Records {
  for _, col := range row {
   title, ok := col.(*redshiftdata_types.FieldMemberStringValue)
   if !ok {
    log.Println("Failed to parse the field")
   } else {
    log.Printf("The Movie title field is %s\n", title.Value)
   }
  }
 }
}
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK pour Go .
  - CreateCluster
  - DescribeClusters

- DescribeStatement
- ExecuteStatement
- GetStatementResult
- ListDatabasesPaginator
- ModifyCluster

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Exécutez un scénario interactif illustrant les fonctionnalités d'Amazon Redshift.

```
import com.example.redshift.User;
import com.google.gson.Gson;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import software.amazon.awssdk.regions.Region;
import
 software.amazon.awssdk.services.redshift.model.ClusterAlreadyExistsException;
import software.amazon.awssdk.services.redshift.model.CreateClusterResponse;
import software.amazon.awssdk.services.redshift.model.DeleteClusterResponse;
import software.amazon.awssdk.services.redshift.model.ModifyClusterResponse;
import software.amazon.awssdk.services.redshift.model.RedshiftException;
import
 software.amazon.awssdk.services.redshiftdata.model.ExecuteStatementResponse;
import software.amazon.awssdk.services.redshiftdata.model.RedshiftDataException;
import java.util.Scanner;
import java.util.concurrent.CompletableFuture;
import software.amazon.awssdk.services.secretsmanager.SecretsManagerClient;
import
 software.amazon.awssdk.services.secretsmanager.model.GetSecretValueRequest;
import
 software.amazon.awssdk.services.secretsmanager.model.GetSecretValueResponse;
```

```
/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 *
 *  This example requires an AWS Secrets Manager secret that contains the
 *  database credentials. If you do not create a
 *  secret that specifies user name and password, this example will not work. For
 details, see:
 *
 *  https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_how-
services-use-secrets_RS.html
 *
 This Java example performs these tasks:
 *
 * 1. Prompts the user for a unique cluster ID or use the default value.
 * 2. Creates a Redshift cluster with the specified or default cluster Id value.
 * 3. Waits until the Redshift cluster is available for use.
 * 4. Lists all databases using a pagination API call.
 * 5. Creates a table named "Movies" with fields ID, title, and year.
 * 6. Inserts a specified number of records into the "Movies" table by reading
 the Movies JSON file.
 * 7. Prompts the user for a movie release year.
 * 8. Runs a SQL query to retrieve movies released in the specified year.
 * 9. Modifies the Redshift cluster.
 * 10. Prompts the user for confirmation to delete the Redshift cluster.
 * 11. If confirmed, deletes the specified Redshift cluster.
 */

public class RedshiftScenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");
    private static final Logger logger =
 LoggerFactory.getLogger(RedshiftScenario.class);

    static RedshiftActions redshiftActions = new RedshiftActions();
    public static void main(String[] args) throws Exception {
        final String usage = """
```

```
            Usage:
                <jsonFilePath> <secretName>\s

            Where:
                jsonFilePath - The path to the Movies JSON file (you can locate
that file in ../../../resources/sample_files/movies.json)
                secretName - The name of the secret that belongs to Secret
Manager that stores the user name and password used in this scenario.
            """;

        if (args.length != 2) {
            logger.info(usage);
            return;
        }

        String jsonFilePath = args[0];
        String secretName = args[1];
        Scanner scanner = new Scanner(System.in);
        logger.info(DASHES);
        logger.info("Welcome to the Amazon Redshift SDK Basics scenario.");
        logger.info("""
            This Java program demonstrates how to interact with Amazon Redshift
by using the AWS SDK for Java (v2).\s
            Amazon Redshift is a fully managed, petabyte-scale data warehouse
service hosted in the cloud.

            The program's primary functionalities include cluster creation,
verification of cluster readiness,\s
            list databases, table creation, data population within the table, and
execution of SQL statements.
            Furthermore, it demonstrates the process of querying data from the
Movie table.\s

            Upon completion of the program, all AWS resources are cleaned up.
            """);

        logger.info("Lets get started...");
        logger.info("""
            First, we will retrieve the user name and password from Secrets
Manager.

            Using Amazon Secrets Manager to store Redshift credentials provides
several security benefits.
```

```
            It allows you to securely store and manage sensitive information,
 such as passwords, API keys, and
            database credentials, without embedding them directly in your
 application code.

            More information can be found here:

            https://docs.aws.amazon.com/secretsmanager/latest/userguide/
integrating_how-services-use-secrets_RS.html
            """);
        Gson gson = new Gson();
        User user = gson.fromJson(String.valueOf(getSecretValues(secretName)),
 User.class);
        waitForInputToContinue(scanner);
        logger.info(DASHES);

        try {
            runScenario(user, scanner, jsonFilePath);
        } catch (RuntimeException e) {
            e.printStackTrace();
        } catch (Throwable e) {
            throw new RuntimeException(e);
        }
    }

    private static void runScenario(User user, Scanner scanner,  String
 jsonFilePath) throws Throwable {
        String databaseName = "dev";
        System.out.println(DASHES);
        logger.info("Create a Redshift Cluster");
        logger.info("A Redshift cluster refers to the collection of computing
 resources and storage that work together to process and analyze large volumes of
 data.");
        logger.info("Enter a cluster id value or accept the default by hitting
 Enter (default is redshift-cluster-movies): ");
        String userClusterId = scanner.nextLine();
        String clusterId = userClusterId.isEmpty() ? "redshift-cluster-movies" :
 userClusterId;
        try {
            CompletableFuture<CreateClusterResponse> future =
 redshiftActions.createClusterAsync(clusterId, user.getUserName(),
 user.getUserPassword());
            CreateClusterResponse response = future.join();
```

```
            logger.info("Cluster successfully created. Cluster Identifier {} ",
 response.cluster().clusterIdentifier());

        } catch (RuntimeException rt) {
            Throwable cause = rt.getCause();
            if (cause instanceof ClusterAlreadyExistsException) {
                logger.info("The Cluster {} already exists. Moving on...",
 clusterId);
            } else {
                logger.info("An unexpected error occurred: " + rt.getMessage());
            }
        }
        logger.info(DASHES);

        logger.info(DASHES);
        logger.info("Wait until {} is available.", clusterId);
        waitForInputToContinue(scanner);
        try {
            CompletableFuture<Void> future =
 redshiftActions.waitForClusterReadyAsync(clusterId);
            future.join();
            logger.info("Cluster is ready!");

        } catch (RuntimeException rt) {
            Throwable cause = rt.getCause();
            if (cause instanceof RedshiftException redshiftEx) {
                logger.info("Redshift error occurred: Error message: {}, Error
 code {}", redshiftEx.getMessage(), redshiftEx.awsErrorDetails().errorCode());
            } else {
                logger.info("An unexpected error occurred: " + rt.getMessage());
            }
            throw cause;
        }
        logger.info(DASHES);

        logger.info(DASHES);
        String databaseInfo = """
            When you created $clusteridD, the dev database is created by default
 and used in this scenario.\s

            To create a custom database, you need to have a CREATEDB privilege.\s
            For more information, see the documentation here: https://
docs.aws.amazon.com/redshift/latest/dg/r_CREATE_DATABASE.html.
          """.replace("$clusteridD", clusterId);
```

```
        logger.info(databaseInfo);
        waitForInputToContinue(scanner);
        logger.info(DASHES);

        logger.info(DASHES);
        logger.info("List databases in {} ",clusterId);
        waitForInputToContinue(scanner);
        try {
            CompletableFuture<Void> future =
redshiftActions.listAllDatabasesAsync(clusterId, user.getUserName(), "dev");
            future.join();
            logger.info("Databases listed successfully.");

        } catch (RuntimeException rt) {
            Throwable cause = rt.getCause();
            if (cause instanceof RedshiftDataException redshiftEx) {
                logger.error("Redshift Data error occurred: {} Error code: {}",
redshiftEx.getMessage(), redshiftEx.awsErrorDetails().errorCode());
            } else {
                logger.error("An unexpected error occurred: {}",
rt.getMessage());
            }
            throw cause;
        }
        logger.info(DASHES);

        logger.info(DASHES);
        logger.info("Now you will create a table named Movies.");
        waitForInputToContinue(scanner);
        try {
            CompletableFuture<ExecuteStatementResponse> future =
redshiftActions.createTableAsync(clusterId, databaseName, user.getUserName());
            future.join();

        } catch (RuntimeException rt) {
            Throwable cause = rt.getCause();
            if (cause instanceof RedshiftDataException redshiftEx) {
                logger.info("Redshift Data error occurred: {} Error code: {}",
redshiftEx.getMessage(), redshiftEx.awsErrorDetails().errorCode());
            } else {
                logger.info("An unexpected error occurred: {}", rt.getMessage());
            }
            throw cause;
```

```
        }
        logger.info(DASHES);

        logger.info(DASHES);
        logger.info("Populate the Movies table using the Movies.json file.");
        logger.info("Specify the number of records you would like to add to the
Movies Table.");
        logger.info("Please enter a value between 50 and 200.");
        int numRecords;
        do {
            logger.info("Enter a value: ");
            while (!scanner.hasNextInt()) {
                logger.info("Invalid input. Please enter a value between 50 and
200.");
                logger.info("Enter a year: ");
                scanner.next();
            }
            numRecords = scanner.nextInt();
        } while (numRecords < 50 || numRecords > 200);
        try {
            redshiftActions.popTableAsync(clusterId, databaseName,
user.getUserName(), jsonFilePath, numRecords).join();  // Wait for the operation
to complete
        } catch (RuntimeException rt) {
            Throwable cause = rt.getCause();
            if (cause instanceof RedshiftDataException redshiftEx) {
                logger.info("Redshift Data error occurred: {} Error code: {}",
redshiftEx.getMessage(), redshiftEx.awsErrorDetails().errorCode());
            } else {
                logger.info("An unexpected error occurred: {}", rt.getMessage());
            }
            throw cause;
        }
        waitForInputToContinue(scanner);
        logger.info(DASHES);

        logger.info(DASHES);
        logger.info("Query the Movies table by year. Enter a value between
2012-2014.");
        int movieYear;
        do {
            logger.info("Enter a year: ");
            while (!scanner.hasNextInt()) {
```

```
                logger.info("Invalid input. Please enter a valid year between
2012 and 2014.");
                logger.info("Enter a year: ");
                scanner.next();
            }
            movieYear = scanner.nextInt();
            scanner.nextLine();
        } while (movieYear < 2012 || movieYear > 2014);

        String id;
        try {
            CompletableFuture<String> future =
redshiftActions.queryMoviesByYearAsync(databaseName, user.getUserName(),
movieYear, clusterId);
            id = future.join();

        } catch (RuntimeException rt) {
            Throwable cause = rt.getCause();
            if (cause instanceof RedshiftDataException redshiftEx) {
                logger.info("Redshift Data error occurred: {} Error code: {}",
redshiftEx.getMessage(), redshiftEx.awsErrorDetails().errorCode());
            } else {
                logger.info("An unexpected error occurred: {}", rt.getMessage());
            }
            throw cause;
        }

        logger.info("The identifier of the statement is " + id);
        waitForInputToContinue(scanner);
        try {
            CompletableFuture<Void> future =
redshiftActions.checkStatementAsync(id);
            future.join();

        } catch (RuntimeException rt) {
            Throwable cause = rt.getCause();
            if (cause instanceof RedshiftDataException redshiftEx) {
                logger.info("Redshift Data error occurred: {} Error code: {}",
redshiftEx.getMessage(), redshiftEx.awsErrorDetails().errorCode());
            } else {
                logger.info("An unexpected error occurred: {}", rt.getMessage());
            }
            throw cause;
        }
```

```
        waitForInputToContinue(scanner);
        try {
            CompletableFuture<Void> future = redshiftActions.getResultsAsync(id);
            future.join();

        } catch (RuntimeException rt) {
            Throwable cause = rt.getCause();
            if (cause instanceof RedshiftDataException redshiftEx) {
                logger.info("Redshift Data error occurred: {} Error code: {}",
 redshiftEx.getMessage(), redshiftEx.awsErrorDetails().errorCode());
            } else {
                logger.info("An unexpected error occurred: {}", rt.getMessage());
            }
            throw cause;
        }
        waitForInputToContinue(scanner);
        logger.info(DASHES);

        logger.info(DASHES);
        logger.info("Now you will modify the Redshift cluster.");
        waitForInputToContinue(scanner);
        try {
            CompletableFuture<ModifyClusterResponse> future =
 redshiftActions.modifyClusterAsync(clusterId);;
            future.join();

        } catch (RuntimeException rt) {
            Throwable cause = rt.getCause();
            if (cause instanceof RedshiftDataException redshiftEx) {
                logger.info("Redshift Data error occurred: {} Error code: {}",
 redshiftEx.getMessage(), redshiftEx.awsErrorDetails().errorCode());
            } else {
                logger.info("An unexpected error occurred: {}", rt.getMessage());
            }
            throw cause;
        }
        waitForInputToContinue(scanner);
        logger.info(DASHES);

        logger.info(DASHES);
        logger.info("Would you like to delete the Amazon Redshift cluster? (y/
n)");
        String delAns = scanner.nextLine().trim();
        if (delAns.equalsIgnoreCase("y")) {
```

```
            logger.info("You selected to delete {} ", clusterId);
            waitForInputToContinue(scanner);
            try {
                CompletableFuture<DeleteClusterResponse> future =
redshiftActions.deleteRedshiftClusterAsync(clusterId);;
                future.join();

            } catch (RuntimeException rt) {
                Throwable cause = rt.getCause();
                if (cause instanceof RedshiftDataException redshiftEx) {
                    logger.info("Redshift Data error occurred: {} Error code:
{}", redshiftEx.getMessage(), redshiftEx.awsErrorDetails().errorCode());
                } else {
                    logger.info("An unexpected error occurred: {}",
rt.getMessage());
                }
                throw cause;
            }
        } else {
            logger.info("The {}  was not deleted", clusterId);
        }
        logger.info(DASHES);

        logger.info(DASHES);
        logger.info("This concludes the Amazon Redshift SDK Basics scenario.");
        logger.info(DASHES);
    }

    private static SecretsManagerClient getSecretClient() {
        Region region = Region.US_EAST_1;
        return SecretsManagerClient.builder()
            .region(region)
            .build();
    }

    private static void waitForInputToContinue(Scanner scanner) {
        while (true) {
            System.out.println("");
            System.out.println("Enter 'c' followed by <ENTER> to continue:");
            String input = scanner.nextLine();

            if (input.trim().equalsIgnoreCase("c")) {
                System.out.println("Continuing with the program...");
                System.out.println("");
```

```
                break;
            } else {
                // Handle invalid input.
                System.out.println("Invalid input. Please try again.");
            }
        }
    }

    // Get the Amazon Redshift credentials from AWS Secrets Manager.
    private static String getSecretValues(String secretName) {
        SecretsManagerClient secretClient = getSecretClient();
        GetSecretValueRequest valueRequest = GetSecretValueRequest.builder()
            .secretId(secretName)
            .build();

        GetSecretValueResponse valueResponse =
 secretClient.getSecretValue(valueRequest);
        return valueResponse.secretString();
    }
}
```

Une classe d’encapsuleur pour les méthodes du kit SDK Amazon Redshift.

```
public class RedshiftActions {

    private static final Logger logger =
 LoggerFactory.getLogger(RedshiftActions.class);
    private static RedshiftDataAsyncClient redshiftDataAsyncClient;

    private static RedshiftAsyncClient redshiftAsyncClient;

    private static RedshiftAsyncClient getAsyncClient() {
        if (redshiftAsyncClient == null) {
            SdkAsyncHttpClient httpClient = NettyNioAsyncHttpClient.builder()
                .maxConcurrency(100)
                .connectionTimeout(Duration.ofSeconds(60))
                .readTimeout(Duration.ofSeconds(60))
                .writeTimeout(Duration.ofSeconds(60))
                .build();

            ClientOverrideConfiguration overrideConfig =
 ClientOverrideConfiguration.builder()
```

```
                .apiCallTimeout(Duration.ofMinutes(2))
                .apiCallAttemptTimeout(Duration.ofSeconds(90))
                .retryStrategy(RetryMode.STANDARD)
                .build();

            redshiftAsyncClient = RedshiftAsyncClient.builder()
                .httpClient(httpClient)
                .overrideConfiguration(overrideConfig)
                .build();
        }
        return redshiftAsyncClient;
    }

    private static RedshiftDataAsyncClient getAsyncDataClient() {
        if (redshiftDataAsyncClient == null) {
            SdkAsyncHttpClient httpClient = NettyNioAsyncHttpClient.builder()
                .maxConcurrency(100)
                .connectionTimeout(Duration.ofSeconds(60))
                .readTimeout(Duration.ofSeconds(60))
                .writeTimeout(Duration.ofSeconds(60))
                .build();

            ClientOverrideConfiguration overrideConfig =
ClientOverrideConfiguration.builder()
                .apiCallTimeout(Duration.ofMinutes(2))
                .apiCallAttemptTimeout(Duration.ofSeconds(90))
                .retryStrategy(RetryMode.STANDARD)
                .build();

            redshiftDataAsyncClient = RedshiftDataAsyncClient.builder()
                .httpClient(httpClient)
                .overrideConfiguration(overrideConfig)
                .build();
        }
        return redshiftDataAsyncClient;
    }

    /**
     * Creates a new Amazon Redshift cluster asynchronously.
     * @param clusterId     the unique identifier for the cluster
     * @param username      the username for the administrative user
     * @param userPassword  the password for the administrative user
     * @return a CompletableFuture that represents the asynchronous operation of
creating the cluster
```

```
     * @throws RuntimeException if the cluster creation fails
     */
    public CompletableFuture<CreateClusterResponse> createClusterAsync(String
clusterId, String username, String userPassword) {
        CreateClusterRequest clusterRequest = CreateClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .masterUsername(username)
            .masterUserPassword(userPassword)
            .nodeType("ra3.4xlarge")
            .publiclyAccessible(true)
            .numberOfNodes(2)
            .build();

        return getAsyncClient().createCluster(clusterRequest)
            .whenComplete((response, exception) -> {
                if (response != null) {
                    logger.info("Created cluster ");
                } else {
                    throw new RuntimeException("Failed to create cluster: " +
exception.getMessage(), exception);
                }
            });
    }

    /**
     * Waits asynchronously for the specified cluster to become available.
     * @param clusterId the identifier of the cluster to wait for
     * @return a {@link CompletableFuture} that completes when the cluster is
ready
     */
    public CompletableFuture<Void> waitForClusterReadyAsync(String clusterId) {
        DescribeClustersRequest clustersRequest =
DescribeClustersRequest.builder()
            .clusterIdentifier(clusterId)
            .build();

        logger.info("Waiting for cluster to become available. This may take a few
minutes.");
        long startTime = System.currentTimeMillis();

        // Recursive method to poll the cluster status.
        return checkClusterStatusAsync(clustersRequest, startTime);
    }
```

```
   private CompletableFuture<Void>
checkClusterStatusAsync(DescribeClustersRequest clustersRequest, long startTime)
{
       return getAsyncClient().describeClusters(clustersRequest)
           .thenCompose(clusterResponse -> {
               List<Cluster> clusterList = clusterResponse.clusters();
               boolean clusterReady = false;
               for (Cluster cluster : clusterList) {
                   if ("available".equals(cluster.clusterStatus())) {
                       clusterReady = true;
                       break;
                   }
               }

               if (clusterReady) {
                   logger.info(String.format("Cluster is available!"));
                   return CompletableFuture.completedFuture(null);
               } else {
                   long elapsedTimeMillis = System.currentTimeMillis() -
startTime;
                   long elapsedSeconds = elapsedTimeMillis / 1000;
                   long minutes = elapsedSeconds / 60;
                   long seconds = elapsedSeconds % 60;
                   System.out.printf("\rElapsed Time: %02d:%02d - Waiting for
cluster...", minutes, seconds);
                   System.out.flush();

                   // Wait 1 second before the next status check
                   return CompletableFuture.runAsync(() -> {
                       try {
                           TimeUnit.SECONDS.sleep(1);
                       } catch (InterruptedException e) {
                           throw new RuntimeException("Error during sleep: " +
e.getMessage(), e);
                       }
                   }).thenCompose(ignored ->
checkClusterStatusAsync(clustersRequest, startTime));
               }
           }).exceptionally(exception -> {
               throw new RuntimeException("Failed to get cluster status: " +
exception.getMessage(), exception);
           });
   }
```

```
   /**
    * Lists all databases asynchronously for the specified cluster, database
user, and database.
    * @param clusterId the identifier of the cluster to list databases for
    * @param dbUser the database user to use for the list databases request
    * @param database the database to list databases for
    * @return a {@link CompletableFuture} that completes when the database
listing is complete, or throws a {@link RuntimeException} if there was an error
    */
   public CompletableFuture<Void> listAllDatabasesAsync(String clusterId, String
dbUser, String database) {
       ListDatabasesRequest databasesRequest = ListDatabasesRequest.builder()
           .clusterIdentifier(clusterId)
           .dbUser(dbUser)
           .database(database)
           .build();

       // Asynchronous paginator for listing databases.
       ListDatabasesPublisher databasesPaginator =
getAsyncDataClient().listDatabasesPaginator(databasesRequest);
       CompletableFuture<Void> future = databasesPaginator.subscribe(response ->
{
           response.databases().forEach(db -> {
               logger.info("The database name is {} ", db);
           });
       });

       // Return the future for asynchronous handling.
       return future.exceptionally(exception -> {
           throw new RuntimeException("Failed to list databases: " +
exception.getMessage(), exception);
       });
   }

   /**
    * Creates an asynchronous task to execute a SQL statement for creating a new
table.
    *
    * @param clusterId    the identifier of the Amazon Redshift cluster
    * @param databaseName the name of the database to create the table in
    * @param userName     the username to use for the database connection
    * @return a {@link CompletableFuture} that completes with the result of the
SQL statement execution
    * @throws RuntimeException if there is an error creating the table
```

```
    */
   public CompletableFuture<ExecuteStatementResponse> createTableAsync(String
clusterId, String databaseName, String userName) {
       ExecuteStatementRequest createTableRequest =
ExecuteStatementRequest.builder()
           .clusterIdentifier(clusterId)
           .dbUser(userName)
           .database(databaseName)
           .sql("CREATE TABLE Movies (" +
               "id INT PRIMARY KEY, " +
               "title VARCHAR(100), " +
               "year INT)")
           .build();

       return getAsyncDataClient().executeStatement(createTableRequest)
           .whenComplete((response, exception) -> {
               if (exception != null) {
                   throw new RuntimeException("Error creating table: " +
exception.getMessage(), exception);
               } else {
                   logger.info("Table created: Movies");
               }
           });
   }

   /**
    * Asynchronously pops a table from a JSON file.
    *
    * @param clusterId   the ID of the cluster
    * @param databaseName the name of the database
    * @param userName    the username
    * @param fileName    the name of the JSON file
    * @param number      the number of records to process
    * @return a CompletableFuture that completes with the number of records
added to the Movies table
    */
   public CompletableFuture<Integer> popTableAsync(String clusterId, String
databaseName, String userName, String fileName, int number) {
       return CompletableFuture.supplyAsync(() -> {
               try {
                   JsonParser parser = new JsonFactory().createParser(new
File(fileName));
                   JsonNode rootNode = new ObjectMapper().readTree(parser);
                   Iterator<JsonNode> iter = rootNode.iterator();
```

```
                    return iter;
                } catch (IOException e) {
                    throw new RuntimeException("Failed to read or parse JSON
file: " + e.getMessage(), e);
                }
            }).thenCompose(iter -> processNodesAsync(clusterId, databaseName,
userName, iter, number))
            .whenComplete((result, exception) -> {
                if (exception != null) {
                    logger.info("Error {} ", exception.getMessage());
                } else {
                    logger.info("{} records were added to the Movies table." ,
result);
                }
            });
    }

    private CompletableFuture<Integer> processNodesAsync(String clusterId, String
databaseName, String userName, Iterator<JsonNode> iter, int number) {
        return CompletableFuture.supplyAsync(() -> {
            int t = 0;
            try {
                while (iter.hasNext()) {
                    if (t == number)
                        break;
                    JsonNode currentNode = iter.next();
                    int year = currentNode.get("year").asInt();
                    String title = currentNode.get("title").asText();

                    // Use SqlParameter to avoid SQL injection.
                    List<SqlParameter> parameterList = new ArrayList<>();
                    String sqlStatement = "INSERT INTO Movies
VALUES( :id , :title, :year);";
                    SqlParameter idParam = SqlParameter.builder()
                        .name("id")
                        .value(String.valueOf(t))
                        .build();

                    SqlParameter titleParam = SqlParameter.builder()
                        .name("title")
                        .value(title)
                        .build();

                    SqlParameter yearParam = SqlParameter.builder()
```

```
                        .name("year")
                        .value(String.valueOf(year))
                        .build();
                    parameterList.add(idParam);
                    parameterList.add(titleParam);
                    parameterList.add(yearParam);

                    ExecuteStatementRequest insertStatementRequest =
ExecuteStatementRequest.builder()
                        .clusterIdentifier(clusterId)
                        .sql(sqlStatement)
                        .database(databaseName)
                        .dbUser(userName)
                        .parameters(parameterList)
                        .build();


getAsyncDataClient().executeStatement(insertStatementRequest);
                    logger.info("Inserted: " + title + " (" + year + ")");
                    t++;
                }
            } catch (RedshiftDataException e) {
                throw new RuntimeException("Error inserting data: " +
e.getMessage(), e);
            }
            return t;
        });
    }

    /**
     * Checks the status of an SQL statement asynchronously and handles the
completion of the statement.
     *
     * @param sqlId the ID of the SQL statement to check
     * @return a {@link CompletableFuture} that completes when the SQL
statement's status is either "FINISHED" or "FAILED"
     */
    public CompletableFuture<Void> checkStatementAsync(String sqlId) {
        DescribeStatementRequest statementRequest =
DescribeStatementRequest.builder()
            .id(sqlId)
            .build();

        return getAsyncDataClient().describeStatement(statementRequest)
```

```
            .thenCompose(response -> {
                String status = response.statusAsString();
                logger.info("... Status: {} ", status);

                if ("FAILED".equals(status)) {
                    throw new RuntimeException("The Query Failed. Ending
program");
                } else if ("FINISHED".equals(status)) {
                    return CompletableFuture.completedFuture(null);
                } else {
                    // Sleep for 1 second and recheck status
                    return CompletableFuture.runAsync(() -> {
                        try {
                            TimeUnit.SECONDS.sleep(1);
                        } catch (InterruptedException e) {
                            throw new RuntimeException("Error during sleep: " +
e.getMessage(), e);
                        }
                    }).thenCompose(ignore -> checkStatementAsync(sqlId)); //
Recursively call until status is FINISHED or FAILED
                }
            }).whenComplete((result, exception) -> {
                if (exception != null) {
                    // Handle exceptions
                    logger.info("Error: {} ", exception.getMessage());
                } else {
                    logger.info("The statement is finished!");
                }
            });
    }

    /**
     * Asynchronously retrieves the results of a statement execution.
     *
     * @param statementId the ID of the statement for which to retrieve the
results
     * @return a {@link CompletableFuture} that completes when the statement
result has been processed
     */
    public CompletableFuture<Void> getResultsAsync(String statementId) {
        GetStatementResultRequest resultRequest =
GetStatementResultRequest.builder()
            .id(statementId)
            .build();
```

```
       return getAsyncDataClient().getStatementResult(resultRequest)
           .handle((response, exception) -> {
               if (exception != null) {
                   logger.info("Error getting statement result {} ",
exception.getMessage());
                   throw new RuntimeException("Error getting statement result: "
+ exception.getMessage(), exception);
               }

               // Extract and print the field values using streams if the
response is valid.
               response.records().stream()
                   .flatMap(List::stream)
                   .map(Field::stringValue)
                   .filter(value -> value != null)
                   .forEach(value -> System.out.println("The Movie title field
is " + value));

               return response;
           }).thenAccept(response -> {
               // Optionally add more logic here if needed after handling the
response
           });
   }


   /**
    * Asynchronously queries movies by a given year from a Redshift database.
    *
    * @param database    the name of the database to query
    * @param dbUser      the user to connect to the database with
    * @param year        the year to filter the movies by
    * @param clusterId   the identifier of the Redshift cluster to connect to
    * @return a {@link CompletableFuture} containing the response ID of the
executed SQL statement
    */
   public CompletableFuture<String> queryMoviesByYearAsync(String database,
                                                           String dbUser,
                                                           int year,
                                                           String
clusterId) {

       String sqlStatement = "SELECT * FROM Movies WHERE year = :year";
```

```
        SqlParameter yearParam = SqlParameter.builder()
            .name("year")
            .value(String.valueOf(year))
            .build();

        ExecuteStatementRequest statementRequest =
ExecuteStatementRequest.builder()
            .clusterIdentifier(clusterId)
            .database(database)
            .dbUser(dbUser)
            .parameters(yearParam)
            .sql(sqlStatement)
            .build();

        return CompletableFuture.supplyAsync(() -> {
            try {
                ExecuteStatementResponse response =
getAsyncDataClient().executeStatement(statementRequest).join(); // Use join() to
wait for the result
                return response.id();
            } catch (RedshiftDataException e) {
                throw new RuntimeException("Error executing statement: " +
e.getMessage(), e);
            }
        }).exceptionally(exception -> {
            logger.info("Error: {}", exception.getMessage());
            return "";
        });
    }

    /**
     * Modifies an Amazon Redshift cluster asynchronously.
     *
     * @param clusterId the identifier of the cluster to be modified
     * @return a {@link CompletableFuture} that completes when the cluster
modification is complete
     */
    public CompletableFuture<ModifyClusterResponse> modifyClusterAsync(String
clusterId) {
        ModifyClusterRequest modifyClusterRequest =
ModifyClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .preferredMaintenanceWindow("wed:07:30-wed:08:00")
            .build();
```

```
        return getAsyncClient().modifyCluster(modifyClusterRequest)
            .whenComplete((clusterResponse, exception) -> {
                if (exception != null) {
                    if (exception.getCause() instanceof RedshiftException) {
                        logger.info("Error: {} ", exception.getMessage());
                    } else {
                        logger.info("Unexpected error: {} ",
exception.getMessage());
                    }
                } else {
                    logger.info("The modified cluster was successfully modified
and has "
                        + clusterResponse.cluster().preferredMaintenanceWindow()
+ " as the maintenance window");
                }
            });
    }

    /**
     * Deletes a Redshift cluster asynchronously.
     *
     * @param clusterId the identifier of the Redshift cluster to be deleted
     * @return a {@link CompletableFuture} that represents the asynchronous
operation of deleting the Redshift cluster
     */
    public CompletableFuture<DeleteClusterResponse>
deleteRedshiftClusterAsync(String clusterId) {
        DeleteClusterRequest deleteClusterRequest =
DeleteClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .skipFinalClusterSnapshot(true)
            .build();

        return getAsyncClient().deleteCluster(deleteClusterRequest)
            .whenComplete((response, exception) -> {
                if (exception != null) {
                    // Handle exceptions
                    if (exception.getCause() instanceof RedshiftException) {
                        logger.info("Error: {}", exception.getMessage());
                    } else {
                        logger.info("Unexpected error: {}",
exception.getMessage());
                    }
```

```
                } else {
                    // Handle successful response
                    logger.info("The status is {}",
 response.cluster().clusterStatus());
                }
            });
    }
}
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK for Java 2.x .
  - CreateCluster
  - DescribeClusters
  - DescribeStatement
  - ExecuteStatement
  - GetStatementResult
  - ListDatabasesPaginator
  - ModifyCluster

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class RedshiftScenario:
    """Runs an interactive scenario that shows how to get started with
 Redshift."""

    def __init__(self, redshift_wrapper, redshift_data_wrapper):
        self.redshift_wrapper = redshift_wrapper
        self.redshift_data_wrapper = redshift_data_wrapper
```

```
    def redhift_scenario(self, json_file_path):
        database_name = "dev"

        print(DASHES)
        print("Welcome to the Amazon Redshift SDK Getting Started example.")
        print(
            """
      This Python program demonstrates how to interact with Amazon Redshift
      using the AWS SDK for Python (Boto3).

      Amazon Redshift is a fully managed, petabyte-scale data warehouse
      service hosted in the cloud.

      The program's primary functionalities include cluster creation,
      verification of cluster readiness, listing databases, table creation,
      populating data within the table, and executing SQL statements.

      It also demonstrates querying data from the Movies table.

      Upon completion, all AWS resources are cleaned up.
    """
        )
        if not os.path.isfile(json_file_path):
            logging.error(f"The file {json_file_path} does not exist.")
            return

        print("Let's get started...")
        user_name = q.ask("Please enter your user name (default is awsuser):")
        user_name = user_name if user_name else "awsuser"

        print(DASHES)
        user_password = q.ask(
            "Please enter your user password (default is AwsUser1000):"
        )
        user_password = user_password if user_password else "AwsUser1000"

        print(DASHES)
        print(
            """A Redshift cluster refers to the collection of computing resources
and storage that work
            together to process and analyze large volumes of data."""
        )
        cluster_id = q.ask(
```

```
            "Enter a cluster identifier value (default is redshift-cluster-
movies): "
        )
        cluster_id = cluster_id if cluster_id else "redshift-cluster-movies"

        self.redshift_wrapper.create_cluster(
            cluster_id, "ra3.4xlarge", user_name, user_password, True, 2
        )

        print(DASHES)
        print(f"Wait until {cluster_id} is available. This may take a few
 minutes...")
        q.ask("Press Enter to continue...")

        self.wait_cluster_available(cluster_id)

        print(DASHES)

        print(
            f"""
      When you created {cluster_id}, the dev database is created by default and
 used in this scenario.

      To create a custom database, you need to have a CREATEDB privilege.
      For more information, see the documentation here:
      https://docs.aws.amazon.com/redshift/latest/dg/r_CREATE_DATABASE.html.
     """
        )
        q.ask("Press Enter to continue...")
        print(DASHES)

        print(DASHES)
        print(f"List databases in {cluster_id}")
        q.ask("Press Enter to continue...")
        databases = self.redshift_data_wrapper.list_databases(
            cluster_id, database_name, user_name
        )
        print(f"The cluster contains {len(databases)} database(s).")
        for database in databases:
            print(f"    Database: {database}")
        print(DASHES)

        print(DASHES)
        print("Now you will create a table named Movies.")
```

```
        q.ask("Press Enter to continue...")

        self.create_table(cluster_id, database_name, user_name)

        print(DASHES)

        print("Populate the Movies table using the Movies.json file.")
        print(
            "Specify the number of records you would like to add to the Movies
Table."
        )
        print("Please enter a value between 50 and 200.")

        while True:
            try:
                num_records = int(q.ask("Enter a value: ", q.is_int))
                if 50 <= num_records <= 200:
                    break
                else:
                    print("Invalid input. Please enter a value between 50 and
200.")
            except ValueError:
                print("Invalid input. Please enter a value between 50 and 200.")

        self.populate_table(
            cluster_id, database_name, user_name, json_file_path, num_records
        )

        print(DASHES)
        print("Query the Movies table by year. Enter a value between 2012-2014.")

        while True:
            movie_year = int(q.ask("Enter a year: ", q.is_int))
            if 2012 <= movie_year <= 2014:
                break
            else:
                print("Invalid input. Please enter a valid year between 2012 and
2014.")

        # Function to query database
        sql_id = self.query_movies_by_year(
            database_name, user_name, movie_year, cluster_id
        )
```

```
        print(f"The identifier of the statement is {sql_id}")

        print("Checking statement status...")
        self.wait_statement_finished(sql_id)
        result = self.redshift_data_wrapper.get_statement_result(sql_id)

        self.display_movies(result)

        print(DASHES)

        print(DASHES)
        print("Now you will modify the Redshift cluster.")
        q.ask("Press Enter to continue...")

        preferred_maintenance_window = "wed:07:30-wed:08:00"
        self.redshift_wrapper.modify_cluster(cluster_id,
preferred_maintenance_window)

        print(DASHES)

        print(DASHES)
        delete = q.ask("Do you want to delete the cluster? (y/n) ", q.is_yesno)

        if delete:
            print(f"You selected to delete {cluster_id}")
            q.ask("Press Enter to continue...")
            self.redshift_wrapper.delete_cluster(cluster_id)
        else:
            print(f"Cluster {cluster_id}cluster_id was not deleted")

        print(DASHES)
        print("This concludes the Amazon Redshift SDK Getting Started scenario.")
        print(DASHES)

    def create_table(self, cluster_id, database, username):
        self.redshift_data_wrapper.execute_statement(
            cluster_identifier=cluster_id,
            database_name=database,
            user_name=username,
            sql="CREATE TABLE Movies (statement_id INT PRIMARY KEY, title
VARCHAR(100), year INT)",
        )

        print("Table created: Movies")
```

```
    def populate_table(self, cluster_id, database, username, file_name, number):
        with open(file_name) as f:
            data = json.load(f)

        i = 0
        for record in data:
            if i == number:
                break

            statement_id = i
            title = record["title"]
            year = record["year"]
            i = i + 1
            parameters = [
                {"name": "statement_id", "value": str(statement_id)},
                {"name": "title", "value": title},
                {"name": "year", "value": str(year)},
            ]

            self.redshift_data_wrapper.execute_statement(
                cluster_identifier=cluster_id,
                database_name=database,
                user_name=username,
                sql="INSERT INTO Movies VALUES(:statement_id, :title, :year)",
                parameter_list=parameters,
            )

        print(f"{i} records inserted into Movies table")

    def wait_cluster_available(self, cluster_id):
        """
        Waits for a cluster to be available.

        :param cluster_id: The cluster identifier.

        Note: The cluster_available waiter can also be used.
        It is not used in this case to allow an elapsed time message.
        """
        cluster_ready = False
        start_time = time.time()

        while not cluster_ready:
```

```
            time.sleep(30)
            cluster = self.redshift_wrapper.describe_clusters(cluster_id)
            status = cluster[0]["ClusterStatus"]
            if status == "available":
                cluster_ready = True
            elif status != "creating":
                raise Exception(
                    f"Cluster {cluster_id} creation failed with status {status}."
                )

            elapsed_seconds = int(round(time.time() - start_time))
            minutes = int(elapsed_seconds // 60)
            seconds = int(elapsed_seconds % 60)

            print(f"Elapsed Time: {minutes}:{seconds:02d} - status {status}...")

            if minutes > 30:
                raise Exception(
                    f"Cluster {cluster_id} is not available after 30 minutes."
                )

    def query_movies_by_year(self, database, username, year, cluster_id):
        sql = "SELECT * FROM Movies WHERE year = :year"

        params = [{"name": "year", "value": str(year)}]

        response = self.redshift_data_wrapper.execute_statement(
            cluster_identifier=cluster_id,
            database_name=database,
            user_name=username,
            sql=sql,
            parameter_list=params,
        )

        return response["Id"]

    @staticmethod
    def display_movies(response):
        metadata = response["ColumnMetadata"]
        records = response["Records"]

        title_column_index = None
        for i in range(len(metadata)):
            if metadata[i]["name"] == "title":
```

```
                title_column_index = i
                break

        if title_column_index is None:
            print("No title column found.")
            return

        print(f"Found {len(records)} movie(s).")
        for record in records:
            print(f"   {record[title_column_index]['stringValue']}")

    def wait_statement_finished(self, sql_id):
        while True:
            time.sleep(1)
            response = self.redshift_data_wrapper.describe_statement(sql_id)
            status = response["Status"]
            print(f"Statement status is {status}.")

            if status == "FAILED":
                print(f"The query failed because {response['Error']}. Ending
 program")
                raise Exception("The Query Failed. Ending program")
            elif status == "FINISHED":
                break
```

Fonction principale montrant la mise en œuvre du scénario.

```
def main():
    redshift_client = boto3.client("redshift")
    redshift_data_client = boto3.client("redshift-data")
    redshift_wrapper = RedshiftWrapper(redshift_client)
    redshift_data_wrapper = RedshiftDataWrapper(redshift_data_client)
    redshift_scenario = RedshiftScenario(redshift_wrapper, redshift_data_wrapper)
    redshift_scenario.redhift_scenario(
        f"{os.path.dirname(__file__)}/../../../resources/sample_files/
movies.json"
    )
```

Les fonctions d'encapsuleur utilisées dans le scénario.

```
    def create_cluster(
        self,
        cluster_identifier,
        node_type,
        master_username,
        master_user_password,
        publicly_accessible,
        number_of_nodes,
    ):
        """
        Creates a cluster.

        :param cluster_identifier: The name of the cluster.
        :param node_type: The type of node in the cluster.
        :param master_username: The master username.
        :param master_user_password: The master user password.
        :param publicly_accessible: Whether the cluster is publicly accessible.
        :param number_of_nodes: The number of nodes in the cluster.
        :return: The cluster.
        """

        try:
            cluster = self.client.create_cluster(
                ClusterIdentifier=cluster_identifier,
                NodeType=node_type,
                MasterUsername=master_username,
                MasterUserPassword=master_user_password,
                PubliclyAccessible=publicly_accessible,
                NumberOfNodes=number_of_nodes,
            )
            return cluster
        except ClientError as err:
            logging.error(
                "Couldn't create a cluster. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


    def describe_clusters(self, cluster_identifier):
        """
```

```
        Describes a cluster.

        :param cluster_identifier: The cluster identifier.
        :return: A list of clusters.
        """
        try:
            kwargs = {}
            if cluster_identifier:
                kwargs["ClusterIdentifier"] = cluster_identifier

            paginator = self.client.get_paginator("describe_clusters")
            clusters = []
            for page in paginator.paginate(**kwargs):
                clusters.extend(page["Clusters"])

            return clusters

        except ClientError as err:
            logging.error(
                "Couldn't describe a cluster. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


    def execute_statement(
        self, cluster_identifier, database_name, user_name, sql,
parameter_list=None
    ):
        """
        Executes a SQL statement.

        :param cluster_identifier: The cluster identifier.
        :param database_name: The database name.
        :param user_name: The user's name.
        :param sql: The SQL statement.
        :param parameter_list: The optional SQL statement parameters.
        :return: The SQL statement result.
        """

        try:
            kwargs = {
                "ClusterIdentifier": cluster_identifier,
```

```
                "Database": database_name,
                "DbUser": user_name,
                "Sql": sql,
            }
            if parameter_list:
                kwargs["Parameters"] = parameter_list
            response = self.client.execute_statement(**kwargs)
            return response
        except ClientError as err:
            logging.error(
                "Couldn't execute statement. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


    def describe_statement(self, statement_id):
        """
        Describes a SQL statement.

        :param statement_id: The SQL statement identifier.
        :return: The SQL statement result.
        """
        try:
            response = self.client.describe_statement(Id=statement_id)
            return response
        except ClientError as err:
            logging.error(
                "Couldn't describe statement. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


    def get_statement_result(self, statement_id):
        """
        Gets the result of a SQL statement.

        :param statement_id: The SQL statement identifier.
        :return: The SQL statement result.
        """
        try:
```

```
            result = {
                "Records": [],
            }
            paginator = self.client.get_paginator("get_statement_result")
            for page in paginator.paginate(Id=statement_id):
                if "ColumnMetadata" not in result:
                    result["ColumnMetadata"] = page["ColumnMetadata"]
                result["Records"].extend(page["Records"])
            return result
        except ClientError as err:
            logging.error(
                "Couldn't get statement result. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


    def modify_cluster(self, cluster_identifier, preferred_maintenance_window):
        """
        Modifies a cluster.

        :param cluster_identifier: The cluster identifier.
        :param preferred_maintenance_window: The preferred maintenance window.
        """
        try:
            self.client.modify_cluster(
                ClusterIdentifier=cluster_identifier,
                PreferredMaintenanceWindow=preferred_maintenance_window,
            )
        except ClientError as err:
            logging.error(
                "Couldn't modify a cluster. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


    def list_databases(self, cluster_identifier, database_name, database_user):
        """
        Lists databases in a cluster.

        :param cluster_identifier: The cluster identifier.
```

```
        :param database_name: The database name.
        :param database_user: The database user.
        :return: The list of databases.
        """
        try:
            paginator = self.client.get_paginator("list_databases")
            databases = []
            for page in paginator.paginate(
                ClusterIdentifier=cluster_identifier,
                Database=database_name,
                DbUser=database_user,
            ):
                databases.extend(page["Databases"])

            return databases
        except ClientError as err:
            logging.error(
                "Couldn't list databases. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


    def delete_cluster(self, cluster_identifier):
        """
        Deletes a cluster.

        :param cluster_identifier: The cluster identifier.
        """
        try:
            self.client.delete_cluster(
                ClusterIdentifier=cluster_identifier,
SkipFinalClusterSnapshot=True
            )
        except ClientError as err:
            logging.error(
                "Couldn't delete a cluster. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK for Python (Boto3).
  - CreateCluster
  - DescribeClusters
  - DescribeStatement
  - ExecuteStatement
  - GetStatementResult
  - ListDatabasesPaginator
  - ModifyCluster

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezL'utilisation de ce service avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Actions pour Amazon Redshift utilisant AWS Kits SDK

Les exemples de code suivants montrent comment effectuer des actions Amazon Redshift individuelles avec AWS des SDK. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Ces extraits appellent l'API Amazon Redshift et sont des extraits de code de programmes plus volumineux qui doivent être exécutés en contexte. Vous pouvez voir les actions dans leur contexte dans Scénarios d'utilisation d'Amazon Redshift AWS Kits SDK.

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour obtenir la liste complète, consultez la référence des API Amazon Redshift.

Exemples

- À utiliser CreateClusteravec un AWS SDK ou CLI
- À utiliser DeleteClusteravec un AWS SDK ou CLI
- À utiliser DescribeClustersavec un AWS SDK ou CLI
- À utiliser DescribeStatementavec un AWS Kit SDK
- À utiliser ExecuteStatementavec un AWS Kit SDK
- À utiliser GetStatementResultavec un AWS Kit SDK

- À utiliser ListDatabasesavec un AWS Kit SDK
- À utiliser ModifyClusteravec un AWS SDK ou CLI

À utiliser **`CreateCluster`**avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `CreateCluster`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans les exemples de code suivants :

- Principes de base
- Commencer à utiliser des clusters d'entrepôts de données provisionnés

.NET

SDK pour .NET (v4)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /// <summary>
   /// Create a new Amazon Redshift cluster.
   /// </summary>
   /// <param name="clusterIdentifier">The identifier for the cluster.</param>
   /// <param name="databaseName">The name of the database.</param>
   /// <param name="masterUsername">The master username.</param>
   /// <param name="masterUserPassword">The master user password.</param>
   /// <param name="nodeType">The node type for the cluster.</param>
   /// <returns>The cluster that was created.</returns>
   public async Task<Cluster> CreateClusterAsync(string clusterIdentifier,
string databaseName,
       string masterUsername, string masterUserPassword, string nodeType =
"ra3.large")
   {
       try
       {
```

```
            var request = new CreateClusterRequest
            {
                ClusterIdentifier = clusterIdentifier,
                DBName = databaseName,
                MasterUsername = masterUsername,
                MasterUserPassword = masterUserPassword,
                NodeType = nodeType,
                NumberOfNodes = 1,
                ClusterType = "single-node"
            };

            var response = await _redshiftClient.CreateClusterAsync(request);
            Console.WriteLine($"Created cluster {clusterIdentifier}");
            return response.Cluster;
        }
        catch (ClusterAlreadyExistsException ex)
        {
            Console.WriteLine($"Cluster already exists: {ex.Message}");
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't create cluster. Here's why:
{ex.Message}");
            throw;
        }
    }
```

- Pour plus de détails sur l'API, voir CreateClusterla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

L' ParametersThis exemple Create a Cluster with Minimal crée un cluster avec un ensemble minimal de paramètres. JSON est le format de sortie par défaut. Commande :

```
aws redshift create-cluster --node-type dw.hs1.xlarge --number-of-nodes 2 --
master-username adminuser --master-user-password TopSecret1 --cluster-identifier
 mycluster
```

Résultat :

```
{
   "Cluster": {
      "NodeType": "dw.hs1.xlarge",
      "ClusterVersion": "1.0",
      "PubliclyAccessible": "true",
      "MasterUsername": "adminuser",
      "ClusterParameterGroups": [
         {
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "default.redshift-1.0"
         } ],
      "ClusterSecurityGroups": [
         {
            "Status": "active",
            "ClusterSecurityGroupName": "default"
         } ],
      "AllowVersionUpgrade": true,
      "VpcSecurityGroups": \[],
      "PreferredMaintenanceWindow": "sat:03:30-sat:04:00",
      "AutomatedSnapshotRetentionPeriod": 1,
      "ClusterStatus": "creating",
      "ClusterIdentifier": "mycluster",
      "DBName": "dev",
      "NumberOfNodes": 2,
      "PendingModifiedValues": {
         "MasterUserPassword": "\****"
      }
   },
   "ResponseMetadata": {
      "RequestId": "7cf4bcfc-64dd-11e2-bea9-49e0ce183f07"
   }
}
```

- Pour plus de détails sur l'API, voir CreateClusterla section Référence des AWS CLI commandes.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import (
 "context"
 "errors"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/redshift"
 "github.com/aws/aws-sdk-go-v2/service/redshift/types"
)



// RedshiftActions wraps Redshift service actions.
type RedshiftActions struct {
 RedshiftClient *redshift.Client
}



// CreateCluster sends a request to create a cluster with the given clusterId
 using the provided credentials.
func (actor RedshiftActions) CreateCluster(ctx context.Context, clusterId string,
 userName string, userPassword string, nodeType string, clusterType string,
 publiclyAccessible bool) (*redshift.CreateClusterOutput, error) {
 // Create a new Redshift cluster
 input := &redshift.CreateClusterInput{
  ClusterIdentifier:  aws.String(clusterId),
  MasterUserPassword: aws.String(userPassword),
  MasterUsername:     aws.String(userName),
  NodeType:           aws.String(nodeType),
```

```
  ClusterType:        aws.String(clusterType),
  PubliclyAccessible: aws.Bool(publiclyAccessible),
 }
 var opErr *types.ClusterAlreadyExistsFault
 output, err := actor.RedshiftClient.CreateCluster(ctx, input)
 if err != nil && errors.As(err, &opErr) {
  log.Println("Cluster already exists")
  return nil, nil
 } else if err != nil {
  log.Printf("Failed to create Redshift cluster: %v\n", err)
  return nil, err
 }

 log.Printf("Created cluster %s\n", *output.Cluster.ClusterIdentifier)
 return output, nil
}
```

- Pour plus de détails sur l'API, voir CreateClusterla section Référence des AWS SDK pour Go API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez le cluster.

```
    /**
     * Creates a new Amazon Redshift cluster asynchronously.
     * @param clusterId     the unique identifier for the cluster
     * @param username      the username for the administrative user
     * @param userPassword  the password for the administrative user
     * @return a CompletableFuture that represents the asynchronous operation of
 creating the cluster
```

```
     * @throws RuntimeException if the cluster creation fails
     */
    public CompletableFuture<CreateClusterResponse> createClusterAsync(String
clusterId, String username, String userPassword) {
        CreateClusterRequest clusterRequest = CreateClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .masterUsername(username)
            .masterUserPassword(userPassword)
            .nodeType("ra3.4xlarge")
            .publiclyAccessible(true)
            .numberOfNodes(2)
            .build();

        return getAsyncClient().createCluster(clusterRequest)
            .whenComplete((response, exception) -> {
                if (response != null) {
                    logger.info("Created cluster ");
                } else {
                    throw new RuntimeException("Failed to create cluster: " +
exception.getMessage(), exception);
                }
            });
    }
```

- Pour plus de détails sur l'API, voir CreateClusterla section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez le client.

```
import { RedshiftClient } from "@aws-sdk/client-redshift";
```

```
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Créez le cluster.

```
// Import required AWS SDK clients and commands for Node.js
import { CreateClusterCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "./libs/redshiftClient.js";

const params = {
  ClusterIdentifier: "CLUSTER_NAME", // Required
  NodeType: "NODE_TYPE", //Required
  MasterUsername: "MASTER_USER_NAME", // Required - must be lowercase
  MasterUserPassword: "MASTER_USER_PASSWORD", // Required - must contain at least
 one uppercase letter, and one number
  ClusterType: "CLUSTER_TYPE", // Required
  IAMRoleARN: "IAM_ROLE_ARN", // Optional - the ARN of an IAM role with
 permissions your cluster needs to access other AWS services on your behalf, such
 as Amazon S3.
  ClusterSubnetGroupName: "CLUSTER_SUBNET_GROUPNAME", //Optional - the name of a
 cluster subnet group to be associated with this cluster. Defaults to 'default'
 if not specified.
  DBName: "DATABASE_NAME", // Optional - defaults to 'dev' if not specified
  Port: "PORT_NUMBER", // Optional - defaults to '5439' if not specified
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new CreateClusterCommand(params));
    console.log(
      `Cluster ${data.Cluster.ClusterIdentifier} successfully created`,
    );
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- Pour plus de détails sur l'API, voir CreateClusterla section Référence des AWS SDK pour JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez le cluster.

```
suspend fun createCluster(
    clusterId: String?,
    masterUsernameVal: String?,
    masterUserPasswordVal: String?,
) {
    val clusterRequest =
        CreateClusterRequest {
            clusterIdentifier = clusterId
            availabilityZone = "us-east-1a"
            masterUsername = masterUsernameVal
            masterUserPassword = masterUserPasswordVal
            nodeType = "ra3.4xlarge"
            publiclyAccessible = true
            numberOfNodes = 2
        }

    RedshiftClient.fromEnvironment { region = "us-east-1" }.use { redshiftClient
 ->
        val clusterResponse = redshiftClient.createCluster(clusterRequest)
        println("Created cluster ${clusterResponse.cluster?.clusterIdentifier}")
    }
}
```

- Pour plus de détails sur l'API, consultez CreateClusterla section AWS SDK pour la référence de l'API Kotlin.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
        self.client = redshift_client


    def create_cluster(
        self,
        cluster_identifier,
        node_type,
        master_username,
        master_user_password,
        publicly_accessible,
        number_of_nodes,
    ):
        """
        Creates a cluster.

        :param cluster_identifier: The name of the cluster.
        :param node_type: The type of node in the cluster.
        :param master_username: The master username.
        :param master_user_password: The master user password.
        :param publicly_accessible: Whether the cluster is publicly accessible.
        :param number_of_nodes: The number of nodes in the cluster.
        :return: The cluster.
        """
```

```
        try:
            cluster = self.client.create_cluster(
                ClusterIdentifier=cluster_identifier,
                NodeType=node_type,
                MasterUsername=master_username,
                MasterUserPassword=master_user_password,
                PubliclyAccessible=publicly_accessible,
                NumberOfNodes=number_of_nodes,
            )
            return cluster
        except ClientError as err:
            logging.error(
                "Couldn't create a cluster. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

Le code suivant instancie l' RedshiftWrapper objet.

```
    client = boto3.client("redshift")
    redhift_wrapper = RedshiftWrapper(client)
```

- Pour plus de détails sur l'API, consultez CreateClusterle AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez le cluster.

```
    TRY.
        " Example values: iv_cluster_identifier = 'my-redshift-cluster'
        " Example values: iv_node_type = 'ra3.4xlarge'
        " Example values: iv_master_username = 'awsuser'
        " Example values: iv_master_password = 'AwsUser1000'
        " Example values: iv_publicly_accessible = abap_true
        " Example values: iv_number_of_nodes = 2
        oo_result = lo_rsh->createcluster(
          iv_clusteridentifier = iv_cluster_identifier
          iv_nodetype = iv_node_type
          iv_masterusername = iv_master_username
          iv_masteruserpassword = iv_master_password
          iv_publiclyaccessible = iv_publicly_accessible
          iv_numberofnodes = iv_number_of_nodes
        ).
        MESSAGE 'Redshift cluster created successfully.' TYPE 'I'.
      CATCH /aws1/cx_rshclustalrdyexfault.
        MESSAGE 'Cluster already exists.' TYPE 'I'.
      CATCH /aws1/cx_rshclstquotaexcdfault.
        MESSAGE 'Cluster quota exceeded.' TYPE 'I'.
    ENDTRY.
```

- Pour plus de détails sur l'API, consultez CreateClusterla section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezL'utilisation de ce service avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **`DeleteCluster`**avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `DeleteCluster`.

Les exemples d’actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l’exemple de code suivant :

- Commencer à utiliser des clusters d'entrepôts de données provisionnés

.NET

SDK pour .NET (v4)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /// <summary>
   /// Delete an Amazon Redshift cluster without a final snapshot.
   /// </summary>
   /// <param name="clusterIdentifier">The identifier for the cluster.</param>
   /// <returns>True if successful.</returns>
   public async Task<bool> DeleteClusterWithoutSnapshotAsync(string
clusterIdentifier)
   {
       try
       {
           var request = new DeleteClusterRequest
           {
               ClusterIdentifier = clusterIdentifier,
               SkipFinalClusterSnapshot = true
           };

           var response = await _redshiftClient.DeleteClusterAsync(request);
           Console.WriteLine($"The {clusterIdentifier} was deleted");
           return true;
       }
       catch (ClusterNotFoundException ex)
       {
           Console.WriteLine($"Cluster not found: {ex.Message}");
           return false;
       }
       catch (Exception ex)
       {
           Console.WriteLine($"Couldn't delete cluster. Here's why:
{ex.Message}");
           return false;
       }
   }
```

- Pour plus de détails sur l'API, voir DeleteClusterla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Supprimer un cluster sans cluster final SnapshotThis Exemple de suppression d'un cluster, forçant ainsi la suppression des données afin qu'aucun instantané final du cluster ne soit créé.Commande :

```
aws redshift delete-cluster --cluster-identifier mycluster --skip-final-cluster-snapshot
```

Supprimer un cluster, autoriser un cluster final, SnapshotThis par exemple, supprime un cluster, mais spécifie un instantané du cluster.Commande :

```
aws redshift delete-cluster --cluster-identifier mycluster --final-cluster-snapshot-identifier myfinalsnapshot
```

- Pour plus de détails sur l'API, voir DeleteClusterla section Référence des AWS CLI commandes.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import (
 "context"
 "errors"
```

```
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/redshift"
 "github.com/aws/aws-sdk-go-v2/service/redshift/types"
)



// RedshiftActions wraps Redshift service actions.
type RedshiftActions struct {
 RedshiftClient *redshift.Client
}



// DeleteCluster deletes the given cluster.
func (actor RedshiftActions) DeleteCluster(ctx context.Context, clusterId string)
 (bool, error) {
 input := redshift.DeleteClusterInput{
  ClusterIdentifier:        aws.String(clusterId),
  SkipFinalClusterSnapshot: aws.Bool(true),
 }
 _, err := actor.RedshiftClient.DeleteCluster(ctx, &input)
 var opErr *types.ClusterNotFoundFault
 if err != nil && errors.As(err, &opErr) {
  log.Println("Cluster was not found. Where could it be?")
  return false, err
 } else if err != nil {
  log.Printf("Failed to delete Redshift cluster: %v\n", err)
  return false, err
 }
 waiter := redshift.NewClusterDeletedWaiter(actor.RedshiftClient)
 err = waiter.Wait(ctx, &redshift.DescribeClustersInput{
  ClusterIdentifier: aws.String(clusterId),
 }, 5*time.Minute)
 if err != nil {
  log.Printf("Wait time exceeded for deleting cluster, continuing: %v\n", err)
 }
 log.Printf("The cluster %s was deleted\n", clusterId)
 return true, nil
}
```

- Pour plus de détails sur l'API, voir DeleteClusterla section Référence des AWS SDK pour Go API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Supprimez le cluster.

```
    /**
     * Deletes a Redshift cluster asynchronously.
     *
     * @param clusterId the identifier of the Redshift cluster to be deleted
     * @return a {@link CompletableFuture} that represents the asynchronous
operation of deleting the Redshift cluster
     */
    public CompletableFuture<DeleteClusterResponse>
deleteRedshiftClusterAsync(String clusterId) {
        DeleteClusterRequest deleteClusterRequest =
DeleteClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .skipFinalClusterSnapshot(true)
            .build();

        return getAsyncClient().deleteCluster(deleteClusterRequest)
            .whenComplete((response, exception) -> {
                if (exception != null) {
                    // Handle exceptions
                    if (exception.getCause() instanceof RedshiftException) {
                        logger.info("Error: {}", exception.getMessage());
                    } else {
                        logger.info("Unexpected error: {}",
exception.getMessage());
                    }
```

```
                } else {
                    // Handle successful response
                    logger.info("The status is {}",
 response.cluster().clusterStatus());
                }
            });
    }
```

- Pour plus de détails sur l'API, voir DeleteClusterla section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez le client.

```
import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Créez le cluster.

```
// Import required AWS SDK clients and commands for Node.js
import { DeleteClusterCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "./libs/redshiftClient.js";

const params = {
  ClusterIdentifier: "CLUSTER_NAME",
  SkipFinalClusterSnapshot: false,
```

```
  FinalClusterSnapshotIdentifier: "CLUSTER_SNAPSHOT_ID",
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new DeleteClusterCommand(params));
    console.log("Success, cluster deleted. ", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- Pour plus de détails sur l'API, voir DeleteClusterla section Référence des AWS SDK pour JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Supprimez le cluster.

```
suspend fun deleteRedshiftCluster(clusterId: String?) {
    val request =
        DeleteClusterRequest {
            clusterIdentifier = clusterId
            skipFinalClusterSnapshot = true
        }

    RedshiftClient.fromEnvironment { region = "us-west-2" }.use { redshiftClient
 ->
        val response = redshiftClient.deleteCluster(request)
        println("The status is ${response.cluster?.clusterStatus}")
    }
```

```
}
```

- Pour plus de détails sur l'API, consultez DeleteClusterla section AWS SDK pour la référence de l'API Kotlin.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
        self.client = redshift_client


    def delete_cluster(self, cluster_identifier):
        """
        Deletes a cluster.

        :param cluster_identifier: The cluster identifier.
        """
        try:
            self.client.delete_cluster(
                ClusterIdentifier=cluster_identifier,
 SkipFinalClusterSnapshot=True
            )
        except ClientError as err:
            logging.error(
```

```
                "Couldn't delete a cluster. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

Le code suivant instancie l' RedshiftWrapper objet.

```
    client = boto3.client("redshift")
    redhift_wrapper = RedshiftWrapper(client)
```

- Pour plus de détails sur l'API, consultez DeleteClusterle AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Supprimez le cluster.

```
    TRY.
        " Example values: iv_cluster_identifier = 'my-redshift-cluster'
        lo_rsh->deletecluster(
          iv_clusteridentifier = iv_cluster_identifier
          iv_skipfinalclustersnapshot = abap_true
        ).
        MESSAGE 'Redshift cluster deleted successfully.' TYPE 'I'.
      CATCH /aws1/cx_rshclustnotfoundfault.
        MESSAGE 'Cluster not found.' TYPE 'I'.
      CATCH /aws1/cx_rshinvcluststatefault.
        MESSAGE 'Invalid cluster state for deletion.' TYPE 'I'.
    ENDTRY.
```

- Pour plus de détails sur l'API, consultez DeleteClusterla section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezL'utilisation de ce service avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **`DescribeClusters`**avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `DescribeClusters`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans les exemples de code suivants :

- Principes de base
- Commencer à utiliser des clusters d'entrepôts de données provisionnés

.NET

SDK pour .NET (v4)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /// <summary>
   /// Describe Amazon Redshift clusters.
   /// </summary>
   /// <param name="clusterIdentifier">Optional cluster identifier to describe a
specific cluster.</param>
   /// <returns>A list of clusters.</returns>
   public async Task<List<Cluster>> DescribeClustersAsync(string?
clusterIdentifier = null)
   {
```

```
        try
        {
            var clusters = new List<Cluster>();
            var request = new DescribeClustersRequest();
            if (!string.IsNullOrEmpty(clusterIdentifier))
            {
                request.ClusterIdentifier = clusterIdentifier;
            }

            var clustersPaginator =
_redshiftClient.Paginators.DescribeClusters(request);
            await foreach (var response in clustersPaginator.Responses)
            {
                if (response.Clusters != null)
                    clusters.AddRange(response.Clusters);
            }

            Console.WriteLine($"{clusters.Count} cluster(s) retrieved.");
            foreach (var cluster in clusters)
            {
                Console.WriteLine($"\t{cluster.ClusterIdentifier} (Status:
{cluster.ClusterStatus})");
            }

            return clusters;
        }
        catch (ClusterNotFoundException ex)
        {
            Console.WriteLine($"Cluster {clusterIdentifier} not found:
{ex.Message}");
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't describe clusters. Here's why:
{ex.Message}");
            throw;
        }
    }
```

- Pour plus de détails sur l'API, voir DescribeClustersla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

L' ClustersThis exemple Get a Description of All renvoie une description de tous les clusters du compte. JSON est le format de sortie par défaut. Commande :

```
aws redshift describe-clusters
```

Résultat :

```
{
   "Clusters": [
   {
      "NodeType": "dw.hs1.xlarge",
      "Endpoint": {
         "Port": 5439,
         "Address": "mycluster.coqoarplqhsn.us-east-1.redshift.amazonaws.com"
      },
      "ClusterVersion": "1.0",
      "PubliclyAccessible": "true",
      "MasterUsername": "adminuser",
      "ClusterParameterGroups": [
         {
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "default.redshift-1.0"
         } ],
      "ClusterSecurityGroups": [
         {
            "Status": "active",
            "ClusterSecurityGroupName": "default"
         } ],
      "AllowVersionUpgrade": true,
      "VpcSecurityGroups": \[],
      "AvailabilityZone": "us-east-1a",
      "ClusterCreateTime": "2013-01-22T21:59:29.559Z",
      "PreferredMaintenanceWindow": "sat:03:30-sat:04:00",
      "AutomatedSnapshotRetentionPeriod": 1,
      "ClusterStatus": "available",
      "ClusterIdentifier": "mycluster",
      "DBName": "dev",
      "NumberOfNodes": 2,
      "PendingModifiedValues": {}
```

```
   } ],
   "ResponseMetadata": {
      "RequestId": "65b71cac-64df-11e2-8f5b-e90bd6c77476"
   }
}
```

Vous pouvez également obtenir les mêmes informations au format texte à l'aide de l'option `--output text`. Commande :

option `--output text`. Commande :

option. Commande :

```
aws redshift describe-clusters --output text
```

Résultat :

```
dw.hs1.xlarge       1.0     true    adminuser       True    us-east-1a
 2013-01-22T21:59:29.559Z        sat:03:30-sat:04:00     1       available
 mycluster       dev     2
ENDPOINT    5439    mycluster.coqoarplqhsn.us-east-1.redshift.amazonaws.com
in-sync     default.redshift-1.0
active      default
PENDINGMODIFIEDVALUES
RESPONSEMETADATA    934281a8-64df-11e2-b07c-f7fbdd006c67
```

- Pour plus de détails sur l'API, voir DescribeClustersla section Référence des AWS CLI commandes.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import (
 "context"
 "errors"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/redshift"
 "github.com/aws/aws-sdk-go-v2/service/redshift/types"
)



// RedshiftActions wraps Redshift service actions.
type RedshiftActions struct {
 RedshiftClient *redshift.Client
}



// DescribeClusters returns information about the given cluster.
func (actor RedshiftActions) DescribeClusters(ctx context.Context, clusterId
 string) (*redshift.DescribeClustersOutput, error) {
 input, err := actor.RedshiftClient.DescribeClusters(ctx,
 &redshift.DescribeClustersInput{
  ClusterIdentifier: aws.String(clusterId),
 })
 var opErr *types.AccessToClusterDeniedFault
 if errors.As(err, &opErr) {
  println("Access to cluster denied.")
  panic(err)
 } else if err != nil {
  println("Failed to describe Redshift clusters.")
  return nil, err
 }
 return input, nil
}
```

- Pour plus de détails sur l'API, voir DescribeClustersla section Référence des AWS SDK pour Go API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Décrivez le cluster.

```
   /**
    * Waits asynchronously for the specified cluster to become available.
    * @param clusterId the identifier of the cluster to wait for
    * @return a {@link CompletableFuture} that completes when the cluster is
ready
    */
   public CompletableFuture<Void> waitForClusterReadyAsync(String clusterId) {
       DescribeClustersRequest clustersRequest =
DescribeClustersRequest.builder()
           .clusterIdentifier(clusterId)
           .build();

       logger.info("Waiting for cluster to become available. This may take a few
minutes.");
       long startTime = System.currentTimeMillis();

       // Recursive method to poll the cluster status.
       return checkClusterStatusAsync(clustersRequest, startTime);
   }

   private CompletableFuture<Void>
checkClusterStatusAsync(DescribeClustersRequest clustersRequest, long startTime)
{
       return getAsyncClient().describeClusters(clustersRequest)
           .thenCompose(clusterResponse -> {
               List<Cluster> clusterList = clusterResponse.clusters();
               boolean clusterReady = false;
               for (Cluster cluster : clusterList) {
                   if ("available".equals(cluster.clusterStatus())) {
                       clusterReady = true;
                       break;
```

```
                    }
                }

                if (clusterReady) {
                    logger.info(String.format("Cluster is available!"));
                    return CompletableFuture.completedFuture(null);
                } else {
                    long elapsedTimeMillis = System.currentTimeMillis() -
startTime;
                    long elapsedSeconds = elapsedTimeMillis / 1000;
                    long minutes = elapsedSeconds / 60;
                    long seconds = elapsedSeconds % 60;
                    System.out.printf("\rElapsed Time: %02d:%02d - Waiting for
cluster...", minutes, seconds);
                    System.out.flush();

                    // Wait 1 second before the next status check
                    return CompletableFuture.runAsync(() -> {
                        try {
                            TimeUnit.SECONDS.sleep(1);
                        } catch (InterruptedException e) {
                            throw new RuntimeException("Error during sleep: " +
e.getMessage(), e);
                        }
                    }).thenCompose(ignored ->
checkClusterStatusAsync(clustersRequest, startTime));
                }
            }).exceptionally(exception -> {
                throw new RuntimeException("Failed to get cluster status: " +
exception.getMessage(), exception);
            });
    }
```

- Pour plus de détails sur l'API, voir DescribeClustersla section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez le client.

```
import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Décrivez vos clusters.

```
// Import required AWS SDK clients and commands for Node.js
import { DescribeClustersCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "./libs/redshiftClient.js";

const params = {
  ClusterIdentifier: "CLUSTER_NAME",
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new DescribeClustersCommand(params));
    console.log("Success", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- Pour plus de détails sur l'API, voir DescribeClustersla section Référence des AWS SDK pour JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Décrivez le cluster.

```
suspend fun describeRedshiftClusters() {
    RedshiftClient.fromEnvironment { region = "us-west-2" }.use { redshiftClient
 ->
        val clusterResponse =
 redshiftClient.describeClusters(DescribeClustersRequest {})
        val clusterList = clusterResponse.clusters

        if (clusterList != null) {
            for (cluster in clusterList) {
                println("Cluster database name is ${cluster.dbName}")
                println("Cluster status is ${cluster.clusterStatus}")
            }
        }
    }
}
```

- Pour plus de détails sur l'API, consultez DescribeClustersla section AWS SDK pour la référence de l'API Kotlin.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
        self.client = redshift_client


    def describe_clusters(self, cluster_identifier):
        """
        Describes a cluster.

        :param cluster_identifier: The cluster identifier.
        :return: A list of clusters.
        """
        try:
            kwargs = {}
            if cluster_identifier:
                kwargs["ClusterIdentifier"] = cluster_identifier

            paginator = self.client.get_paginator("describe_clusters")
            clusters = []
            for page in paginator.paginate(**kwargs):
                clusters.extend(page["Clusters"])

            return clusters

        except ClientError as err:
```

```
            logging.error(
                "Couldn't describe a cluster. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

Le code suivant instancie l' RedshiftWrapper objet.

```
    client = boto3.client("redshift")
    redhift_wrapper = RedshiftWrapper(client)
```

- Pour plus de détails sur l'API, consultez DescribeClustersle AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Décrivez le cluster.

```
    TRY.
        " Example values: iv_cluster_identifier = 'my-redshift-
cluster' (optional)
        oo_result = lo_rsh->describeclusters(
          iv_clusteridentifier = iv_cluster_identifier
        ).
        lt_clusters = oo_result->get_clusters( ).
        lv_cluster_count = lines( lt_clusters ).
        MESSAGE |Retrieved { lv_cluster_count } cluster(s).| TYPE 'I'.
      CATCH /aws1/cx_rshclustnotfoundfault.
        MESSAGE 'Cluster not found.' TYPE 'I'.
```

```
    ENDTRY.
```

- Pour plus de détails sur l'API, consultez DescribeClustersla section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezL'utilisation de ce service avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **`DescribeStatement`**avec un AWS Kit SDK

Les exemples de code suivants illustrent comment utiliser `DescribeStatement`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET (v4)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Describe a statement execution.
    /// </summary>
    /// <param name="statementId">The statement ID.</param>
    /// <returns>The statement description.</returns>
    public async Task<DescribeStatementResponse> DescribeStatementAsync(string
statementId)
    {
        try
        {
```

```
            var request = new DescribeStatementRequest
            {
                Id = statementId
            };

            var response = await
_redshiftDataClient.DescribeStatementAsync(request);
            return response;
        }
        catch (Amazon.RedshiftDataAPIService.Model.ResourceNotFoundException ex)
        {
            Console.WriteLine($"Statement not found: {ex.Message}");
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't describe statement. Here's why:
{ex.Message}");
            throw;
        }
    }
```

- Pour plus de détails sur l'API, voir DescribeStatementla section Référence des AWS SDK pour .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /**
     * Checks the status of an SQL statement asynchronously and handles the
completion of the statement.
     *
     * @param sqlId the ID of the SQL statement to check
```

```
    * @return a {@link CompletableFuture} that completes when the SQL
statement's status is either "FINISHED" or "FAILED"
    */
   public CompletableFuture<Void> checkStatementAsync(String sqlId) {
       DescribeStatementRequest statementRequest =
DescribeStatementRequest.builder()
           .id(sqlId)
           .build();

       return getAsyncDataClient().describeStatement(statementRequest)
           .thenCompose(response -> {
               String status = response.statusAsString();
               logger.info("... Status: {} ", status);

               if ("FAILED".equals(status)) {
                   throw new RuntimeException("The Query Failed. Ending
program");
               } else if ("FINISHED".equals(status)) {
                   return CompletableFuture.completedFuture(null);
               } else {
                   // Sleep for 1 second and recheck status
                   return CompletableFuture.runAsync(() -> {
                       try {
                           TimeUnit.SECONDS.sleep(1);
                       } catch (InterruptedException e) {
                           throw new RuntimeException("Error during sleep: " +
e.getMessage(), e);
                       }
                   }).thenCompose(ignore -> checkStatementAsync(sqlId)); //
Recursively call until status is FINISHED or FAILED
               }
           }).whenComplete((result, exception) -> {
               if (exception != null) {
                   // Handle exceptions
                   logger.info("Error: {} ", exception.getMessage());
               } else {
                   logger.info("The statement is finished!");
               }
           });
   }
```

- Pour plus de détails sur l'API, voir DescribeStatementla section Référence des AWS SDK for Java 2.x API.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class RedshiftDataWrapper:
    """Encapsulates Amazon Redshift data."""

    def __init__(self, client):
        """
        :param client: A Boto3 RedshiftDataWrapper client.
        """
        self.client = client


    def describe_statement(self, statement_id):
        """
        Describes a SQL statement.

        :param statement_id: The SQL statement identifier.
        :return: The SQL statement result.
        """
        try:
            response = self.client.describe_statement(Id=statement_id)
            return response
        except ClientError as err:
            logging.error(
                "Couldn't describe statement. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

Le code suivant instancie l' RedshiftDataWrapper objet.

```
    client = boto3.client("redshift-data")
    redshift_data_wrapper = RedshiftDataWrapper(client)
```

- Pour plus de détails sur l'API, consultez DescribeStatementle AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        " Example values: iv_statement_id = 'xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx'
        oo_result = lo_rsd->describestatement(
          iv_id = iv_statement_id
        ).
        lv_status = oo_result->get_status( ).
        MESSAGE |Statement status: { lv_status }| TYPE 'I'.
      CATCH /aws1/cx_rsdresourcenotfoundex.
        MESSAGE 'Statement not found.' TYPE 'I'.
      CATCH /aws1/cx_rsdinternalserverex.
        MESSAGE 'Internal server error.' TYPE 'I'.
    ENDTRY.
```

- Pour plus de détails sur l'API, consultez DescribeStatementla section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezL'utilisation de ce service avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **`ExecuteStatement`**avec un AWS Kit SDK

Les exemples de code suivants illustrent comment utiliser `ExecuteStatement`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Exécute une instruction SQL pour créer une table de base de données.

```
   /**
    * Creates an asynchronous task to execute a SQL statement for creating a new
table.
    *
    * @param clusterId    the identifier of the Amazon Redshift cluster
    * @param databaseName the name of the database to create the table in
    * @param userName     the username to use for the database connection
    * @return a {@link CompletableFuture} that completes with the result of the
SQL statement execution
    * @throws RuntimeException if there is an error creating the table
    */
   public CompletableFuture<ExecuteStatementResponse> createTableAsync(String
clusterId, String databaseName, String userName) {
       ExecuteStatementRequest createTableRequest =
ExecuteStatementRequest.builder()
```

```
            .clusterIdentifier(clusterId)
            .dbUser(userName)
            .database(databaseName)
            .sql("CREATE TABLE Movies (" +
                "id INT PRIMARY KEY, " +
                "title VARCHAR(100), " +
                "year INT)")
            .build();

        return getAsyncDataClient().executeStatement(createTableRequest)
            .whenComplete((response, exception) -> {
                if (exception != null) {
                    throw new RuntimeException("Error creating table: " +
exception.getMessage(), exception);
                } else {
                    logger.info("Table created: Movies");
                }
            });
    }
```

Exécute une instruction SQL pour insérer des données dans une table de base de données.

```
    /**
     * Asynchronously pops a table from a JSON file.
     *
     * @param clusterId   the ID of the cluster
     * @param databaseName the name of the database
     * @param userName    the username
     * @param fileName    the name of the JSON file
     * @param number      the number of records to process
     * @return a CompletableFuture that completes with the number of records
added to the Movies table
     */
    public CompletableFuture<Integer> popTableAsync(String clusterId, String
databaseName, String userName, String fileName, int number) {
        return CompletableFuture.supplyAsync(() -> {
                try {
                    JsonParser parser = new JsonFactory().createParser(new
File(fileName));
                    JsonNode rootNode = new ObjectMapper().readTree(parser);
                    Iterator<JsonNode> iter = rootNode.iterator();
                    return iter;
```

```
                } catch (IOException e) {
                    throw new RuntimeException("Failed to read or parse JSON
file: " + e.getMessage(), e);
                }
            }).thenCompose(iter -> processNodesAsync(clusterId, databaseName,
userName, iter, number))
            .whenComplete((result, exception) -> {
                if (exception != null) {
                    logger.info("Error {} ", exception.getMessage());
                } else {
                    logger.info("{} records were added to the Movies table." ,
result);
                }
            });
    }

    private CompletableFuture<Integer> processNodesAsync(String clusterId, String
databaseName, String userName, Iterator<JsonNode> iter, int number) {
        return CompletableFuture.supplyAsync(() -> {
            int t = 0;
            try {
                while (iter.hasNext()) {
                    if (t == number)
                        break;
                    JsonNode currentNode = iter.next();
                    int year = currentNode.get("year").asInt();
                    String title = currentNode.get("title").asText();

                    // Use SqlParameter to avoid SQL injection.
                    List<SqlParameter> parameterList = new ArrayList<>();
                    String sqlStatement = "INSERT INTO Movies
VALUES( :id , :title, :year);";
                    SqlParameter idParam = SqlParameter.builder()
                        .name("id")
                        .value(String.valueOf(t))
                        .build();

                    SqlParameter titleParam = SqlParameter.builder()
                        .name("title")
                        .value(title)
                        .build();

                    SqlParameter yearParam = SqlParameter.builder()
                        .name("year")
```

```
                        .value(String.valueOf(year))
                        .build();
                    parameterList.add(idParam);
                    parameterList.add(titleParam);
                    parameterList.add(yearParam);

                    ExecuteStatementRequest insertStatementRequest =
ExecuteStatementRequest.builder()
                        .clusterIdentifier(clusterId)
                        .sql(sqlStatement)
                        .database(databaseName)
                        .dbUser(userName)
                        .parameters(parameterList)
                        .build();


getAsyncDataClient().executeStatement(insertStatementRequest);
                    logger.info("Inserted: " + title + " (" + year + ")");
                    t++;
                }
            } catch (RedshiftDataException e) {
                throw new RuntimeException("Error inserting data: " +
e.getMessage(), e);
            }
            return t;
        });
    }
```

Exécute une instruction SQL pour interroger une table de base de données.

```
    /**
     * Asynchronously queries movies by a given year from a Redshift database.
     *
     * @param database    the name of the database to query
     * @param dbUser      the user to connect to the database with
     * @param year        the year to filter the movies by
     * @param clusterId   the identifier of the Redshift cluster to connect to
     * @return a {@link CompletableFuture} containing the response ID of the
executed SQL statement
     */
    public CompletableFuture<String> queryMoviesByYearAsync(String database,
                                                            String dbUser,
```

```
                                                                    int year,
                                                                    String
clusterId) {

        String sqlStatement = "SELECT * FROM Movies WHERE year = :year";
        SqlParameter yearParam = SqlParameter.builder()
            .name("year")
            .value(String.valueOf(year))
            .build();

        ExecuteStatementRequest statementRequest =
ExecuteStatementRequest.builder()
            .clusterIdentifier(clusterId)
            .database(database)
            .dbUser(dbUser)
            .parameters(yearParam)
            .sql(sqlStatement)
            .build();

        return CompletableFuture.supplyAsync(() -> {
            try {
                ExecuteStatementResponse response =
getAsyncDataClient().executeStatement(statementRequest).join(); // Use join() to
wait for the result
                return response.id();
            } catch (RedshiftDataException e) {
                throw new RuntimeException("Error executing statement: " +
e.getMessage(), e);
            }
        }).exceptionally(exception -> {
            logger.info("Error: {}", exception.getMessage());
            return "";
        });
    }
```

- Pour plus de détails sur l'API, voir ExecuteStatementla section Référence des AWS SDK for Java 2.x API.

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        " Example values: iv_cluster_identifier = 'redshift-cluster-movies'
        " Example values: iv_database_name = 'dev'
        " Example values: iv_user_name = 'awsuser'
        " Example values: iv_sql = 'SELECT * FROM movies WHERE year = :year'
        " Example values: it_parameter_list - SQL parameters for parameterized
queries

        " Only pass parameters if the list is not empty
        IF it_parameter_list IS NOT INITIAL.
          oo_result = lo_rsd->executestatement(
            iv_clusteridentifier = iv_cluster_identifier
            iv_database = iv_database_name
            iv_dbuser = iv_user_name
            iv_sql = iv_sql
            it_parameters = it_parameter_list
          ).
        ELSE.
          oo_result = lo_rsd->executestatement(
            iv_clusteridentifier = iv_cluster_identifier
            iv_database = iv_database_name
            iv_dbuser = iv_user_name
            iv_sql = iv_sql
          ).
        ENDIF.

        lv_statement_id = oo_result->get_id( ).
        MESSAGE |Statement executed. ID: { lv_statement_id }| TYPE 'I'.
      CATCH /aws1/cx_rsdexecutestatementex.
        MESSAGE 'Statement execution error.' TYPE 'I'.
      CATCH /aws1/cx_rsdresourcenotfoundex.
        MESSAGE 'Resource not found.' TYPE 'I'.
```

```
    ENDTRY.
```

- Pour plus de détails sur l'API, consultez ExecuteStatementla section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezL'utilisation de ce service avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **`GetStatementResult`**avec un AWS Kit SDK

Les exemples de code suivants illustrent comment utiliser `GetStatementResult`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET (v4)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Get the results of a statement execution.
    /// </summary>
    /// <param name="statementId">The statement ID.</param>
    /// <returns>A list of result rows.</returns>
    public async Task<List<List<Field>>> GetStatementResultAsync(string
statementId)
    {
        try
```

```
        {
            var request = new GetStatementResultRequest
            {
                Id = statementId
            };

            var response = await
_redshiftDataClient.GetStatementResultAsync(request);
            return response.Records;
        }
        catch (Amazon.RedshiftDataAPIService.Model.ResourceNotFoundException ex)
        {
            Console.WriteLine($"Statement not found: {ex.Message}");
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't get statement result. Here's why:
{ex.Message}");
            throw;
        }
    }
```

- Pour plus de détails sur l'API, voir GetStatementResultla section Référence des AWS SDK pour .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Vérifiez le résultat de l'instruction.

```
    /**
     * Asynchronously retrieves the results of a statement execution.
```

```
    *
    * @param statementId the ID of the statement for which to retrieve the
results
    * @return a {@link CompletableFuture} that completes when the statement
result has been processed
    */
   public CompletableFuture<Void> getResultsAsync(String statementId) {
       GetStatementResultRequest resultRequest =
GetStatementResultRequest.builder()
           .id(statementId)
           .build();

       return getAsyncDataClient().getStatementResult(resultRequest)
           .handle((response, exception) -> {
               if (exception != null) {
                   logger.info("Error getting statement result {} ",
exception.getMessage());
                   throw new RuntimeException("Error getting statement result: "
+ exception.getMessage(), exception);
               }

               // Extract and print the field values using streams if the
response is valid.
               response.records().stream()
                   .flatMap(List::stream)
                   .map(Field::stringValue)
                   .filter(value -> value != null)
                   .forEach(value -> System.out.println("The Movie title field
is " + value));

               return response;
           }).thenAccept(response -> {
               // Optionally add more logic here if needed after handling the
response
           });
   }
```

- Pour plus de détails sur l'API, voir GetStatementResultla section Référence des AWS SDK for Java 2.x API.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class RedshiftDataWrapper:
    """Encapsulates Amazon Redshift data."""

    def __init__(self, client):
        """
        :param client: A Boto3 RedshiftDataWrapper client.
        """
        self.client = client


    def get_statement_result(self, statement_id):
        """
        Gets the result of a SQL statement.

        :param statement_id: The SQL statement identifier.
        :return: The SQL statement result.
        """
        try:
            result = {
                "Records": [],
            }
            paginator = self.client.get_paginator("get_statement_result")
            for page in paginator.paginate(Id=statement_id):
                if "ColumnMetadata" not in result:
                    result["ColumnMetadata"] = page["ColumnMetadata"]
                result["Records"].extend(page["Records"])
            return result
        except ClientError as err:
            logging.error(
                "Couldn't get statement result. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
```

```
            )
            raise
```

Le code suivant instancie l' RedshiftDataWrapper objet.

```
    client = boto3.client("redshift-data")
    redshift_data_wrapper = RedshiftDataWrapper(client)
```

- Pour plus de détails sur l'API, consultez GetStatementResultle AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Vérifiez le résultat de l'instruction.

```
    TRY.
        " Example values: iv_statement_id = 'xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx'
        " Handle pagination for large result sets

        DO.
          lo_result_page = lo_rsd->getstatementresult(
            iv_id = iv_statement_id
            iv_nexttoken = lv_next_token
          ).

          " Collect records from this page
          lt_page_records = lo_result_page->get_records( ).
          APPEND LINES OF lt_page_records TO lt_all_records.
```

```
        " Check if there are more pages
        lv_next_token = lo_result_page->get_nexttoken( ).
        IF lv_next_token IS INITIAL.
          EXIT. " No more pages
        ENDIF.
      ENDDO.

      " For the last call, set oo_result for return value
      oo_result = lo_result_page.
      lv_record_count = lines( lt_all_records ).
      MESSAGE |Retrieved { lv_record_count } record(s).| TYPE 'I'.
    CATCH /aws1/cx_rsdresourcenotfoundex.
      MESSAGE 'Statement not found or results not available.' TYPE 'I'.
    CATCH /aws1/cx_rsdinternalserverex.
      MESSAGE 'Internal server error.' TYPE 'I'.
  ENDTRY.
```

- Pour plus de détails sur l'API, consultez GetStatementResultla section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezL'utilisation de ce service avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **`ListDatabases`**avec un AWS Kit SDK

Les exemples de code suivants illustrent comment utiliser `ListDatabases`.

.NET

SDK pour .NET (v4)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// List databases in a Redshift cluster.
```

```
    /// </summary>
    /// <param name="clusterIdentifier">The cluster identifier.</param>
    /// <param name="dbUser">The database user.</param>
    /// <param name="dbUser">The database name for authentication.</param>
    /// <returns>A list of database names.</returns>
    public async Task<List<string>> ListDatabasesAsync(string clusterIdentifier,
string dbUser, string databaseName)
    {
        try
        {
            var request = new ListDatabasesRequest
            {
                ClusterIdentifier = clusterIdentifier,
                DbUser = dbUser,
                Database = databaseName
            };

            var response = await _redshiftDataClient.ListDatabasesAsync(request);
            var databases = new List<string>();

            foreach (var database in response.Databases)
            {
                Console.WriteLine($"The database name is : {database}");
                databases.Add(database);
            }

            return databases;
        }
        catch (Amazon.RedshiftDataAPIService.Model.ValidationException ex)
        {
            Console.WriteLine($"Validation error: {ex.Message}");
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't list databases. Here's why:
{ex.Message}");
            throw;
        }
    }
```

- Pour plus de détails sur l'API, voir ListDatabasesla section Référence des AWS SDK pour .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /**
    * Lists all databases asynchronously for the specified cluster, database
user, and database.
    * @param clusterId the identifier of the cluster to list databases for
    * @param dbUser the database user to use for the list databases request
    * @param database the database to list databases for
    * @return a {@link CompletableFuture} that completes when the database
listing is complete, or throws a {@link RuntimeException} if there was an error
    */
   public CompletableFuture<Void> listAllDatabasesAsync(String clusterId, String
dbUser, String database) {
       ListDatabasesRequest databasesRequest = ListDatabasesRequest.builder()
           .clusterIdentifier(clusterId)
           .dbUser(dbUser)
           .database(database)
           .build();

       // Asynchronous paginator for listing databases.
       ListDatabasesPublisher databasesPaginator =
getAsyncDataClient().listDatabasesPaginator(databasesRequest);
       CompletableFuture<Void> future = databasesPaginator.subscribe(response ->
{
           response.databases().forEach(db -> {
               logger.info("The database name is {} ", db);
           });
       });

       // Return the future for asynchronous handling.
```

```
        return future.exceptionally(exception -> {
            throw new RuntimeException("Failed to list databases: " +
exception.getMessage(), exception);
        });
    }
```

- Pour plus de détails sur l'API, voir ListDatabasesla section Référence des AWS SDK for Java 2.x API.

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        " Example values: iv_cluster_identifier = 'redshift-cluster-movies'
        " Example values: iv_database_name = 'dev'
        " Example values: iv_database_user = 'awsuser'
        oo_result = lo_rsd->listdatabases(
          iv_clusteridentifier = iv_cluster_identifier
          iv_database = iv_database_name
          iv_dbuser = iv_database_user
        ).
        lt_databases = oo_result->get_databases( ).
        lv_db_count = lines( lt_databases ).
        MESSAGE |Retrieved { lv_db_count } database(s).| TYPE 'I'.
      CATCH /aws1/cx_rsddatabaseconnex.
        MESSAGE 'Database connection error.' TYPE 'I'.
      CATCH /aws1/cx_rsdresourcenotfoundex.
        MESSAGE 'Cluster not found.' TYPE 'I'.
    ENDTRY.
```

- Pour plus de détails sur l'API, consultez ListDatabasesla section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezL'utilisation de ce service avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **`ModifyCluster`**avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `ModifyCluster`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET (v4)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /// <summary>
   /// Modify an Amazon Redshift cluster.
   /// </summary>
   /// <param name="clusterIdentifier">The identifier for the cluster.</param>
   /// <param name="preferredMaintenanceWindow">The preferred maintenance
window.</param>
   /// <returns>True if successful.</returns>
   public async Task<bool> ModifyClusterAsync(string clusterIdentifier, string
preferredMaintenanceWindow)
   {
       try
       {
           var request = new ModifyClusterRequest
           {
               ClusterIdentifier = clusterIdentifier,
               PreferredMaintenanceWindow = preferredMaintenanceWindow
```

```
            };

            var response = await _redshiftClient.ModifyClusterAsync(request);
            Console.WriteLine($"The modified cluster was successfully modified
and has {response.Cluster.PreferredMaintenanceWindow} as the maintenance
window");
            return true;
        }
        catch (ClusterNotFoundException ex)
        {
            Console.WriteLine($"Cluster {clusterIdentifier} not found:
{ex.Message}");
            return false;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Couldn't modify cluster. Here's why:
{ex.Message}");
            return false;
        }
    }
```

- Pour plus de détails sur l'API, voir ModifyClusterla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Associer un groupe de sécurité à l'aide d'un ClusterThis exemple montre comment associer un groupe de sécurité de cluster au cluster spécifié.Commande :

```
aws redshift modify-cluster --cluster-identifier mycluster --cluster-security-
groups mysecuritygroup
```

Modifier la fenêtre de maintenance pour ClusterThis montrer comment modifier la fenêtre de maintenance hebdomadaire préférée pour un cluster afin qu'elle soit la fenêtre minimale de quatre heures commençant le dimanche à 23 h 15 et se terminant le lundi à 15 h 15 : AM.Command

```
aws redshift modify-cluster --cluster-identifier mycluster --preferred-
maintenance-window Sun:23:15-Mon:03:15
```

Modifiez le mot de passe principal. L' ClusterThis exemple montre comment modifier le mot de passe principal d'un cluster.Commande :

```
aws redshift modify-cluster --cluster-identifier mycluster --master-user-password
 A1b2c3d4
```

- Pour plus de détails sur l'API, voir ModifyClusterla section Référence des AWS CLI commandes.

Go

Kit SDK pour Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import (
 "context"
 "errors"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/redshift"
 "github.com/aws/aws-sdk-go-v2/service/redshift/types"
)



// RedshiftActions wraps Redshift service actions.
type RedshiftActions struct {
 RedshiftClient *redshift.Client
}
```

```
// ModifyCluster sets the preferred maintenance window for the given cluster.
func (actor RedshiftActions) ModifyCluster(ctx context.Context, clusterId string,
 maintenanceWindow string) *redshift.ModifyClusterOutput {
 // Modify the cluster's maintenance window
 input := &redshift.ModifyClusterInput{
  ClusterIdentifier:          aws.String(clusterId),
  PreferredMaintenanceWindow: aws.String(maintenanceWindow),
 }

 var opErr *types.InvalidClusterStateFault
 output, err := actor.RedshiftClient.ModifyCluster(ctx, input)
 if err != nil && errors.As(err, &opErr) {
  log.Println("Cluster is in an invalid state.")
  panic(err)
 } else if err != nil {
  log.Printf("Failed to modify Redshift cluster: %v\n", err)
  panic(err)
 }

 log.Printf("The cluster was successfully modified and now has %s as the
 maintenance window\n", *output.Cluster.PreferredMaintenanceWindow)
 return output
}
```

- Pour plus de détails sur l'API, voir ModifyClusterla section Référence des AWS SDK pour Go API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Modifiez un cluster.

```
   /**
    * Modifies an Amazon Redshift cluster asynchronously.
    *
    * @param clusterId the identifier of the cluster to be modified
    * @return a {@link CompletableFuture} that completes when the cluster
modification is complete
    */
   public CompletableFuture<ModifyClusterResponse> modifyClusterAsync(String
clusterId) {
       ModifyClusterRequest modifyClusterRequest =
ModifyClusterRequest.builder()
           .clusterIdentifier(clusterId)
           .preferredMaintenanceWindow("wed:07:30-wed:08:00")
           .build();

       return getAsyncClient().modifyCluster(modifyClusterRequest)
           .whenComplete((clusterResponse, exception) -> {
               if (exception != null) {
                   if (exception.getCause() instanceof RedshiftException) {
                       logger.info("Error: {} ", exception.getMessage());
                   } else {
                       logger.info("Unexpected error: {} ",
exception.getMessage());
                   }
               } else {
                   logger.info("The modified cluster was successfully modified
and has "
                       + clusterResponse.cluster().preferredMaintenanceWindow()
+ " as the maintenance window");
               }
           });
   }
```

- Pour plus de détails sur l'API, voir ModifyClusterla section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez le client.

```
import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Modifiez un cluster.

```
// Import required AWS SDK clients and commands for Node.js
import { ModifyClusterCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "./libs/redshiftClient.js";

// Set the parameters
const params = {
  ClusterIdentifier: "CLUSTER_NAME",
  MasterUserPassword: "NEW_MASTER_USER_PASSWORD",
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new ModifyClusterCommand(params));
    console.log("Success was modified.", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- Pour plus de détails sur l'API, voir ModifyClusterla section Référence des AWS SDK pour JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Modifiez un cluster.

```
suspend fun modifyCluster(clusterId: String?) {
    val modifyClusterRequest =
        ModifyClusterRequest {
            clusterIdentifier = clusterId
            preferredMaintenanceWindow = "wed:07:30-wed:08:00"
        }

    RedshiftClient { region = "us-west-2" }.use { redshiftClient ->
        val clusterResponse = redshiftClient.modifyCluster(modifyClusterRequest)
        println(
            "The modified cluster was successfully modified and has
 ${clusterResponse.cluster?.preferredMaintenanceWindow} as the maintenance
 window",
        )
    }
}
```

- Pour plus de détails sur l'API, consultez ModifyClusterla section AWS SDK pour la référence de l'API Kotlin.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
        self.client = redshift_client


    def modify_cluster(self, cluster_identifier, preferred_maintenance_window):
        """
        Modifies a cluster.

        :param cluster_identifier: The cluster identifier.
        :param preferred_maintenance_window: The preferred maintenance window.
        """
        try:
            self.client.modify_cluster(
                ClusterIdentifier=cluster_identifier,
                PreferredMaintenanceWindow=preferred_maintenance_window,
            )
        except ClientError as err:
            logging.error(
                "Couldn't modify a cluster. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

Le code suivant instancie l' RedshiftWrapper objet.

```
    client = boto3.client("redshift")
    redhift_wrapper = RedshiftWrapper(client)
```

- Pour plus de détails sur l'API, consultez ModifyClusterle AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Modifiez un cluster.

```
    TRY.
        " Example values: iv_cluster_identifier = 'my-redshift-cluster'
        " Example values: iv_pref_maintenance_wn = 'wed:07:30-wed:08:00'
        lo_rsh->modifycluster(
          iv_clusteridentifier = iv_cluster_identifier
          iv_preferredmaintenancewin00 = iv_pref_maintenance_wn
        ).
        MESSAGE 'Redshift cluster modified successfully.' TYPE 'I'.
      CATCH /aws1/cx_rshclustnotfoundfault.
        MESSAGE 'Cluster not found.' TYPE 'I'.
      CATCH /aws1/cx_rshinvcluststatefault.
        MESSAGE 'Invalid cluster state for modification.' TYPE 'I'.
    ENDTRY.
```

- Pour plus de détails sur l'API, consultez ModifyClusterla section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezL'utilisation de ce service avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Scénarios d'utilisation d'Amazon Redshift AWS Kits SDK

Les exemples de code suivants vous montrent comment implémenter des scénarios courants dans Amazon Redshift avec des AWS SDK. Ces scénarios vous montrent comment accomplir des tâches spécifiques en appelant plusieurs fonctions dans Amazon Redshift ou en les combinant avec d'autres Services AWS. Chaque exemple inclut un lien vers le code source complet, où vous trouverez des instructions sur la configuration et l'exécution du code.

Les scénarios ciblent un niveau d'expérience intermédiaire pour vous aider à comprendre les actions de service dans leur contexte.

Exemples

- Créer un outil de suivi des éléments Amazon Redshift.
- Commencez avec les entrepôts de données sans serveur à l'aide de la CLI
- Commencer à utiliser des clusters d'entrepôts de données provisionnés

Créer un outil de suivi des éléments Amazon Redshift.

Les exemples de code suivants montrent comment créer une application web qui suit et crée des rapports sur les éléments de travail à l'aide d'une base de données Amazon Redshift.

Java

SDK pour Java 2.x

Montre comment créer une application web qui suit et génère des rapports sur les éléments de travail stockés dans une base de données Amazon Redshift.

Pour obtenir le code source complet et les instructions sur la façon de configurer une API Spring REST qui interroge les données Amazon Redshift et pour une utilisation par une application React, consultez l'exemple complet sur. GitHub

Les services utilisés dans cet exemple

- Amazon Redshift

- Amazon SES

Kotlin

SDK pour Kotlin

Montre comment créer une application web qui suit et génère des rapports sur les éléments de travail stockés dans une base de données Amazon Redshift.

Pour obtenir le code source complet et les instructions sur la façon de configurer une API Spring REST qui interroge les données Amazon Redshift et pour une utilisation par une application React, consultez l'exemple complet sur. GitHub

Les services utilisés dans cet exemple

- Amazon Redshift
- Amazon SES

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezL'utilisation de ce service avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Commencez avec les entrepôts de données sans serveur à l'aide de la CLI

L'exemple de code suivant illustre comment :

- Utiliser secrets-manager CreateSecret
- Utiliser secrets-manager DeleteSecret
- Utiliser secrets-manager GetSecretValue
- Utiliser redshift CreateNamespace
- Utiliser redshift CreateWorkgroup
- Utiliser redshift DeleteNamespace
- Utiliser iam CreateRole

Bash

AWS CLI avec le script Bash

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code.

```
#!/bin/bash

# Amazon Redshift Serverless Tutorial Script with Secrets Manager (No jq
 dependency)
# This script creates a Redshift Serverless environment, loads sample data, and
 runs queries
# Uses AWS Secrets Manager for secure password management without requiring jq

# Set up logging
LOG_FILE="redshift-serverless-tutorial-v4.log"
exec > >(tee -a "$LOG_FILE") 2>&1

echo "Starting Amazon Redshift Serverless tutorial script at $(date)"
echo "All commands and outputs will be logged to $LOG_FILE"

# Function to check for errors in command output
check_error() {
  local output=$1
  local cmd=$2

  if echo "$output" | grep -i "error\|exception\|fail" > /dev/null; then
    echo "ERROR: Command failed: $cmd"
    echo "Output: $output"
    cleanup_resources
    exit 1
  fi
}

# Function to generate a secure password that meets Redshift requirements
generate_secure_password() {
  # Redshift password requirements:
  # - 8-64 characters
```

```
  # - At least one uppercase letter
  # - At least one lowercase letter
  # - At least one decimal digit
  # - Can contain printable ASCII characters except /, ", ', \, @, space

  local password=""
  local valid=false
  local attempts=0
  local max_attempts=10

  while [[ "$valid" == false && $attempts -lt $max_attempts ]]; do
    # Generate base password with safe characters
    local base=$(openssl rand -base64 12 | tr -d '/+=' | head -c 12)

    # Ensure we have at least one of each required character type
    local upper=$(echo "ABCDEFGHIJKLMNOPQRSTUVWXYZ" | fold -w1 | shuf -n1)
    local lower=$(echo "abcdefghijklmnopqrstuvwxyz" | fold -w1 | shuf -n1)
    local digit=$(echo "0123456789" | fold -w1 | shuf -n1)
    local special=$(echo "!#$%&*()_+-=[]{}|;:,.<>?" | fold -w1 | shuf -n1)

    # Combine and shuffle
    password="${base}${upper}${lower}${digit}${special}"
    password=$(echo "$password" | fold -w1 | shuf | tr -d '\n')

    # Validate password meets requirements
    if [[ ${#password} -ge 8 && ${#password} -le 64 ]] && \
       [[ "$password" =~ [A-Z] ]] && \
       [[ "$password" =~ [a-z] ]] && \
       [[ "$password" =~ [0-9] ]] && \
       [[ ! "$password" =~ [/\"\'\\@[:space:]] ]]; then
      valid=true
    fi

    ((attempts++))
  done

  if [[ "$valid" == false ]]; then
    echo "ERROR: Failed to generate valid password after $max_attempts attempts"
    exit 1
  fi

  echo "$password"
}
```

```
# Function to create secret in AWS Secrets Manager
create_secret() {
  local secret_name=$1
  local username=$2
  local password=$3
  local description=$4

  echo "Creating secret in AWS Secrets Manager: $secret_name"

  # Create the secret using AWS CLI without jq
  local secret_output=$(aws secretsmanager create-secret \
    --name "$secret_name" \
    --description "$description" \
    --secret-string "{\"username\":\"$username\",\"password\":\"$password\"}" \
    --tags Key=project,Value=doc-smith Key=tutorial,Value=redshift-serverless
 2>&1)

  if echo "$secret_output" | grep -i "error\|exception\|fail" > /dev/null; then
    echo "ERROR: Failed to create secret: $secret_output"
    return 1
  fi

  echo "Secret created successfully: $secret_name"
  return 0
}

# Function to retrieve password from AWS Secrets Manager
get_password_from_secret() {
  local secret_name=$1

  # Get the secret value and extract password using sed/grep instead of jq
  local secret_value=$(aws secretsmanager get-secret-value \
    --secret-id "$secret_name" \
    --query 'SecretString' \
    --output text 2>/dev/null)

  if [[ $? -eq 0 ]]; then
    # Extract password from JSON using sed
    echo "$secret_value" | sed -n 's/.*"password":"\([^"]*\)".*/\1/p'
  else
    echo ""
  fi
}
```

```
# Function to wait for a resource to be available
wait_for_resource() {
  local resource_type=$1
  local resource_name=$2
  local max_attempts=$3
  local wait_seconds=$4
  local check_cmd=$5

  echo "Waiting for $resource_type $resource_name to be available..."

  for ((i=1; i<=$max_attempts; i++)); do
    local output=$($check_cmd 2>/dev/null)
    local status=$(echo "$output" | grep -o '"Status": "[^"]*' | cut -d'"' -f4 ||
 echo "")

    if [[ "$status" == "AVAILABLE" ]]; then
      echo "$resource_type $resource_name is now available"
      return 0
    fi

    echo "Attempt $i/$max_attempts: $resource_type $resource_name status:
 $status. Waiting $wait_seconds seconds..."
    sleep $wait_seconds
  done

  echo "ERROR: Timed out waiting for $resource_type $resource_name to be
 available"
  return 1
}

# Function to wait for a resource to be deleted
wait_for_resource_deletion() {
  local resource_type=$1
  local resource_name=$2
  local max_attempts=$3
  local wait_seconds=$4
  local check_cmd=$5

  echo "Waiting for $resource_type $resource_name to be deleted..."

  for ((i=1; i<=$max_attempts; i++)); do
    local output=$($check_cmd 2>&1)

    if echo "$output" | grep -i "not found\|does not exist" > /dev/null; then
```

```
      echo "$resource_type $resource_name has been deleted"
      return 0
    fi

    echo "Attempt $i/$max_attempts: $resource_type $resource_name is still being
 deleted. Waiting $wait_seconds seconds..."
    sleep $wait_seconds
  done

  echo "ERROR: Timed out waiting for $resource_type $resource_name to be deleted"
  return 1
}

# Function to clean up resources
cleanup_resources() {
  echo ""
  echo "========================================="
  echo "CLEANUP CONFIRMATION"
  echo "========================================="
  echo "The following resources were created:"
  echo "- Redshift Serverless Workgroup: $WORKGROUP_NAME"
  echo "- Redshift Serverless Namespace: $NAMESPACE_NAME"
  echo "- IAM Role: $ROLE_NAME"
  echo "- Secrets Manager Secret: $SECRET_NAME"
  echo ""
  echo "Do you want to clean up all created resources? (y/n): "
  read -r CLEANUP_CHOICE

  if [[ "${CLEANUP_CHOICE,,}" == "y" ]]; then
    echo "Cleaning up resources..."

    # Delete the workgroup
    echo "Deleting Redshift Serverless workgroup $WORKGROUP_NAME..."
    WORKGROUP_DELETE_OUTPUT=$(aws redshift-serverless delete-workgroup --
workgroup-name "$WORKGROUP_NAME" 2>&1)
    echo "$WORKGROUP_DELETE_OUTPUT"

    # Wait for workgroup to be deleted before deleting namespace
    wait_for_resource_deletion "workgroup" "$WORKGROUP_NAME" 20 30 "aws redshift-
serverless get-workgroup --workgroup-name $WORKGROUP_NAME"

    # Delete the namespace
    echo "Deleting Redshift Serverless namespace $NAMESPACE_NAME..."
```

```
    NAMESPACE_DELETE_OUTPUT=$(aws redshift-serverless delete-namespace --
namespace-name "$NAMESPACE_NAME" 2>&1)
    echo "$NAMESPACE_DELETE_OUTPUT"

    # Wait for namespace to be deleted
    wait_for_resource_deletion "namespace" "$NAMESPACE_NAME" 20 30 "aws redshift-
serverless get-namespace --namespace-name $NAMESPACE_NAME"

    # Delete the IAM role policy
    echo "Deleting IAM role policy..."
    POLICY_DELETE_OUTPUT=$(aws iam delete-role-policy --role-name "$ROLE_NAME" --
policy-name S3Access 2>&1)
    echo "$POLICY_DELETE_OUTPUT"

    # Delete the IAM role
    echo "Deleting IAM role $ROLE_NAME..."
    ROLE_DELETE_OUTPUT=$(aws iam delete-role --role-name "$ROLE_NAME" 2>&1)
    echo "$ROLE_DELETE_OUTPUT"

    # Delete the secret
    echo "Deleting Secrets Manager secret $SECRET_NAME..."
    SECRET_DELETE_OUTPUT=$(aws secretsmanager delete-secret --secret-id
 "$SECRET_NAME" --force-delete-without-recovery 2>&1)
    echo "$SECRET_DELETE_OUTPUT"

    echo "Cleanup completed."
  else
    echo "Cleanup skipped. Resources will remain in your AWS account."
  fi
}

# Check if required tools are available
if ! command -v openssl &> /dev/null; then
    echo "ERROR: openssl is required but not installed. Please install openssl to
 continue."
    exit 1
fi

# Generate unique names for resources
RANDOM_SUFFIX=$(cat /dev/urandom | tr -dc 'a-z0-9' | head -c 6)
NAMESPACE_NAME="rs-namespace-${RANDOM_SUFFIX}"
WORKGROUP_NAME="rs-workgroup-${RANDOM_SUFFIX}"
ROLE_NAME="RedshiftServerlessS3Role-${RANDOM_SUFFIX}"
SECRET_NAME="redshift-serverless-admin-${RANDOM_SUFFIX}"
```

```
DB_NAME="dev"
ADMIN_USERNAME="admin"

# Generate secure password
echo "Generating secure password..."
ADMIN_PASSWORD=$(generate_secure_password)

# Create secret in AWS Secrets Manager
create_secret "$SECRET_NAME" "$ADMIN_USERNAME" "$ADMIN_PASSWORD" "Admin
 credentials for Redshift Serverless namespace $NAMESPACE_NAME"
if [[ $? -ne 0 ]]; then
  echo "ERROR: Failed to create secret in AWS Secrets Manager"
  exit 1
fi

# Track created resources
CREATED_RESOURCES=()

echo "Using the following resource names:"
echo "- Namespace: $NAMESPACE_NAME"
echo "- Workgroup: $WORKGROUP_NAME"
echo "- IAM Role: $ROLE_NAME"
echo "- Secret: $SECRET_NAME"
echo "- Database: $DB_NAME"
echo "- Admin Username: $ADMIN_USERNAME"
echo "- Admin Password: [STORED IN SECRETS MANAGER]"

# Step 1: Create IAM role for S3 access
echo "Creating IAM role for Redshift Serverless S3 access..."

# Create trust policy document
cat > redshift-trust-policy.json << EOF
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift-serverless.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

```
EOF

# Create S3 access policy document
cat > redshift-s3-policy.json << EOF
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::redshift-downloads",
        "arn:aws:s3:::redshift-downloads/*"
      ]
    }
  ]
}
EOF

# Create IAM role
echo "Creating IAM role $ROLE_NAME..."
ROLE_OUTPUT=$(aws iam create-role --role-name "$ROLE_NAME" --assume-role-policy-
document file://redshift-trust-policy.json 2>&1)
echo "$ROLE_OUTPUT"
check_error "$ROLE_OUTPUT" "aws iam create-role"
aws iam tag-role --role-name "$ROLE_NAME" \
  --tags Key=project,Value=doc-smith Key=tutorial,Value=redshift-serverless
CREATED_RESOURCES+=("IAM Role: $ROLE_NAME")

# Attach S3 policy to the role
echo "Attaching S3 access policy to role $ROLE_NAME..."
POLICY_OUTPUT=$(aws iam put-role-policy --role-name "$ROLE_NAME" --policy-name
 S3Access --policy-document file://redshift-s3-policy.json 2>&1)
echo "$POLICY_OUTPUT"
check_error "$POLICY_OUTPUT" "aws iam put-role-policy"

# Get the role ARN
ROLE_ARN=$(aws iam get-role --role-name "$ROLE_NAME" --query 'Role.Arn' --output
 text)
echo "Role ARN: $ROLE_ARN"
```

```
# Step 2: Create a namespace
echo "Creating Redshift Serverless namespace $NAMESPACE_NAME..."
NAMESPACE_OUTPUT=$(aws redshift-serverless create-namespace \
  --namespace-name "$NAMESPACE_NAME" \
  --admin-username "$ADMIN_USERNAME" \
  --admin-user-password "$ADMIN_PASSWORD" \
  --db-name "$DB_NAME" \
  --tags Key=project,Value=doc-smith Key=tutorial,Value=redshift-serverless 2>&1)
echo "$NAMESPACE_OUTPUT"
check_error "$NAMESPACE_OUTPUT" "aws redshift-serverless create-namespace"
CREATED_RESOURCES+=("Redshift Serverless Namespace: $NAMESPACE_NAME")

# Wait for namespace to be available
wait_for_resource "namespace" "$NAMESPACE_NAME" 10 30 "aws redshift-serverless
 get-namespace --namespace-name $NAMESPACE_NAME"

# Associate IAM role with namespace
echo "Associating IAM role with namespace..."
UPDATE_NAMESPACE_OUTPUT=$(aws redshift-serverless update-namespace \
  --namespace-name "$NAMESPACE_NAME" \
  --iam-roles "$ROLE_ARN" 2>&1)
echo "$UPDATE_NAMESPACE_OUTPUT"
check_error "$UPDATE_NAMESPACE_OUTPUT" "aws redshift-serverless update-namespace"

# Step 3: Create a workgroup
echo "Creating Redshift Serverless workgroup $WORKGROUP_NAME..."
WORKGROUP_OUTPUT=$(aws redshift-serverless create-workgroup \
  --workgroup-name "$WORKGROUP_NAME" \
  --namespace-name "$NAMESPACE_NAME" \
  --base-capacity 8 \
  --tags Key=project,Value=doc-smith Key=tutorial,Value=redshift-serverless 2>&1)
echo "$WORKGROUP_OUTPUT"
check_error "$WORKGROUP_OUTPUT" "aws redshift-serverless create-workgroup"
CREATED_RESOURCES+=("Redshift Serverless Workgroup: $WORKGROUP_NAME")

# Wait for workgroup to be available
wait_for_resource "workgroup" "$WORKGROUP_NAME" 20 30 "aws redshift-serverless
 get-workgroup --workgroup-name $WORKGROUP_NAME"

# Get workgroup endpoint
WORKGROUP_ENDPOINT=$(aws redshift-serverless get-workgroup \
  --workgroup-name "$WORKGROUP_NAME" \
  --query 'workgroup.endpoint.address' \
  --output text)
```

```
echo "Workgroup endpoint: $WORKGROUP_ENDPOINT"

# Wait additional time for the endpoint to be fully operational
echo "Waiting for endpoint to be fully operational..."
sleep 60

# Step 4: Create tables for sample data
echo "Creating tables for sample data..."

# Create users table
echo "Creating users table..."
USERS_TABLE_OUTPUT=$(aws redshift-data execute-statement \
  --database "$DB_NAME" \
  --workgroup-name "$WORKGROUP_NAME" \
  --sql "CREATE TABLE users(
    userid INTEGER NOT NULL DISTKEY SORTKEY,
    username CHAR(8),
    firstname VARCHAR(30),
    lastname VARCHAR(30),
    city VARCHAR(30),
    state CHAR(2),
    email VARCHAR(100),
    phone CHAR(14),
    likesports BOOLEAN,
    liketheatre BOOLEAN,
    likeconcerts BOOLEAN,
    likejazz BOOLEAN,
    likeclassical BOOLEAN,
    likeopera BOOLEAN,
    likerock BOOLEAN,
    likevegas BOOLEAN,
    likebroadway BOOLEAN,
    likemusicals BOOLEAN
  );" 2>&1)
echo "$USERS_TABLE_OUTPUT"
check_error "$USERS_TABLE_OUTPUT" "aws redshift-data execute-statement (users
 table)"
USERS_QUERY_ID=$(echo "$USERS_TABLE_OUTPUT" | grep -o '"Id": "[^"]*' | cut -d'"'
 -f4)

# Wait for query to complete
echo "Waiting for users table creation to complete..."
sleep 5
```

```
# Create event table
echo "Creating event table..."
EVENT_TABLE_OUTPUT=$(aws redshift-data execute-statement \
  --database "$DB_NAME" \
  --workgroup-name "$WORKGROUP_NAME" \
  --sql "CREATE TABLE event(
    eventid INTEGER NOT NULL DISTKEY,
    venueid SMALLINT NOT NULL,
    catid SMALLINT NOT NULL,
    dateid SMALLINT NOT NULL SORTKEY,
    eventname VARCHAR(200),
    starttime TIMESTAMP
  );" 2>&1)
echo "$EVENT_TABLE_OUTPUT"
check_error "$EVENT_TABLE_OUTPUT" "aws redshift-data execute-statement (event
 table)"
EVENT_QUERY_ID=$(echo "$EVENT_TABLE_OUTPUT" | grep -o '"Id": "[^"]*' | cut -d'"'
 -f4)

# Wait for query to complete
echo "Waiting for event table creation to complete..."
sleep 5

# Create sales table
echo "Creating sales table..."
SALES_TABLE_OUTPUT=$(aws redshift-data execute-statement \
  --database "$DB_NAME" \
  --workgroup-name "$WORKGROUP_NAME" \
  --sql "CREATE TABLE sales(
    salesid INTEGER NOT NULL,
    listid INTEGER NOT NULL DISTKEY,
    sellerid INTEGER NOT NULL,
    buyerid INTEGER NOT NULL,
    eventid INTEGER NOT NULL,
    dateid SMALLINT NOT NULL SORTKEY,
    qtysold SMALLINT NOT NULL,
    pricepaid DECIMAL(8,2),
    commission DECIMAL(8,2),
    saletime TIMESTAMP
  );" 2>&1)
echo "$SALES_TABLE_OUTPUT"
check_error "$SALES_TABLE_OUTPUT" "aws redshift-data execute-statement (sales
 table)"
```

```
SALES_QUERY_ID=$(echo "$SALES_TABLE_OUTPUT" | grep -o '"Id": "[^"]*' | cut -d'"'
 -f4)

# Wait for tables to be created
echo "Waiting for tables to be created..."
sleep 10

# Step 5: Load sample data from Amazon S3
echo "Loading sample data from Amazon S3..."

# Load data into users table
echo "Loading data into users table..."
USERS_LOAD_OUTPUT=$(aws redshift-data execute-statement \
  --database "$DB_NAME" \
  --workgroup-name "$WORKGROUP_NAME" \
  --sql "COPY users
    FROM 's3://redshift-downloads/tickit/allusers_pipe.txt'
    DELIMITER '|'
    TIMEFORMAT 'YYYY-MM-DD HH:MI:SS'
    IGNOREHEADER 1
    IAM_ROLE '$ROLE_ARN';" 2>&1)
echo "$USERS_LOAD_OUTPUT"
check_error "$USERS_LOAD_OUTPUT" "aws redshift-data execute-statement (load
 users)"
USERS_LOAD_QUERY_ID=$(echo "$USERS_LOAD_OUTPUT" | grep -o '"Id": "[^"]*' | cut -
d'"' -f4)

# Wait for data loading to complete
echo "Waiting for users data loading to complete..."
sleep 10

# Load data into event table
echo "Loading data into event table..."
EVENT_LOAD_OUTPUT=$(aws redshift-data execute-statement \
  --database "$DB_NAME" \
  --workgroup-name "$WORKGROUP_NAME" \
  --sql "COPY event
    FROM 's3://redshift-downloads/tickit/allevents_pipe.txt'
    DELIMITER '|'
    TIMEFORMAT 'YYYY-MM-DD HH:MI:SS'
    IGNOREHEADER 1
    IAM_ROLE '$ROLE_ARN';" 2>&1)
echo "$EVENT_LOAD_OUTPUT"
```

```
check_error "$EVENT_LOAD_OUTPUT" "aws redshift-data execute-statement (load
 event)"
EVENT_LOAD_QUERY_ID=$(echo "$EVENT_LOAD_OUTPUT" | grep -o '"Id": "[^"]*' | cut -
d'"' -f4)

# Wait for data loading to complete
echo "Waiting for event data loading to complete..."
sleep 10

# Load data into sales table
echo "Loading data into sales table..."
SALES_LOAD_OUTPUT=$(aws redshift-data execute-statement \
  --database "$DB_NAME" \
  --workgroup-name "$WORKGROUP_NAME" \
  --sql "COPY sales
    FROM 's3://redshift-downloads/tickit/sales_tab.txt'
    DELIMITER '\t'
    TIMEFORMAT 'MM/DD/YYYY HH:MI:SS'
    IGNOREHEADER 1
    IAM_ROLE '$ROLE_ARN';" 2>&1)
echo "$SALES_LOAD_OUTPUT"
check_error "$SALES_LOAD_OUTPUT" "aws redshift-data execute-statement (load
 sales)"
SALES_LOAD_QUERY_ID=$(echo "$SALES_LOAD_OUTPUT" | grep -o '"Id": "[^"]*' | cut -
d'"' -f4)

# Wait for data loading to complete
echo "Waiting for sales data loading to complete..."
sleep 30

# Step 6: Run sample queries
echo "Running sample queries..."

# Query 1: Find top 10 buyers by quantity
echo "Running query: Find top 10 buyers by quantity..."
QUERY1_OUTPUT=$(aws redshift-data execute-statement \
  --database "$DB_NAME" \
  --workgroup-name "$WORKGROUP_NAME" \
  --sql "SELECT firstname, lastname, total_quantity
    FROM (SELECT buyerid, sum(qtysold) total_quantity
          FROM sales
          GROUP BY buyerid
          ORDER BY total_quantity desc limit 10) Q, users
    WHERE Q.buyerid = userid
```

```
    ORDER BY Q.total_quantity desc;" 2>&1)
echo "$QUERY1_OUTPUT"
check_error "$QUERY1_OUTPUT" "aws redshift-data execute-statement (query 1)"
QUERY1_ID=$(echo "$QUERY1_OUTPUT" | grep -o '"Id": "[^"]*' | cut -d'"' -f4)

# Wait for query to complete
echo "Waiting for query 1 to complete..."
sleep 10

# Get query 1 results
echo "Getting results for query 1..."
QUERY1_STATUS_OUTPUT=$(aws redshift-data describe-statement --id "$QUERY1_ID"
 2>&1)
echo "$QUERY1_STATUS_OUTPUT"
check_error "$QUERY1_STATUS_OUTPUT" "aws redshift-data describe-statement (query
 1)"

QUERY1_STATUS=$(echo "$QUERY1_STATUS_OUTPUT" | grep -o '"Status": "[^"]*' | cut -
d'"' -f4)
if [ "$QUERY1_STATUS" == "FINISHED" ]; then
  QUERY1_RESULTS=$(aws redshift-data get-statement-result --id "$QUERY1_ID" 2>&1)
  echo "Query 1 Results:"
  echo "$QUERY1_RESULTS"
else
  echo "Query 1 is not yet complete. Status: $QUERY1_STATUS"
  echo "Waiting additional time for query to complete..."
  sleep 20

  # Check again
  QUERY1_STATUS_OUTPUT=$(aws redshift-data describe-statement --id "$QUERY1_ID"
 2>&1)
  QUERY1_STATUS=$(echo "$QUERY1_STATUS_OUTPUT" | grep -o '"Status": "[^"]*' | cut
 -d'"' -f4)

  if [ "$QUERY1_STATUS" == "FINISHED" ]; then
    QUERY1_RESULTS=$(aws redshift-data get-statement-result --id "$QUERY1_ID"
 2>&1)
    echo "Query 1 Results:"
    echo "$QUERY1_RESULTS"
  else
    echo "Query 1 is still not complete. Status: $QUERY1_STATUS"
  fi
fi
```

```
# Query 2: Find events in the 99.9 percentile in terms of all time total sales
echo "Running query: Find events in the 99.9 percentile in terms of all time
 total sales..."
QUERY2_OUTPUT=$(aws redshift-data execute-statement \
  --database "$DB_NAME" \
  --workgroup-name "$WORKGROUP_NAME" \
  --sql "SELECT eventname, total_price
    FROM (SELECT eventid, total_price, ntile(1000) over(order by total_price
 desc) as percentile
          FROM (SELECT eventid, sum(pricepaid) total_price
                FROM sales
                GROUP BY eventid)) Q, event E
    WHERE Q.eventid = E.eventid
    AND percentile = 1
    ORDER BY total_price desc;" 2>&1)
echo "$QUERY2_OUTPUT"
check_error "$QUERY2_OUTPUT" "aws redshift-data execute-statement (query 2)"
QUERY2_ID=$(echo "$QUERY2_OUTPUT" | grep -o '"Id": "[^"]*' | cut -d'"' -f4)

# Wait for query to complete
echo "Waiting for query 2 to complete..."
sleep 10

# Get query 2 results
echo "Getting results for query 2..."
QUERY2_STATUS_OUTPUT=$(aws redshift-data describe-statement --id "$QUERY2_ID"
 2>&1)
echo "$QUERY2_STATUS_OUTPUT"
check_error "$QUERY2_STATUS_OUTPUT" "aws redshift-data describe-statement (query
 2)"

QUERY2_STATUS=$(echo "$QUERY2_STATUS_OUTPUT" | grep -o '"Status": "[^"]*' | cut -
d'"' -f4)
if [ "$QUERY2_STATUS" == "FINISHED" ]; then
  QUERY2_RESULTS=$(aws redshift-data get-statement-result --id "$QUERY2_ID" 2>&1)
  echo "Query 2 Results:"
  echo "$QUERY2_RESULTS"
else
  echo "Query 2 is not yet complete. Status: $QUERY2_STATUS"
  echo "Waiting additional time for query to complete..."
  sleep 20

  # Check again
```

```
  QUERY2_STATUS_OUTPUT=$(aws redshift-data describe-statement --id "$QUERY2_ID"
 2>&1)
  QUERY2_STATUS=$(echo "$QUERY2_STATUS_OUTPUT" | grep -o '"Status": "[^"]*' | cut
 -d'"' -f4)

  if [ "$QUERY2_STATUS" == "FINISHED" ]; then
    QUERY2_RESULTS=$(aws redshift-data get-statement-result --id "$QUERY2_ID"
 2>&1)
    echo "Query 2 Results:"
    echo "$QUERY2_RESULTS"
  else
    echo "Query 2 is still not complete. Status: $QUERY2_STATUS"
  fi
fi

# Summary
echo ""
echo "========================================="
echo "TUTORIAL SUMMARY"
echo "========================================="
echo "You have successfully:"
echo "1. Created a Redshift Serverless namespace and workgroup"
echo "2. Created an IAM role with S3 access permissions"
echo "3. Stored admin credentials securely in AWS Secrets Manager"
echo "4. Created tables for sample data"
echo "5. Loaded sample data from Amazon S3"
echo "6. Run sample queries on the data"
echo ""
echo "Redshift Serverless Resources:"
echo "- Namespace: $NAMESPACE_NAME"
echo "- Workgroup: $WORKGROUP_NAME"
echo "- Database: $DB_NAME"
echo "- Endpoint: $WORKGROUP_ENDPOINT"
echo "- Credentials Secret: $SECRET_NAME"
echo ""
echo "To connect to your Redshift Serverless database using SQL tools:"
echo "- Host: $WORKGROUP_ENDPOINT"
echo "- Database: $DB_NAME"
echo "- Username: $ADMIN_USERNAME"
echo "- Password: Retrieve from AWS Secrets Manager secret '$SECRET_NAME'"
echo ""
echo "To retrieve the password from Secrets Manager (without jq):"
echo "aws secretsmanager get-secret-value --secret-id $SECRET_NAME --query
 'SecretString' --output text | sed -n 's/.*\"password\":\"\([^\"]*\)\".*/\1/p'"
```

```
echo ""

# Clean up temporary files
rm -f redshift-trust-policy.json redshift-s3-policy.json

# Clean up resources
cleanup_resources

echo "Tutorial completed at $(date)"
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des commandes de l'AWS CLI .
  - CreateNamespace
  - CreateRole
  - CreateSecret
  - CreateWorkgroup
  - DeleteNamespace
  - DeleteRole
  - DeleteRolePolicy
  - DeleteSecret
  - DeleteWorkgroup
  - GetNamespace
  - GetRole
  - GetSecretValue
  - GetWorkgroup
  - PutRolePolicy
  - UpdateNamespace

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezL'utilisation de ce service avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Commencer à utiliser des clusters d'entrepôts de données provisionnés

L'exemple de code suivant illustre comment :

- Création d'un cluster Redshift
- Création d'un rôle IAM pour l'accès à S3
- Création de tables et chargement de données
- Exécuter des exemples de requêtes
- nettoyer des ressources ;

Bash

AWS CLI avec le script Bash

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code.

```
#!/bin/bash

# Amazon Redshift Provisioned Cluster Tutorial Script
# This script creates a Redshift cluster, loads sample data, runs queries, and
 cleans up resources
# Version 4: Security improvements and best practices

set -euo pipefail

# Set up logging
LOG_FILE="redshift_tutorial.log"
exec > >(tee -a "$LOG_FILE") 2>&1

echo "Starting Amazon Redshift tutorial script at $(date)"
echo "All commands and outputs will be logged to $LOG_FILE"

# Function to handle errors
handle_error() {
    echo "ERROR: $1" >&2
    echo "Resources created so far:"
```

```
    if [ -n "${CLUSTER_ID:-}" ]; then echo "- Redshift Cluster: $CLUSTER_ID"; fi
    if [ -n "${ROLE_NAME:-}" ]; then echo "- IAM Role: $ROLE_NAME"; fi

    echo "Attempting to clean up resources..."
    cleanup_resources
    exit 1
}

# Function to clean up resources
cleanup_resources() {
    echo "Cleaning up resources..."

    # Delete the cluster if it exists
    if [ -n "${CLUSTER_ID:-}" ]; then
        echo "Deleting Redshift cluster: $CLUSTER_ID"
        aws redshift delete-cluster --cluster-identifier "$CLUSTER_ID" --skip-
final-cluster-snapshot 2>/dev/null || true
        echo "Waiting for cluster deletion to complete..."
        aws redshift wait cluster-deleted --cluster-identifier "$CLUSTER_ID" 2>/
dev/null || true
        echo "Cluster deleted successfully."
    fi

    # Delete the IAM role if it exists
    if [ -n "${ROLE_NAME:-}" ]; then
        echo "Removing IAM role policy..."
        aws iam delete-role-policy --role-name "$ROLE_NAME" --policy-name
 RedshiftS3Access 2>/dev/null || true

        echo "Deleting IAM role: $ROLE_NAME"
        aws iam delete-role --role-name "$ROLE_NAME" 2>/dev/null || true
    fi

    # Clean up temporary files
    rm -f redshift-trust-policy.json redshift-s3-policy.json

    echo "Cleanup completed."
}

# Trap errors and cleanup
trap 'handle_error "Script interrupted"' INT TERM

# Function to wait for SQL statement to complete
wait_for_statement() {
```

```
    local statement_id=$1
    local max_attempts=30
    local attempt=1
    local status=""

    echo "Waiting for statement $statement_id to complete..."

    while [ $attempt -le $max_attempts ]; do
        status=$(aws redshift-data describe-statement --id "$statement_id" --
query 'Status' --output text 2>/dev/null || echo "")

        if [ "$status" == "FINISHED" ]; then
            echo "Statement completed successfully."
            return 0
        elif [ "$status" == "FAILED" ]; then
            local error=$(aws redshift-data describe-statement --id
 "$statement_id" --query 'Error' --output text 2>/dev/null || echo "Unknown
 error")
            echo "Statement failed with error: $error" >&2
            return 1
        elif [ "$status" == "ABORTED" ]; then
            echo "Statement was aborted." >&2
            return 1
        fi

        echo "Statement status: $status. Waiting... (Attempt $attempt/
$max_attempts)"
        sleep 10
        ((attempt++))
    done

    echo "Timed out waiting for statement to complete." >&2
    return 1
}

# Function to check if IAM role is attached to cluster
check_role_attached() {
    local role_arn=$1
    local max_attempts=10
    local attempt=1

    echo "Checking if IAM role is attached to the cluster..."

    while [ $attempt -le $max_attempts ]; do
```

```
        local status=$(aws redshift describe-clusters \
            --cluster-identifier "$CLUSTER_ID" \
            --query "Clusters[0].IamRoles[?IamRoleArn=='$role_arn'].ApplyStatus"
 \
            --output text 2>/dev/null || echo "")

        if [ "$status" == "in-sync" ]; then
            echo "IAM role is successfully attached to the cluster."
            return 0
        fi

        echo "IAM role status: $status. Waiting... (Attempt $attempt/
$max_attempts)"
        sleep 30
        ((attempt++))
    done

    echo "Timed out waiting for IAM role to be attached." >&2
    return 1
}

# Validate required commands
for cmd in aws jq; do
    if ! command -v "$cmd" &> /dev/null; then
        handle_error "Required command '$cmd' not found. Please install it and
 try again."
    fi
done

# Validate AWS credentials
if ! aws sts get-caller-identity &>/dev/null; then
    handle_error "AWS credentials not configured or invalid"
fi

# Variables to track created resources
CLUSTER_ID="examplecluster"
ROLE_NAME="RedshiftS3Role-$(date +%s)"
DB_NAME="dev"
DB_USER="awsuser"

# Generate secure password using AWS Secrets Manager or random string
if command -v openssl &> /dev/null; then
    DB_PASSWORD=$(openssl rand -base64 32 | tr -d "=+/" | cut -c1-20)
else
```

```
    DB_PASSWORD="TempPass$(date +%s | md5sum | cut -c1-20)"
fi

# Validate password meets requirements
if [ ${#DB_PASSWORD} -lt 8 ]; then
    handle_error "Generated password does not meet minimum length requirement"
fi

# Store password securely (optional: use AWS Secrets Manager in production)
echo "Generated database password (store securely): $DB_PASSWORD"

echo "=== Step 1: Creating Amazon Redshift Cluster ==="

# Create the Redshift cluster with encryption and audit logging enabled
echo "Creating Redshift cluster: $CLUSTER_ID"
CLUSTER_RESULT=$(aws redshift create-cluster \
  --cluster-identifier "$CLUSTER_ID" \
  --node-type ra3.xlplus \
  --number-of-nodes 2 \
  --master-username "$DB_USER" \
  --master-user-password "$DB_PASSWORD" \
  --db-name "$DB_NAME" \
  --port 5439 \
  --encrypted \
  --tags Key=project,Value=doc-smith Key=tutorial,Value=redshift-provisioned \
  2>&1) || handle_error "Failed to create Redshift cluster"

echo "$CLUSTER_RESULT"
echo "Waiting for cluster to become available..."

# Wait for the cluster to be available
aws redshift wait cluster-available --cluster-identifier "$CLUSTER_ID" ||
 handle_error "Timeout waiting for cluster to become available"

# Get cluster status to confirm
CLUSTER_STATUS=$(aws redshift describe-clusters \
  --cluster-identifier "$CLUSTER_ID" \
  --query 'Clusters[0].ClusterStatus' \
  --output text)

echo "Cluster status: $CLUSTER_STATUS"

echo "=== Step 2: Creating IAM Role for S3 Access ==="
```

```
# Create trust policy file with restricted permissions
echo "Creating trust policy for Redshift"
cat > redshift-trust-policy.json << 'EOF'
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF

chmod 600 redshift-trust-policy.json

# Create IAM role
echo "Creating IAM role: $ROLE_NAME"
ROLE_RESULT=$(aws iam create-role \
  --role-name "$ROLE_NAME" \
  --assume-role-policy-document file://redshift-trust-policy.json 2>&1) ||
 handle_error "Failed to create IAM role"

echo "$ROLE_RESULT"

# Get the role ARN
ROLE_ARN=$(aws iam get-role --role-name "$ROLE_NAME" --query 'Role.Arn' --output
 text)
echo "Role ARN: $ROLE_ARN"

# Tag the IAM role
echo "Tagging IAM role: $ROLE_NAME"
aws iam tag-role --role-name "$ROLE_NAME" --tags Key=project,Value=doc-smith
 Key=tutorial,Value=redshift-provisioned

# Create policy document for S3 access with principle of least privilege
echo "Creating S3 access policy"
cat > redshift-s3-policy.json << 'EOF'
{
  "Version":"2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::redshift-downloads",
        "arn:aws:s3:::redshift-downloads/*"
      ]
    }
  ]
}
EOF

chmod 600 redshift-s3-policy.json

# Attach policy to role
echo "Attaching S3 access policy to role"
POLICY_RESULT=$(aws iam put-role-policy \
  --role-name "$ROLE_NAME" \
  --policy-name RedshiftS3Access \
  --policy-document file://redshift-s3-policy.json 2>&1) || handle_error "Failed
 to attach policy to role"

echo "$POLICY_RESULT"

# Attach role to cluster
echo "Attaching IAM role to Redshift cluster"
ATTACH_ROLE_RESULT=$(aws redshift modify-cluster-iam-roles \
  --cluster-identifier "$CLUSTER_ID" \
  --add-iam-roles "$ROLE_ARN" 2>&1) || handle_error "Failed to attach role to
 cluster"

echo "$ATTACH_ROLE_RESULT"

# Wait for the role to be attached
echo "Waiting for IAM role to be attached to the cluster..."
if ! check_role_attached "$ROLE_ARN"; then
    handle_error "Failed to attach IAM role to cluster"
fi

echo "=== Step 3: Getting Cluster Connection Information ==="
```

```
# Get cluster endpoint
CLUSTER_INFO=$(aws redshift describe-clusters \
  --cluster-identifier "$CLUSTER_ID" \
  --query 'Clusters[0].Endpoint.{Address:Address,Port:Port}' \
  --output json)

echo "Cluster endpoint information:"
echo "$CLUSTER_INFO"

echo "=== Step 4: Creating Tables and Loading Data ==="

echo "Creating sales table"
SALES_TABLE_ID=$(aws redshift-data execute-statement \
  --cluster-identifier "$CLUSTER_ID" \
  --database "$DB_NAME" \
  --db-user "$DB_USER" \
  --sql "DROP TABLE IF EXISTS sales; CREATE TABLE sales(salesid integer not null,
 listid integer not null distkey, sellerid integer not null, buyerid integer
 not null, eventid integer not null, dateid smallint not null sortkey, qtysold
 smallint not null, pricepaid decimal(8,2), commission decimal(8,2), saletime
 timestamp);" \
  --query 'Id' --output text)

echo "Sales table creation statement ID: $SALES_TABLE_ID"

# Wait for statement to complete
if ! wait_for_statement "$SALES_TABLE_ID"; then
    handle_error "Failed to create sales table"
fi

echo "Creating date table"
DATE_TABLE_ID=$(aws redshift-data execute-statement \
  --cluster-identifier "$CLUSTER_ID" \
  --database "$DB_NAME" \
  --db-user "$DB_USER" \
  --sql "DROP TABLE IF EXISTS date; CREATE TABLE date(dateid smallint not null
 distkey sortkey, caldate date not null, day character(3) not null, week smallint
 not null, month character(5) not null, qtr character(5) not null, year smallint
 not null, holiday boolean default('N'));" \
  --query 'Id' --output text)

echo "Date table creation statement ID: $DATE_TABLE_ID"

# Wait for statement to complete
```

```
if ! wait_for_statement "$DATE_TABLE_ID"; then
    handle_error "Failed to create date table"
fi

echo "Loading data into sales table"
SALES_LOAD_ID=$(aws redshift-data execute-statement \
  --cluster-identifier "$CLUSTER_ID" \
  --database "$DB_NAME" \
  --db-user "$DB_USER" \
  --sql "COPY sales FROM 's3://redshift-downloads/tickit/sales_tab.txt' DELIMITER
 '\t' TIMEFORMAT 'MM/DD/YYYY HH:MI:SS' REGION 'us-east-1' IAM_ROLE '$ROLE_ARN';"
 \
  --query 'Id' --output text)

echo "Sales data load statement ID: $SALES_LOAD_ID"

# Wait for statement to complete
if ! wait_for_statement "$SALES_LOAD_ID"; then
    handle_error "Failed to load data into sales table"
fi

echo "Loading data into date table"
DATE_LOAD_ID=$(aws redshift-data execute-statement \
  --cluster-identifier "$CLUSTER_ID" \
  --database "$DB_NAME" \
  --db-user "$DB_USER" \
  --sql "COPY date FROM 's3://redshift-downloads/tickit/date2008_pipe.txt'
 DELIMITER '|' REGION 'us-east-1' IAM_ROLE '$ROLE_ARN';" \
  --query 'Id' --output text)

echo "Date data load statement ID: $DATE_LOAD_ID"

# Wait for statement to complete
if ! wait_for_statement "$DATE_LOAD_ID"; then
    handle_error "Failed to load data into date table"
fi

echo "=== Step 5: Running Example Queries ==="

echo "Running query: Get definition for the sales table"
QUERY1_ID=$(aws redshift-data execute-statement \
  --cluster-identifier "$CLUSTER_ID" \
  --database "$DB_NAME" \
  --db-user "$DB_USER" \
```

```
  --sql "SELECT * FROM pg_table_def WHERE tablename = 'sales';" \
  --query 'Id' --output text)

echo "Query 1 statement ID: $QUERY1_ID"

# Wait for statement to complete
if ! wait_for_statement "$QUERY1_ID"; then
    handle_error "Query 1 failed"
fi

# Get and display results
echo "Query 1 results (first 10 rows):"
aws redshift-data get-statement-result --id "$QUERY1_ID" --max-items 10

echo "Running query: Find total sales on a given calendar date"
QUERY2_ID=$(aws redshift-data execute-statement \
  --cluster-identifier "$CLUSTER_ID" \
  --database "$DB_NAME" \
  --db-user "$DB_USER" \
  --sql "SELECT sum(qtysold) FROM sales, date WHERE sales.dateid = date.dateid
 AND caldate = '2008-01-05';" \
  --query 'Id' --output text)

echo "Query 2 statement ID: $QUERY2_ID"

# Wait for statement to complete
if ! wait_for_statement "$QUERY2_ID"; then
    handle_error "Query 2 failed"
fi

# Get and display results
echo "Query 2 results:"
aws redshift-data get-statement-result --id "$QUERY2_ID"

echo "=== Tutorial Complete ==="
echo "The following resources were created:"
echo "- Redshift Cluster: $CLUSTER_ID"
echo "- IAM Role: $ROLE_NAME"

echo ""
echo "========================================="
echo "CLEANUP CONFIRMATION"
echo "========================================="
echo "Cleaning up all created resources..."
```

```
cleanup_resources
echo "All resources have been cleaned up."

# Securely clear password from memory
DB_PASSWORD=""

echo "Script completed at $(date)"
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des commandes de l'AWS CLI .
  - CreateCluster
  - CreateRole
  - DeleteCluster
  - DeleteRole
  - DeleteRolePolicy
  - DescribeClusters
  - GetRole
  - ModifyClusterIamRoles
  - PutRolePolicy
  - Attente

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezL'utilisation de ce service avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Historique du document

> **Note**
>
> Pour une description des nouvelles fonctionnalités d'Amazon Redshift, consultez Nouveautés.

La table suivante décrit les modifications significatives apportées au document Guide de gestion Amazon Redshift après juin 2018. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

Version de l'API : 2012-12-01

Pour obtenir une liste des modifications apportées au Manuel du développeur de base de données Amazon Redshift, consultez l'Historique des documents du guide du développeur de base de données Amazon Redshift.

Modification	Description	Date
Le correctif 205 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez le correctif 205 d'Amazon Redshift.	16 septembre 2026
Le correctif 204 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires	11 août 2026

	pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez le correctif 204 d'Amazon Redshift.	
Le correctif 203 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez le correctif 203 d'Amazon Redshift.	6 juillet 2026
Le correctif 202 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez le correctif 202 d'Amazon Redshift.	28 mai 2026

Le patch 201 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez le correctif Amazon Redshift 201.	22 avril 2026
Le correctif 200 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez Amazon Redshift patch 200.	26 mars 2026
Le patch 199 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez le correctif 199 d'Amazon Redshift.	4 mars 2026

Le correctif 198 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez le correctif 198 d'Amazon Redshift.	3 février 2026
Mise à jour des politiques gérées Amazon Redshift	Ajout d'une nouvelle politique `AmazonRedshiftFederatedAuthorization` gérée.	21 novembre 2025
Le correctif 197 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez le correctif 197 d'Amazon Redshift.	20 novembre 2025

Le patch 196 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez le correctif 196 d'Amazon Redshift.	10 novembre 2025
Le patch 195 d'Amazon Redshift est sorti.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 195 d'Amazon Redshift.	24 octobre 2025

Le patch 194 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 194 d'Amazon Redshift.	1er octobre 2025
Le patch 193 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 193 d'Amazon Redshift.	26 août 2025

Le correctif 192 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 192 d'Amazon Redshift.	30 juillet 2025
Le correctif 191 d'Amazon Redshift est sorti.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 191 d'Amazon Redshift.	24 juin 2025

Le patch 190 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 190 d'Amazon Redshift.	7 mai 2025
Mise à jour des politiques gérées Amazon Redshift	Mises à jour de la politique gérée par `AmazonRedshiftServiceLinkedRolePolicy` avec l'autorisation `lakeformation:GetDataAccess` .	13 mars 2025
Le correctif 189 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 189 d'Amazon Redshift.	07 mars 2025

Le patch 188 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 188 d'Amazon Redshift.	5 février 2025
Le correctif 187 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 187 d'Amazon Redshift.	20 décembre 2024
Mise à jour des politiques gérées Amazon Redshift	Mises à jour de la politique gérée `AmazonRedshiftServiceLinkedRolePolicy` avec les autorisations `glue:GetCatalog` et `glue:GetCatalogs`.	3 décembre 2024

Le correctif 186 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 186 d’Amazon Redshift.	22 octobre 2024
Le correctif 185 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 185 d’Amazon Redshift.	9 octobre 2024

Le correctif 184 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 184 d'Amazon Redshift.	12 septembre 2024
Le correctif 183 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 183 d'Amazon Redshift.	8 août 2024

Le correctif 182 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 182 d'Amazon Redshift.	26 juin 2024
Le correctif 181 d'Amazon Redshift a été publié.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 181 d'Amazon Redshift.	1 mai 2024
Mise à jour des politiques gérées Amazon Redshift	Mise à jour vers la politique gérée `AmazonRedshiftServiceLinkedRolePolicy` avec autorisation `servicequotas:GetServiceQuota` pour accéder aux quotas ou aux limites AWS .	8 mars 2024

Mise à jour des politiques gérées de l'éditeur de requêtes v2	Effectue une mise à jour vers les politiques gérées `AmazonRedshiftQueryEditorV2NoSharing`, `AmazonRedshiftQueryEditorV2ReadSharing`, `AmazonRedshiftQueryEditorV2FullAccess` et `AmazonRedshiftQueryEditorV2ReadWriteSharing` avec les autorisations `redshift-serverless:ListNamespaces` et `redshift-serverless:ListWorkgroups`.	21 février 2024
Mettre à jour la politique de gestion de l'accès en lecture seule d'Amazon Redshift	Met à jour vers la politique gérée `AmazonRedshiftReadOnlyAccess` avec autorisation `redshift:ListRecommendations` pour répertorier les recommandations d'Amazon Redshift Advisor.	7 février 2024

Le correctif 180 d'Amazon Redshift est disponible.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez Correctif 180 d'Amazon Redshift.	29 décembre 2023
Le correctif 179 d'Amazon Redshift est disponible.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez Correctif 179 d'Amazon Redshift.	9 novembre 2023
Mise à jour des politiques gérées Amazon Redshift	Mises à jour de la politique gérée `AmazonRedshiftServiceLinkedRolePolicy` avec les autorisations `ec2:AssignIpv6Addresses` et `ec2:UnassignIpv6Addresses` .	31 octobre 2023

Le correctif 178 d’Amazon Redshift est disponible.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 178 d'Amazon Redshift.	25 septembre 2023
Mise à jour des politiques gérées de l’éditeur de requêtes v2	Effectue une mise à jour vers les politiques gérées `AmazonRedshiftQueryEditorV2NoSharing`, `AmazonRedshiftQueryEditorV2ReadSharing` et `AmazonRedshiftQueryEditorV2ReadWriteSharing` avec les autorisations `sqlworkbench:GetAutocompletionMetadata` et `sqlworkbench:GetAutocompletionResource`.	16 août 2023

Mise à jour de la politique gérée Amazon Redshift	Mises à jour de la politique `AmazonRedshiftServiceLinkedRolePolicy` gérée permettant d'accorder des autorisations AWS Secrets Manager pour créer et gérer les secrets d'identification des administrateurs.	14 août 2023
Le correctif 177 d'Amazon Redshift est disponible.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 177 d'Amazon Redshift.	3 août 2023
Le correctif 176 d'Amazon Redshift est disponible.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 176 d'Amazon Redshift.	8 juin 2023

Le correctif 175 d'Amazon Redshift est disponible.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 175 d'Amazon Redshift.	28 avril 2023
Mise à jour de la politique gérée Amazon Redshift	Mises à jour apportées à la politique gérée `AmazonRedshiftServiceLinkedRolePolicy` afin de supprimer les autorisations pour les actions liées au réseau ec2. Ils étaient spécifiquement associés à la balise de Purpose:RedshiftMigrateToVpcressource.	27 avril 2023
Mettre à jour la politique gérée de l'API de données d'Amazon Redshift	Mises à jour de la politique gérée par `AmazonRedshiftDataFullAccess` avec l'autorisation `redshift:GetClusterCredentialsWithIAM` .	7 avril 2023

Mise à jour des politiques gérées de l'éditeur de requêtes v2	Effectue une mise à jour vers les politiques gérées `AmazonRedshiftQueryEditorV2NoSharing`, `AmazonRedshiftQueryEditorV2ReadSharing` et `AmazonRedshiftQueryEditorV2ReadWriteSharing` avec l'autorisation `sqlworkbench:GetSchemaInference`.	21 mars 2023
Le correctif 174 d'Amazon Redshift est disponible.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 174 d'Amazon Redshift.	11 mars 2023

Mise à jour des politiques gérées de l'éditeur de requêtes v2	Effectue une mise à jour vers les politiques gérées `AmazonRedshiftQueryEditorV2NoSharing`, `AmazonRedshiftQueryEditorV2ReadSharing` et `AmazonRedshiftQueryEditorV2ReadWriteSharing` avec l'autorisation `sqlworkbench:AssociateNotebookWithTab`.	2 février 2023
Le correctif 173 d'Amazon Redshift est disponible.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour en savoir plus sur cette version, consultez Correctif 173 d'Amazon Redshift.	20 janvier 2023

Le correctif 172 d’Amazon Redshift est disponible.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez Amazon Redshift patch 172 (Correctif 172 d'Amazon Redshift).	17 novembre 2022
Le correctif 171 d’Amazon Redshift est disponible.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez Amazon Redshift patch 171 (Correctif 171 d'Amazon Redshift).	9 novembre 2022

Le correctif 170 d’Amazon Redshift est disponible.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez Correctif 170 d'Amazon Redshift.	20 juillet 2022
Le correctif 169 d’Amazon Redshift est disponible.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez Amazon Redshift patch 169 (Correctif 169 d'Amazon Redshift).	8 juin 2022

Le correctif 168 d’Amazon Redshift est disponible.	Un nouveau correctif Amazon Redshift est en cours de déploiement. Plusieurs semaines sont nécessaires pour qu'une nouvelle version soit disponible dans tous les appareils Amazon Redshift pris en charge. Régions AWS Pour plus d'informations sur cette version, consultez Amazon Redshift patch 168 (Correctif 168 d'Amazon Redshift).	19 avril 2022
Prise en charge des profils d’authentification avec les pilotes Amazon Redshift	Vous pouvez maintenant vous connecter à Amazon Redshift avec un profil d’authentification .	2 août 2021
Support des points de terminaison inter-VPC pour Amazon Redshift, alimenté par AWS PrivateLink	Vous pouvez désormais utiliser les points de terminaison Redshift-managed VPC avec Amazon Redshift.	1 avril 2021
Prise en charge des améliorations apportées à l’éditeur de requêtes Amazon Redshift	Vous pouvez maintenant utiliser l’éditeur de requêtes avec le routage VPC amélioré, des temps d’exécution des requêtes plus longs et plus de types de nœuds de cluster.	17 février 2021
Prise en charge de l’intégration de la console avec les partenaires	Vous pouvez intégrer vos partenaires à l’aide de la console Amazon Redshift.	9 décembre 2020

Prise en charge de la possibilité de déplacer des clusters entre des zones de disponibilité	Vous pouvez désormais déplacer des clusters RA3 entre les zones de disponibilité.	9 décembre 2020
Prise en charge des types de nœuds ra3.xlplus	Vous pouvez maintenant créer des noeuds de type ra3.xlplus.	9 décembre 2020
Prise en charge du pilote JDBC version 2.0	Vous pouvez désormais configurer le pilote JDBC version 2.0.	5 novembre 2020
Prise en charge des fonctions UDF Lambda et de la création de jetons	Vous pouvez maintenant écrire des fonctions UDF Lambda pour activer la création de jetons externe des données.	26 octobre 2020
Prise en charge de la planification de l'exécution d'une instruction SQL	Vous pouvez désormais planifier une requête sur la console Amazon Redshift.	22 octobre 2020
Prise en charge de l'API de données pour Amazon Redshift	Vous pouvez désormais accéder à Amazon Redshift à l'aide de l'API de données intégrée. La documentation mise à jour comprend la Référence de l'API de données Amazon Redshift.	10 septembre 2020
Prise en charge de la surveillance des requêtes de la console Amazon Redshift	Mise à jour du guide pour décrire les nouveaux graphiques de surveillance des requêtes.	7 mai 2020
Prise en charge des limites d'utilisation	Mise à jour du guide pour décrire les limites d'utilisation.	23 avril 2020

Multi-factor authentification	Mise à jour du guide pour décrire la prise en charge de l'authentification multifacteur.	20 avril 2020
Le redimensionnement élastique prend désormais en charge les modifications de type de nœud	Mise à jour de la descripti on du redimensionnement élastique.	6 avril 2020
Prise en charge des types de nœuds ra3.4xlarge avec stockage géré	Mise à jour du guide pour inclure les types de nœuds ra3.4xlarge.	2 avril 2020
Prise en charge de la pause et de la reprise	Mise à jour du guide pour décrire la pause et la reprise des opérations de cluster.	11 mars 2020
Prise en charge de Microsoft Azure AD en tant que fournisseur d'identité	Mise à jour du guide pour décrire les étapes à suivre pour utiliser Microsoft Azure AD en tant que fournisseur d'identité.	10 février 2020
Prise en charge du type de nœud RA3	Mise à jour du guide pour décrire le nouveau type de nœud RA3.	3 décembre 2019
Prise en charge de la nouvelle console	Manuel mis à jour pour décrire la nouvelle console Amazon Redshift.	11 novembre 2019
Mise à jour des informations de sécurité	Mises à jour de la documenta tion sur les informations de sécurité.	24 juin 2019

Améliorations de l’instantané	Amazon Redshift prend désormais en charge plusieurs améliorations relatives à la gestion et à la planification des instantanés.	4 avril 2019
Mise à l’échelle de la simultanéité	Vous pouvez configurer la gestion de la charge de travail (WLM) pour activer le mode de mise à l’échelle de la simultanéité. Pour plus d’informations, consultez Configuration de la gestion de la charge de travail.	21 mars 2019
Mise à jour des pilotes JDBC et ODBC	Amazon Redshift prend désormais en charge les nouvelles versions des pilotes JDBC et ODBC. Pour plus d’informations, consultez Configurer une connexion JDBC.	4 février 2019

Maintenance différée	Si vous avez besoin de replanifier la fenêtre de maintenance de votre cluster, vous avez la possibilité de reporter la maintenance de 14 jours au plus. Si nous avons besoin de mettre à jour du matériel ou d'effectuer d'autres mises à jour obligatoires au cours de votre période de report, nous vous en avertissons et effectuons les modifications requises. Votre cluster n'est pas disponible au cours de ces mises à jour. Pour plus d'informations, consultez Report de la maintenance.	20 novembre 2018

Notification préalable	Amazon Redshift fournit une notification préalable pour certains événements. Ces événements entrent dans la catégorie d'événement `pending`. Par exemple, nous envoyons une notification préalable si une mise à jour matérielle est requise pour l'un des nœuds de votre cluster. Vous pouvez vous abonner aux événements en attente (pending) de la même manière qu'aux autres événements Amazon Redshift. Pour plus d'informations, consultez Abonnement aux notifications d'événement Amazon Redshift.	20 novembre 2018

Elastic resize (Redimensionnement élastique)	Le redimensionnement élastique est la méthode la plus rapide pour redimensionner un cluster. Le redimensionnement élastique ajoute ou supprime des nœuds dans un cluster existant, puis redistribue automatiquement les données aux nouveaux nœuds. Comme elle ne crée pas un nouveau cluster, l'opération de redimensionnement élastique se termine rapidement, généralement en quelques minutes. Pour plus d'informations, consultez Redimensionnement des clusters.	15 novembre 2018
Annuler l'opération de redimensionnement	Vous pouvez désormais annuler une opération de redimensionnement en cours. Pour plus d'informations, consultez Présentation de l'opération de redimensionnement.	2 novembre 2018

Modifier le cluster pour modifier le chiffrement	Vous pouvez modifier un cluster non chiffré pour utiliser le chiffrement AWS Key Management Service (AWS KMS), à l'aide d'une clé AWS gérée ou d'une clé gérée par le client. Lorsque vous modifiez votre cluster pour activer le chiffreme nt KMS, Amazon Redshift migre automatiquement vos données vers un nouveau cluster chiffré. Vous pouvez également migrer un cluster non chiffré vers un cluster chiffré en modifiant le cluster.	16 octobre 2018
Amazon Redshift Spectrum prend en charge le routage VPC amélioré	Vous pouvez désormais utiliser Redshift Spectrum avec le routage VPC amélioré activé pour votre cluster. Vous pouvez avoir besoin d'effectu er des étapes de configura tion supplémentaires. Pour plus d'informations, consultez Utilisation d'Amazon Redshift Spectrum avec le routage VPC amélioré.	10 octobre 2018
Éditeur de requête	Vous pouvez désormais exécuter des requêtes SQL à partir de la console de gestion Amazon Redshift.	4 octobre 2018

Graphique de répartition de l'exécution de la charge de travail	Vous pouvez désormais obtenir une vue détaillée des performances de votre charge de travail en consultant le graphique de répartition de l'exécution de la charge de travail dans la console. Pour plus d'informations, consultez Analyse des performances de la charge de travail.	30 juillet 2018
Suivis de maintenance	Vous pouvez désormais déterminer si votre cluster sera toujours mis à jour vers la dernière version d'Amazon Redshift ou vers une version antérieure en choisissant un suivi de maintenance. Pour plus d'informations, consultez Choix des suivis de maintenance de cluster.	26 juillet 2018

Le tableau suivant décrit les modifications importantes apportées au Guide de gestion Amazon Redshift avant juillet 2018.

Modifier	Description	Date de publication
Nouveaux CloudWatch indicateurs	De nouvelles CloudWatch mesures ont été ajoutées pour surveiller les performances des requêtes. Pour plus d'informations, consultez Données de performances dans Amazon Redshift	17 mai 2018
Chiffrement HSM	Amazon Redshift prend uniquement en charge la gestion AWS CloudHSM des clés du module de sécurité matérielle (HSM). Pour plus d'informations,	6 mars 2018

Modifier	Description	Date de publication
	consultez Chiffrement de base de données Amazon Redshift.	
Création de chaînes de rôles IAM	Si un rôle IAM attaché à votre cluster n'a pas accès aux ressources nécessaires, vous pouvez créer une chaîne avec un autre rôle, lequel peut appartenir à un autre compte. Votre cluster endosse alors provisoirement le rôle relié par la chaîne afin d'accéder aux données. Vous pouvez également accorder des accès entre comptes en créant des chaînes de rôles. Chaque rôle de la chaîne passe au rôle suivant, jusqu'à ce que le cluster endosse le dernier rôle de la chaîne. Une chaîne comprend 10 rôles maximum. Pour plus d'informations, consultez Chaînage des rôles IAM dans Amazon Redshift.	23 février 2018
Nouveaux types de nœuds DC2	La nouvelle génération de types de nœuds de calcul dense (DC) offre des performances bien supérieures à celles des nœuds DC1, pour le même prix. Pour bénéficier d'améliorations de performances, vous pouvez migrer votre cluster DC1 vers des nœuds de type DC2 plus récents. Pour plus d'informations, consultez Clusters et nœuds dans Amazon Redshift.	17 octobre 2017
Certificats ACM	Amazon Redshift remplace les certificats SSL sur vos clusters par les certificats émis par AWS Certificate Manager (ACM). ACM est une autorité de certification publique de confiance, approuvée par la plupart des systèmes actuels. Il se peut que vous ayez besoin de mettre à jour vos certificats actuels d'autorité de certification racine approuvée pour pouvoir continuer à vous connecter à vos clusters à l'aide du protocole SSL. Pour plus d'informations, consultez Transition vers les certificats ACM pour les connexions SSL.	18 septembre 2017

Modifier	Description	Date de publication
Service-linked rôles	Un rôle lié à un service est un type unique de rôle IAM directement lié à Amazon Redshift. Service-linked les rôles sont prédéfinis par Amazon Redshift et incluent toutes les autorisations requises par le service pour appeler AWS des services au nom de votre cluster Amazon Redshift. Pour plus d'informations, consultez Utilisation des rôles liés à un service pour Amazon Redshift.	18 septembre 2017
Authentification de l'utilisateur de base de données IAM	Vous pouvez configurer votre système de manière à permettre aux utilisateurs de créer des informations d'identification utilisateur et de se connecter aux bases de données en fonction de leurs informations d'identification IAM. Vous pouvez aussi configurer votre système pour permettre aux utilisateurs de se connecter à l'aide de l'authentification unique fédérée via un fournisseur d'identité conforme à SAML 2.0. Pour plus d'informations, consultez Utilisation de l'authentification IAM pour générer des informations d'identification de l'utilisateur de base de données.	11 août 2017
Table-level la restauration prend en charge le routage VPC amélioré	Table-level la restauration est désormais prise en charge sur les clusters qui utilisentContrôle du trafic réseau avec le routage VPC amélioré. Pour plus d'informations, consultez Restauration d'une table à partir d'un instantané.	19 juillet 2017

Modifier	Description	Date de publication
Règles de surveillance de requête	À l'aide des règles de surveillance des requêtes WLM, vous pouvez définir des limites de performance basées sur des métriques pour les files d'attente WLM et spécifier l'action à entreprendre lorsqu'une requête dépasse ces limites — log, hop ou abort. Vous définissez les règles de surveillance de requête dans le cadre de la configuration de la gestion de la charge de travail (WLM). Pour plus d'informations, consultez Gestion de la charge de travail.	21 avril 2017
Routage VPC amélioré	Lorsque vous utilisez le routage VPC amélioré Amazon Redshift, Amazon Redshift force l'ensemble du trafic COPY et UNLOAD entre votre cluster et vos référentiels de données à traverser votre réseau Amazon VPC. Pour plus d'informations, consultez Contrôle du trafic réseau avec le routage VPC amélioré Redshift.	le 15 septembre 2016
Nouveaux champs de journal de connexion	Le journal d'audit Journal de connexion comporte deux nouveaux champs pour suivre les connexions SSL. Si vous chargez régulièrement les journaux d'audit dans une table Amazon Redshift, vous devrez ajouter les nouvelles colonnes suivantes à la table cible : sslcompression et sslexpansion.	5 mai 2016

Modifier	Description	Date de publication
Rôles IAM pour les commandes COPY et UNLOAD	Vous pouvez désormais spécifier un ou plusieurs rôles Gestion des identités et des accès AWS (IAM) que votre cluster peut utiliser pour s'authentifier afin d'accéder à d'autres AWS services. Les rôles IAM offrent une alternative plus sécurisée pour fournir une authentification avec les commandes COPY, UNLOAD ou CREATE LIBRARY. Pour plus d'informations, consultez Autorisation d'accès à Amazon Redshift AWS services en votre nom et Autorisation des opérations COPY, UNLOAD, CREATE EXTERNAL FUNCTION et CREATE EXTERNAL SCHEMA à l'aide des rôles IAM.	29 mars 2016
Restaurer à partir de la table	Vous pouvez restaurer une table à partir d'un instantané de cluster vers une nouvelle table dans un cluster actif. Pour plus d'informations, consultez Restauration d'une table à partir d'un instantané.	10 mars 2016
Utilisation de la condition IAM dans les politiques	Vous pouvez restreindre davantage l'accès aux ressources à l'aide de l'élément Condition dans les politiques IAM. Pour plus d'informations, consultez Utilisation de conditions de politique IAM pour un contrôle d'accès précis.	10 décembre 2015
Modifier l'accessibilité publique	Vous pouvez modifier un cluster existant dans un VPC pour changer sont accessibilité publique. Pour plus d'informations, consultez Modification d'un cluster.	20 novembre 2015
Correctifs de la documentation	Publication de divers correctifs de la documentation.	28 août 2015

Modifier	Description	Date de publication
Mise à jour de la documentation	Mise à jour des conseils de dépannage sur la configuration des paramètres réseau pour s'assurer que les hôtes ayant différentes tailles d'unité de transmission maximale (MTU) puissent déterminer la taille de paquet d'une connexion. Pour plus d'informations, consultez Des requêtes semblent se bloquer et parfois échouent à atteindre le cluster.	25 août 2015
Mise à jour de la documentation	Révision de la totalité de la section sur les groupes de paramètres pour une meilleure organisation et plus de clarté. Pour plus d'informations, consultez Groupes de paramètres Amazon Redshift.	17 août 2015
Propriétés dynamiques WLM	Le paramètre de configuration WLM prend désormais en charge l'application dynamique de certaines propriétés. D'autres propriétés restent statiques et nécessitent que les clusters associés soient redémarrés afin que les modifications de configuration puissent être appliquées. Pour plus d'informations, consultez Propriétés WLM dynamiques et statiques et Groupes de paramètres Amazon Redshift.	3 août 2015
Copier des clusters chiffrés KMS vers une autre AWS région	Ajout de contenu sur la configuration des autorisations de copie instantanée pour permettre la copie de clusters AWS KMS chiffrés vers une autre AWS région. Pour plus d'informations, consultez Copier AWS KMS—instantanés chiffrés vers un autre Région AWS.	28 juillet 2015

Modifier	Description	Date de publication
Mise à jour de la documentation	Mise à jour de la section sur le chiffrement de la base de données afin de mieux expliquer comment Amazon Redshift utilise AWS KMS les HSM pour gérer les clés, et comment le processus de chiffrement fonctionne avec chacune de ces options. Pour plus d'informations, consultez Chiffrement de base de données Amazon Redshift.	28 juillet 2015
Nouveau type de nœud	Amazon Redshift propose désormais un nouveau type de nœud, le DS2. Mise à jour des références de documentation sur les types de nœud existants pour utiliser les nouveaux noms présentés dans cette version. Révision également de la section afin de mieux expliquer les combinaisons de types de nœuds et préciser les limites de quota par défaut. Pour plus d'informations, consultez Clusters et nœuds dans Amazon Redshift.	9 juin 2015
Offres relatives aux nœuds réservés	Ajout de contenu sur les nouvelles offres de nœuds réservés. Révision également de la section afin de mieux expliquer et comparer les offres disponibles et présentation d'exemples pour montrer comment la tarification à la demande et de nœud réservé affecte la facturation. Pour plus d'informations, consultez Nœuds réservés.	9 juin 2015
Correctifs de la documentation	Publication de divers correctifs de la documentation.	30 avril 2015

Modifier	Description	Date de publication
Nouvelle fonctionnalité	Cette version d'Amazon Redshift présente de nouveaux pilotes ODBC et JDBC, optimisés pour une utilisation avec Amazon Redshift. Pour plus d'informations, consultez En vous connectant à un entrepôt de données Amazon Redshift à l'aide des outils client SQL.	26 février 2015
Nouvelle fonctionnalité	Cette version d'Amazon Redshift présente les métriques de performances du cluster qui vous permettent d'afficher et d'analyser les détails de l'exécution des requêtes. Pour plus d'informations, consultez Affichage des requêtes et des charges.	26 février 2015
Mise à jour de la documentation	Ajout d'un nouvel exemple de politique illustrant l'octroi d'autorisations aux actions de AWS service et aux ressources courantes sur lesquelles Amazon Redshift s'appuie. Pour plus d'informations, consultez Exemples de politiques gérées par le client.	16 janvier 2015
Mise à jour de la documentation	Instructions mises à jour concernant le réglage de l'unité de transmission maximale (MTU) pour désactiver les trames TCP/IP jumbo. Pour plus d'informations, consultez Utiliser EC2 pour créer votre cluster et Des requêtes semblent se bloquer et parfois échouent à atteindre le cluster.	16 janvier 2015
Mise à jour de la documentation	Nous avons révisé le contenu relatif au `wlm_json_configuration` paramètre et fourni un exemple de syntaxe pour configurer ce paramètre à AWS CLI l'aide des systèmes d'exploitation Linux, macOS et Microsoft Windows. Pour plus d'informations, consultez Gestion de la charge de travail.	13 janvier 2015

Modifier	Description	Date de publication
Mise à jour de la documentation	Ajout des notifications d'événements et des descriptions manquantes. Pour plus d'informations, consultez Notifications d'événement d'un cluster alloué Amazon Redshift.	8 janvier 2015
Mise à jour de la documentation	Mise à jour des recommandations sur les politiques IAM pour les actions et les ressources Amazon Redshift. Révision de la section pour plus d'organisation et de clarté. Pour plus d'informations, consultez Sécurité dans Amazon Redshift.	21 novembre 2014
Nouvelle fonctionnalité	Cette version d'Amazon Redshift introduit la possibilité de chiffrer des clusters à l'aide de clés de chiffrement provenant de AWS Key Management Service ().AWS KMS AWS KMS combine du matériel et des logiciels sécurisés et hautement disponibles pour fournir un système de gestion des clés adapté au cloud. Pour plus d'informations sur Amazon Redshift AWS KMS et les options de chiffrement disponibles, consultez Chiffrement de base de données Amazon Redshift et. Opérations de cluster	12 novembre 2014
Nouvelle fonctionnalité	Cette version d'Amazon Redshift présente la possibilité d'étiqueter les ressources, telles que les clusters et les instantanés. Les balises vous permettent de fournir des métadonnées définies par l'utilisateur afin de classer vos rapports de facturation en fonction de la répartition des coûts et de vous aider à mieux identifier les ressources d'un coup d'œil. Pour plus d'informations, consultez Étiqueter les ressources dans Amazon Redshift..	4 novembre 2014

Modifier	Description	Date de publication
Nouvelle fonctionnalité	Augmentation de la limite de nœud maximale de 128 nœuds pour les tailles de nœud dw1.8xlarge et dw2.8xlarge. Pour plus d'informations, consultez Clusters et nœuds dans Amazon Redshift.	30 octobre 2014
Nouvelle fonctionnalité	Ajout de la possibilité de mettre fin aux requêtes et aux chargements depuis la console Amazon Redshift. Pour plus d'informations, consultez Affichage des requêtes et des charges et Affichage des métriques du cluster pendant les opérations de chargement.	28 octobre 2014
Correctifs de la documentation	Publication de divers correctifs de la documentation.	17 octobre 2014
Nouveau contenu	Ajout de contenu sur l'arrêt et la suppression des clusters. Pour plus d'informations, consultez Arrêt et suppression d'un cluster.	14 août 2014
Mise à jour de la documentation	Clarification du comportement du paramètre Autoriser la mise à niveau de la version pour les clusters. Pour plus d'informations, consultez Clusters Amazon Redshift provisionnés.	14 août 2014
Mise à jour de la documentation	Révision des procédures, captures d'écran et organisation de la rubrique sur l'utilisation de clusters dans la console Amazon Redshift. Pour plus d'informations, consultez Opérations de cluster.	11 juillet 2014
Nouveau contenu	Ajout d'un nouveau didacticiel sur le redimensionnement des clusters Amazon Redshift, notamment sur la manière de redimensionner un cluster tout en réduisant la durée pendant laquelle le cluster est en mode lecture seule. Pour plus d'informations, consultez Redimensionnement d'un cluster.	27 juin 2014

Modifier	Description	Date de publication
Nouvelle fonctionnalité	Ajout de la possibilité de renommer les clusters. Pour plus d'informations, consultez Renommer un cluster et Modification d'un cluster.	2 juin 2014
Nouvelle fonctionnalité	Ajout d'options permettant de sélectionner un groupe de paramètres et un groupe de sécurité différents lorsque vous restaurez un cluster à partir d'un instantané. Pour plus d'informations, consultez Restauration d'un cluster à partir d'un instantané.	12 mai 2014
Nouvelle fonctionnalité	Ajout d'une nouvelle section décrivant comment configurer une CloudWatch alarme Amazon par défaut pour surveiller le pourcentage d'espace disque utilisé dans un cluster Amazon Redshift. Cette alarme est une nouvelle option du processus de création du cluster. Pour plus d'informations, consultez Alarme d'espace disque par défaut.	28 avril 2014
Mise à jour de la documentation	Clarification des informations sur la prise en charge d'ECDHE (Elliptic curve Diffie—Hellman Exchange) dans Amazon Redshift. Pour plus d'informations, consultez SSL.	22 avril 2014
Nouvelle fonctionnalité	Ajout d'une déclaration sur la prise en charge par Amazon Redshift du protocole d'accord de clé ECDH (Elliptic curve Diffie—Hellman). Pour plus d'informations, consultez SSL.	18 avril 2014
Mise à jour de la documentation	Révision et réorganisation des rubriques de la section En vous connectant à un entrepôt de données Amazon Redshift à l'aide des outils client SQL. Ajout d'informations sur les connexions JDBC et ODBC et d'une nouvelle section de résolution des problèmes de connexion.	15 avril 2014

Modifier	Description	Date de publication
Mise à jour de la documentation	Ajout de la version dans les exemples de politiques IAM de ce guide.	3 avril 2014
Mise à jour de la documentation	Ajout d'informations sur le fonctionnement de la tarification lorsque vous redimensionnez un cluster. Pour plus d'informations, consultez Nœuds réservés.	2 avril 2014
Nouvelle fonctionnalité	Ajout d'une section sur un nouveau paramètre, `max_cursor_result_set_size` , qui définit la taille maximale du jeu de résultats, en mégaoctets, qui peut être stocké par curseur individuel. Cette valeur de paramètre affecte également le nombre de curseurs simultanément actifs pour le cluster. Pour plus d'informations, consultez Groupes de paramètres Amazon Redshift.	28 mars 2014
Nouvelle fonctionnalité	Ajout d'une explication sur le champ Version du cluster incluant à présent la version du moteur du cluster et le de révision de la base de données. Pour plus d'informations, consultez Clusters Amazon Redshift provisionnés.	21 mars 2014
Nouvelle fonctionnalité	Mise à jour de la procédure de redimensionnement pour afficher les nouvelles informations de progression du redimensionnement sur l'onglet État du cluster. Pour plus d'informations, consultez Redimensionnement d'un cluster.	21 mars 2014
Mise à jour de la documentation	Réorganisation et mise à jour de Qu'est-ce qu'Amazon Redshift ? et révision de Vue d'ensemble des clusters provisionnés Amazon Redshift. Publication de divers correctifs de la documentation.	21 février 2014

Modifier	Description	Date de publication
Nouvelle fonctionnalité	Ajout de nouveaux types et tailles de nœuds pour les clusters Amazon Redshift et réécriture de la rubrique de présentation du cluster associée basée sur les commentaires, pour une meilleure organisation et plus de clarté. Pour plus d'informations, consultez Clusters Amazon Redshift provisionnés.	23 janvier 2014
Nouvelle fonctionnalité	Ajout d'informations sur l'utilisation d'adresses IP élastiques (EIP) pour les clusters Amazon Redshift accessibles publiquement dans des clouds privés virtuels. Pour plus d'informations sur les adresses EIP dans Amazon Redshift, consultez Ressources Redshift dans un VPC et Création d'un cluster alloué Amazon Redshift ou d'un groupe de travail Amazon Redshift sans serveur dans un VPC.	20 décembre 2013
Nouvelle fonctionnalité	Ajout d'informations sur les AWS CloudTrail journaux d'Amazon Redshift. Pour plus d'informations sur la prise en charge d'Amazon Redshift pour CloudTrail, consultez. Se connecter avec CloudTrail	13 décembre 2013
Nouvelle fonctionnalité	Ajout d'informations sur le nouveau journal d'activité utilisateur et le paramètre de base de données `enable_user_activity_logging` pour la fonction de journalisation des audits de base de données dans Amazon Redshift. Pour plus d'informations sur la journalisation des audits de base de données, consultez Journalisation des audits de base de données. Pour plus d'informations sur les paramètres de la base de données, consultez Groupes de paramètres Amazon Redshift.	6 décembre 2013

Modifier	Description	Date de publication
Nouvelle fonctionnalité	Mise à jour pour décrire la configuration d'Amazon Redshift pour copier automatiquement des instantanés automatisés et manuels vers une région secondaire. AWS Pour plus d'informations sur la configuration de la copie d'instantanés entre régions, consultez Copier un instantané vers un autre AWS Région.	14 novembre 2013
Nouvelle fonctionnalité	Ajout d'une section pour décrire la journalisation des audits d'Amazon Redshift pour la connexion et l'activité de l'utilisateur et le stockage de ces journaux dans Amazon S3. Pour plus d'informations sur la journalisation des audits de base de données, consultez Journalisation des audits de base de données.	11 novembre 2013
Nouvelle fonctionnalité	Ajout d'une section pour décrire le chiffrement Amazon Redshift avec de nouvelles fonctions pour la gestion des clés de chiffrement dans un module de sécurité matérielle (HSM) et la rotation des clés de chiffrement. Pour plus d'informations sur le chiffrement, HSM et la rotation des clés, consultez Chiffrement de base de données Amazon Redshift, Chiffrement à l'aide de modules de sécurité matérielle, et Rotation des clés de chiffrement.	11 novembre 2013
Nouvelle fonctionnalité	Mise à jour pour décrire la publication de notifications d'événements Amazon Redshift à l'aide d'Amazon SNS. Pour plus d'informations sur les notifications d'événement Amazon Redshift, consultez Notifications d'événement d'un cluster alloué Amazon Redshift.	11 novembre 2013
Nouvelle fonctionnalité	Mise à jour pour décrire les autorisations au niveau des ressources IAM. Pour plus d'informations sur les autorisations IAM d'Amazon Redshift, consultez Sécurité dans Amazon Redshift.	9 août 2013

Modifier	Description	Date de publication
Nouvelle fonctionnalité	Mise à jour pour décrire les métriques de progression de la restauration. Pour plus d'informations, consultez Restauration d'un cluster à partir d'un instantané.	9 août 2013
Nouvelle fonctionnalité	Mise à jour pour décrire le partage d'instantané de cluster et créer des métriques de progression d'instantané. Pour plus d'informations, consultez Partage d'un instantané.	17 juillet 2013
Correctifs de la documentation	Publication de divers correctifs de la documentation.	8 juillet 2013
Nouveaux écrans de console	Mise à jour du Guide de gestion Amazon Redshift pour correspondre aux modifications apportées à la console Amazon Redshift.	22 avril 2013
Nouveau guide	Il s'agit de la première édition du guide de gestion Amazon Redshift.	14 février 2013